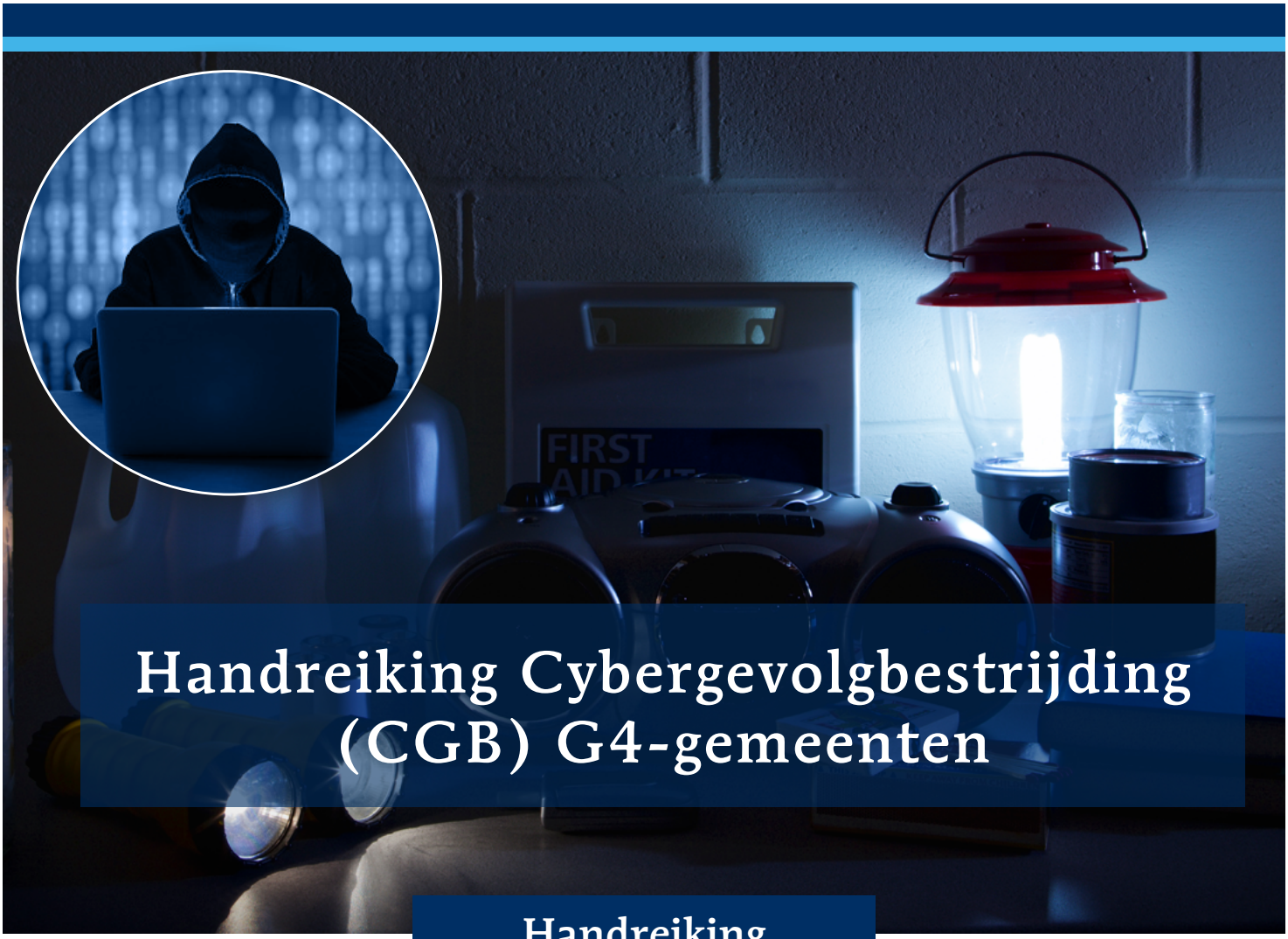


Handreiking Cybergevolgbestrijding (CGB) G4-gemeenten

Handreiking

Deel 2: Koude fase

Naslagwerk cybergevolgbestrijding

Gemeente Amsterdam

Den Haag

Gemeente Rotterdam

Gemeente Utrecht

Openbaar

1 mei 2020

Berenschot

Inhoud

Inleiding

Hoofdstuk 1

1.1 Aanleiding

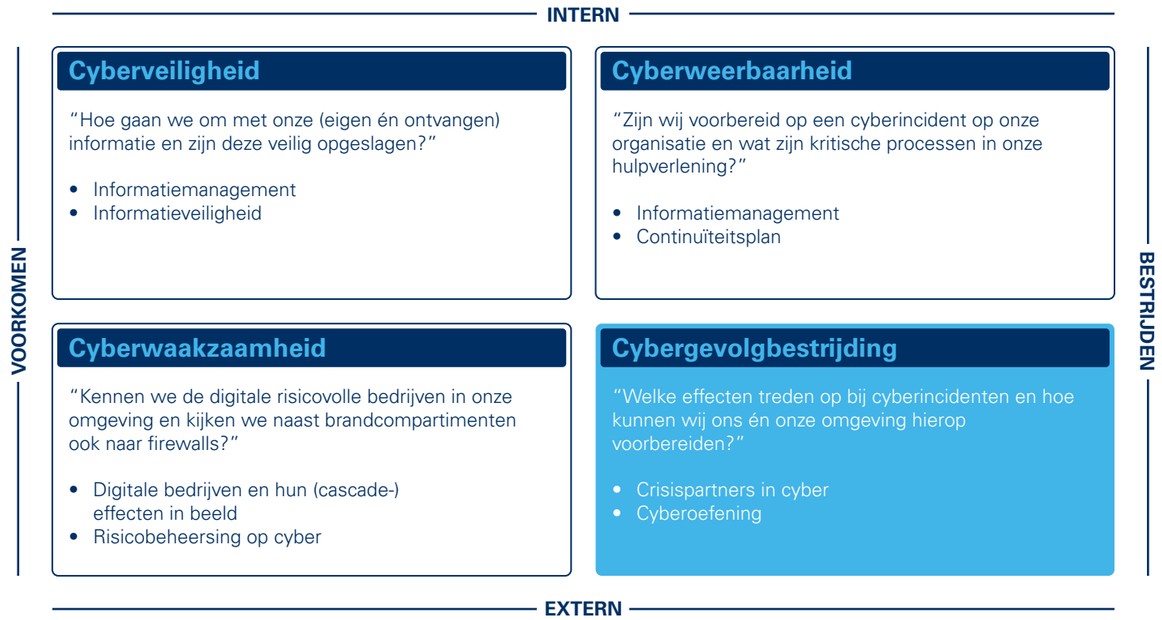
Onze afhankelijkheid van gedigitaliseerde processen en systemen is zo groot geworden dat verstoring, uitval of misbruik kan leiden tot maatschappij-ontwrichtende effecten. Deze maatschappij-ontwrichtende effecten leiden dan tot een crisis waarbij de (lokale) overheid een centrale rol heeft in de crisisbeheersing. Het Cybersecuritybeeld Nederland (CSBN) stelt onder meer dat door de omvang van de dreiging en het achterblijven van de weerbaarheid, risico's ontstaan voor de nationale veiligheid.[1)]

Om de weerbaarheid te vergroten is het essentieel dat de overheid snel en effectief kan reageren op een cybercrisis. Daarom hebben de G4-gemeenten (Amsterdam, Den Haag, Rotterdam en Utrecht) besloten om gezamenlijk te komen tot een Handreiking Cybergevolgbestrijding (CGB). De voorliggende Handreiking CGB is vervolgens ontwikkeld door Berenschot in samenwerking met KPN en adresseert de specifieke kenmerken van een cybercrisis en de consequenties daarvan voor de gevolgbestrijding binnen het (verlengd) lokaal bestuur. Om tot deze handreiking te komen, hebben veel partijen informatie aangeleverd, actief bijgedragen in werksessies en oefeningen of waardevol commentaar geleverd op de handreiking zelf. Dit heeft de handreiking enorm verreikt. Partijen door wie een bijdrage is geleverd, zijn: gemeente Amsterdam, gemeente Den Haag, gemeente Rotterdam, gemeente Utrecht, de Nationale Politie, Veiligheidsregio Amsterdam-Amstelland, Veiligheidsregio Haaglanden, Veiligheidsregio Rotterdam-Rijnmond, Veiligheidsregio Utrecht, het Openbaar Ministerie, IBD, NCTV, NCC, NCSC, IFV en de Werkgroep Digitale Ontwrichting en Cyber.

1.2 Scope, doel en doelgroep

Deze handreiking focust op de gevolgbestrijding van een cybercrisis. Dit betekent dat in kaart wordt gebracht op welke manier cybergevolgbestrijding afwijkt van gevolgbestrijding bij rampen en crises zoals beschreven in het crisisplan van de veiligheidsregio's of het Continuïteitsplan van de G4-gemeenten.[2)] Om de scope van deze handreiking af te bakenen, sluiten we aan bij het cyberkwadrant zoals het in het whitepaper digitale ontwrichting en cyber van het IFV wordt gepositioneerd.[3)] In datzelfde whitepaper wordt ook verwezen naar deze handreiking cybergevolgbestrijding. In de volgende afbeelding is weergegeven hoe cybergevolgbestrijding zich verhoudt tot cyberveiligheid, cyberweerbaarheid en cyberwaakzaamheid (figuur 1).

De handreiking biedt een handelingskader bij cybergevolgbestrijding voor betrokken bestuurders van de *G4* en hun



Figuur 1 Cyberkwadrant (bron: veiligheidsregio IJsselland, 2018)

1) NCSC (2019). *Cybersecuritybeeld Nederland.*

2) N.B. Niet iedere gemeente heeft een continuïteitsplan beschikbaar.

3) IFV (2019). *Whitepaper digitale ontwrichting en cyber.*

directe adviseurs. Deel 1 van de handreiking ‘Warme fase’ is daarbij bedoeld om tijdens een digitale verstoring snel inzicht te krijgen in de verstoring en de mogelijke maatschappelijke effecten ter ondersteuning van de crisisbesluitvorming. In deel 2 van de handreiking ‘Koude fase’ wordt onder meer aandacht besteed aan specifieke kenmerken van een cybercrisis, de daarbij behorende crisisbeheersingsstructuur en de crisisprocessen bij cybergevolgbestrijding. Deel 2 is daarmee meer geschikt als document om in de voorbereiding op een digitale verstoring te gebruiken of als naslagwerk tijdens of na een crisis.

Deze handreiking helpt bestuurders en hun adviseurs zich beter voor te bereiden op het bestrijden van de effecten van een mogelijke cybercrisis en levert handvatten die kunnen helpen tijdens een daadwerkelijke cybercrisis. Goed om daarbij te vermelden is dat de scope van deze handreiking zich beperkt tot de handelingsruimte van de lokale overheid en hun rol in de gevolgbestrijding. Er zijn cybercrises te bedenken die zich op nationale of zelfs internationale schaal afspelen.[4] Hiervoor verwijzen we naar het Nationaal Crisisplan Digitaal (NCP-Digitaal).[5] De Handreiking Cybergevolgbestrijding wordt, na vaststelling in de stuurgroep, door de G4 beschikbaar gesteld voor de overige Nederlandse gemeenten en veiligheidsregio’s.

1.3 Leeswijzer

De handreiking is in twee delen gesplitst. Het deel ‘Warme fase’ is kort en bondig en daarmee geschikt om tijdens een crisis te gebruiken. In het deel ‘Koude fase’ wordt dieper op de onderwerpen uit deel één ingegaan en is meer achtergrondinformatie opgenomen.

De mate van achtergrondkennis op het thema ‘Cyber binnen crisisteams’ is divers. Daarom begint het deel ‘Koude fase’ van de handreiking met een definitie van een cybercrisis, een korte verkenning van het cyberlandschap en een beschrijving van waarin een cybercrisis verschilt van een ‘traditionele’ crisis.

Hoofdstuk 3 staat in het teken van het duiden van de ernst van een cybercrisis. Voor een crisisteam is het essentieel om snel een eerste beeld te kunnen vormen van de verstoring en de mogelijke impact. We gebruiken daarvoor de bouwstenenmethodiek zoals die ook in het NCP-Digitaal wordt gehanteerd. Deze zijn overzichtelijk samengebracht in de Cyber-Crisis-Cirkel (figuur 2). Zo kunnen de bouwstenen eenvoudig in combinatie worden geïnterpreteerd. Het gebruik van de bouwstenen wordt geïllustreerd aan de hand van enkele scenario’s.

Vanuit de eerste duiding wordt in hoofdstuk 4 dieper ingegaan op de consequenties van een cyberverstoring voor de essentiele crisisprocessen. Hieruit volgen aandachtspunten voor de crisisorganisatie die zowel relevant zijn in de voorbereiding op cybergevolgbestrijding als tijdens het daadwerkelijk managen van de gevolgen van deze cyberverstoring.

De handreiking sluit af met een aantal bijlagen waarin aanvullende informatie en uitgangspunten zijn opgenomen zoals een overzicht met mogelijke doelen en methodieken van een cybercrisis, relevante wet- en regelgeving, een netwerkkaart, een documentatielijst en een overzicht van afkortingen.

4) Zoals bijvoorbeeld beschreven in Blackout van Marc Elsberg (2014), waarbij de Europese energievoorziening wordt platgelegd door een cyberaanval.
5) NCSC (2020). *Nationaal Crisisplan Digitaal.*

Cyber als bijzonder crisistype

Hoofdstuk 2

2.1 Definitie van een cybercrisis

De term ‘cyber’ is een containerbegrip voor alles wat met informatie- en communicatietechnologie (ICT) samenhangt. De Nederlandse taal telt meer dan 700 woorden die beginnen met cyber, zoals (cyber)verstoring, (cyber)politie, (cyber)criminaliteit en (cyber)spionage. Dit laat zien hoezeer deze technologie is verweven met onze fysieke wereld. Voor deze G4-handreiking hebben we een cybercrisis gedefinieerd zoals onderstaand staat beschreven. Voor deze definitie sluiten we aan bij de cybersecurity definitie van de Nederlandse Cybersecurity Agenda 2018.[6] Cybergevolgbestrijding is het zoveel mogelijk beperken van de impact van een cybercrisis.

Definitie Cybercrisis

Een cybercrisis is iedere (opzettelijke) verstoring, uitval of misbruik van een gedigitaliseerd proces, (informatie)-systeem of informatiedienst die de maatschappelijke continuïteit, openbare orde en veiligheid bedreigt of verstoort.

2.2 Het cyberlandschap

Cyber is dus een breed begrip. Een cybercrisis is niet eenvoudig af te bakenen als één specifiek soort crisis. Het betreft echter altijd een digitale verstoring. Digitale verstoringen kunnen niet-opzettelijk zijn waarbij de oorzaak van het incident niet met opzet is ontstaan. Niet-opzettelijke verstoringen kunnen bijvoorbeeld veroorzaakt worden door menselijk falen, technisch falen, natuurgeweld (zoals hitte, droogte, vocht). Bij een cybercrisis kunnen verschillende *actoren* betrokken zijn, verschillende *doelwitten* worden geraakt en daarnaast worden verschillende *methodieken* gebruikt om weer verschillende *doelen* te bereiken. Ook heb je verschillende *partners* nodig bij de afhandeling.

- **Actoren:** Indien er sprake is van opzettelijk handelen, spreken we van actoren die een cyberincident veroorzaken, bijvoorbeeld criminelen (netwerken), hacktivisten, cybervandalen, insiders, terroristen of staten. De term ‘actoren’ kan ook worden gebruikt om partijen te benoemen die zich met de crisisbeheersing bezighouden zoals in het NCP-digitaal wordt aangegeven. Om verwarring te voorkomen wordt in dit document alleen naar actoren verwezen bij personen, groepen of organisaties die opzettelijk een cyberincident (dreigen) te veroorzaken. We spreken over partners wanneer het gaat over organisaties die zich met de crisisbeheersing bezighouden.
- **Doelwit:** cyberaanvallen kunnen gericht zijn op ieder individu en iedere organisatie in de maatschappij, van burger, private partijen tot publieke organisaties zoals gemeenten. De impact van een cyberaanval hangt onder andere af van de partij waarop de verstoring is gericht.
- **Doelen:** een cybercrisis kan worden veroorzaakt door storing en uitval van ICT, cyberspionage, cybersabotage, cybercriminaliteit, cyberterrorisme, cyberactivisme (en vandalisme). De doelen van een cybercrisis zijn uitgebreid uitgewerkt in bijlage 1.
- **Methodieken:** de methoden en technieken die gebruikt worden om een cybercrisis te veroorzaken, zijn onder andere een DDoS-aanval, malware-aanval, ransomware-aanval of phishing. Deze staan verder uitgewerkt in bijlage 3.
- **Partners:** specifieke partijen die kunnen worden ingeschakeld ten behoeve van monitoring van het cyberlandschap, bronbestrijding, duiding in de effectbestrijding. Verdere toelichting is uitgewerkt in hoofdstuk 4.

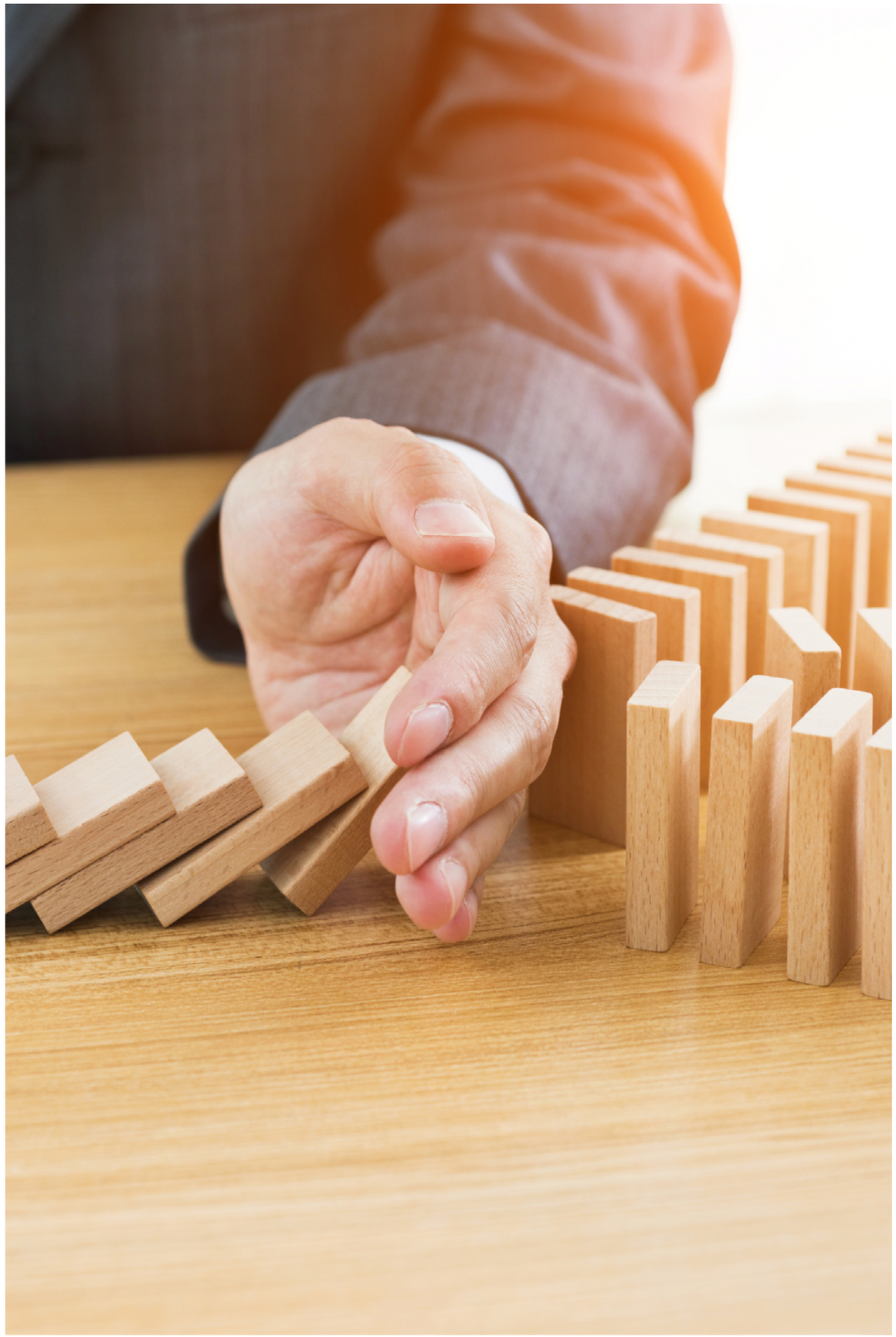
Ieder jaar wordt op landelijk niveau in het CSBN een update gegeven van de grootste cyberdreigingen op dat moment.[7] Het CSBN 2019 van de Nationaal Coördinator Terrorismebestrijding en Veiligheid geeft inzicht in dreigingen, belangen en weerbaarheid op het gebied van cybersecurity in relatie tot de nationale veiligheid. Voor een actueel beeld van de huidige dreigingen is het raadzaam om het CSBN te raadplegen. De Informatie Beveiligingsdienst (IBD) stelt jaarlijks ook een lokaal dreigingsbeeld op, het ‘IBD Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten’, dat online wordt gepubliceerd door de Vereniging van Nederlandse Gemeenten.

6) NCSC (2018). *Nederlandse Cybersecurity agenda: Nederland digitaal veilig.*

7) NCSC (2019). *Cybersecuritybeeld Nederland.*

Duiding van een cybercrisis

Hoofdstuk 3



3.1 De bouwstenen van een cybercrisis

Sommige digitale verstoringen kunnen uitgroeien tot een cybercrisis als er maatschappelijke impact ontstaat, er vermoeden van opzet is en mogelijk gevolgen zijn voor de openbare orde en veiligheid. Om snel een eerste duiding te geven omtrent omvang, ernst, duur en escalatiepotentieel hanteren we zogenaamde 'bouwstenen'. Deze bouwstenen kunnen worden beschouwd als de kenmerken van een crisis, die per situatie verschillen.

De bouwsteenbenadering is gebaseerd op de werkwijze van het NCP-Digitaal.[8] Bij de keuze voor bouwstenen en bouwsteenwaarden is geredeneerd vanuit relevantie voor de crisisrespons.

In deze handreiking wordt de bouwsteenbenadering vooral gebruikt als duidingsinstrument om erachter te komen welke eigenschappen een cybercrisis heeft en zo een snelle inschatting te maken omtrent verwachte ernst, omvang, duur, escalatiepotentieel en gevolgbestrijdingsacties. Ofwel wat is de (verwachte) impact van de crisis op basis waarvan een handelingsperspectief kan worden bepaald.
Kortom, de bouwstenen kunnen worden ingezet in de beeldvormingsfase ten behoeve van het vormen van een adequaat beeld van de situatie en in de oordeelvormingsfase voor het uitdenken van een toekomstige scenario over het verloop van het incidenten.

In de figuur 2 staat een overzicht van alle bouwstenen, vormgegeven in een cirkel. De indeling volgt op hoofdlijnen die van het NCP-Digitaal, waarbij enkele bouwstenen en waarden voor deze handreiking aangepast zijn aan de scope van deze handreiking. Bij een crisis zijn de waardes van meerdere bouwstenen waarschijnlijk nog onbekend.

Of het een klein, gemiddeld, groot of (inter)nationaal scenario is wordt bepaald door de weging van alle beschikbare bouwstenen. Dat betekent bijvoorbeeld dat in een klein scenario (S1) ook elementen van een zwaarder (S2/S4) scenario kunnen zitten, of dat in een zwaar scenario (bijvoorbeeld S3) ook elementen van een lichter scenario kunnen zitten. De cirkel helpt het team doordat verbanden tussen bouwstenen zichtbaar worden gemaakt die in samenhang inzicht geven in de ernst van de situatie.

Ook bij *dreiging* van een cybercrisis is deze benadering goed toepasbaar voor een eerste duiding. Door bij de beeldvormingsronde in de crisisvergadering alle bouwstenen van een waarde te voorzien, komen alle (relevante) eigenschappen van een cybercrisis aan de orde en wordt het beeld over de situatie volledige. In de oordeelsvormingsfase kan dan direct worden nagedacht over wat dit betekent voor de effectbestrijding en crisisrespons.

8) NCSC (2020). *Nationaal Crisisplan Digitaal.*

NB: één van de bouwsteenwaarden betreft de vitale infrastructuur. Landelijk is gedefinieerd wat de vitale infrastructuur is en welke regels daarvoor gelden.[9] Deze staan voor het gemak ook opgenomen in bijlage 6. Lokaal en regionaal kunnen echter andere sectoren of processen als vitaal worden aangemerkt omdat ze bij verstoring grote risico's met zich meebrengen of als kwetsbaar zijn gedefinieerd.

3.2 Impact van een cyberincident

De impact begrijpen van een digitale verstoring is lastig. Dit 'begrijpen' noemen we het duiden van de impact. Een cybercrisis veroorzaakt door een bewuste cyberaanval heeft bijvoorbeeld een andere impact dan een technische storing. En een cyberaanval gericht op de gemeente heeft weer een andere impact dan een cyberaanval gericht op heel Nederland. Denk hierbij aan de wijze van respons, de communicatie en de escalatiemogelijkheden.

Om als crisisteam in staat te zijn deze impact te duiden is digitale expertise essentieel. Iedereen in een crisisteam moet een bepaalde basiskennis hebben van digitale processen en terminologie. Zonder deze basiskennis is het lastig om de experts te begrijpen die het crisisteam kunnen ondersteunen.

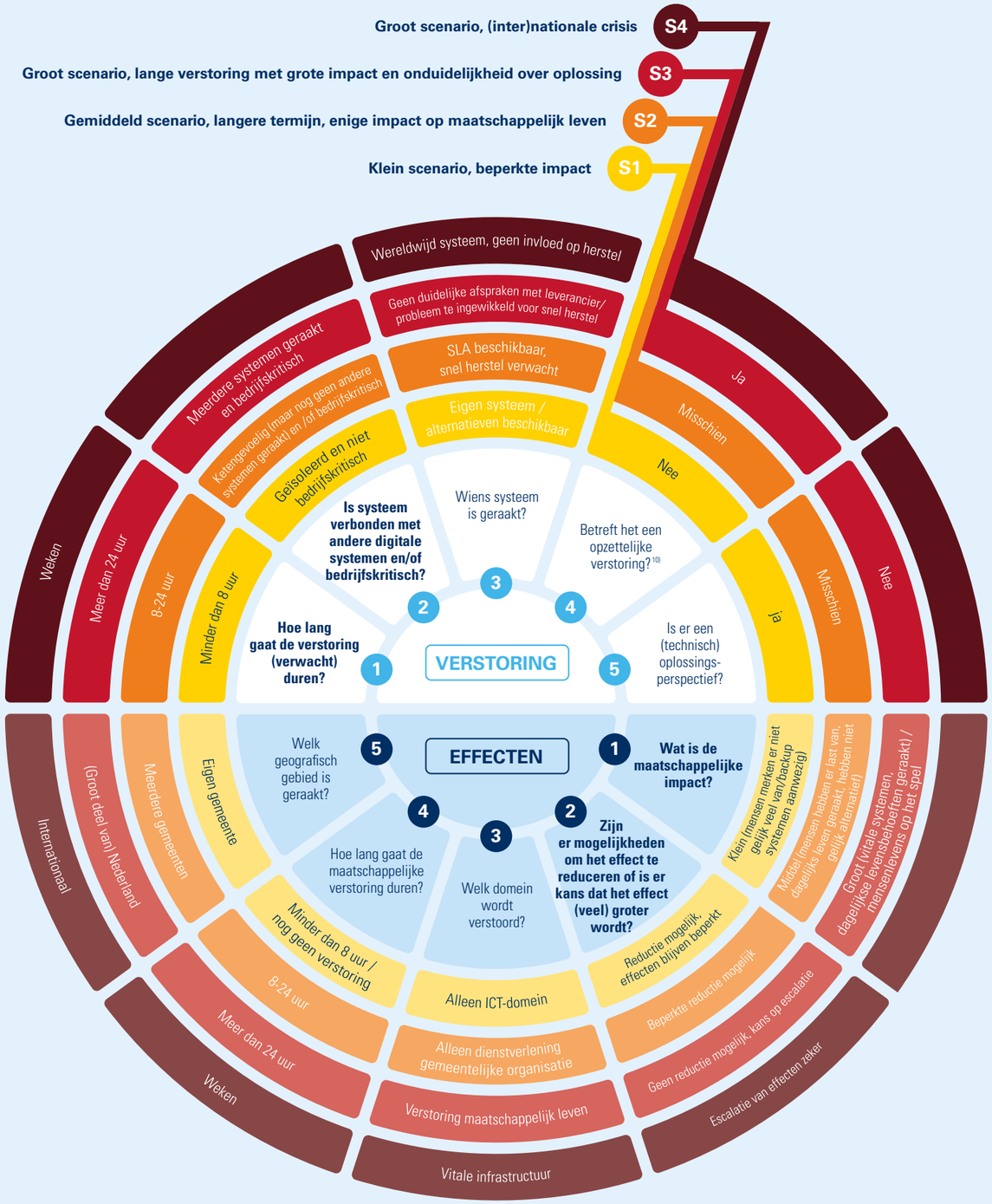
Digitale expertise ter ondersteuning van het crisisteam kan verschillende vormen aannemen:

- Kennis van oplossen technisch component (ver)storing
- Duiden impact technische verstoring op organisatieprocessen (bijvoorbeeld gemeentelijke dienstverlening)
- Duiden impact van de verstoring op het maatschappelijk leven

Kennis van de **technische kant van de verstoring** zit primair bij de leverancier van het geraakte systeem. Deze informatie is vooral relevant voor de teams die zich met het oplossen van de verstoring bezighouden. De getroffen organisatie is zelf verantwoordelijk voor het oplossen van de technische verstoring (al dan niet met behulp van de leverancier) en het continueren van de eigen dienstverlening. Het helpt als vooraf contractuele afspraken zijn gemaakt tussen leverancier en afnemer over informatieoverdracht vanuit de leverancier naar de getroffen organisatie ten behoeve van de crisisbeheersing.

Kennis van **impact van de technische verstoring** op organisatieprocessen zit primair bij de CISO van de geraakte organisatie. Het betrekken van een CISO in het crisisteam kan daarmee beeld- en oordeelsvorming vergemakkelijken. Indien er

9) Overheid.nl. *Besluit beveiliging netwerk- en informatiesystemen.*



Figuur 2 De Cyber-Crisis-Cirkel

10) De politie gaat op voorhand uit van een opzettelijke verstoring tenzij duidelijk is dat dit niet zo is.

meerdere crisisteams actief zijn die een beroep op aanwezigheid van de CISO doen, zal deze goed moeten uitvragen welke informatiebehoefte er ligt vanuit deze crisisteams. Om zo een goede afweging te kunnen maken omtrent aanwezigheid en advies.

Het inschatten van **de impact van verstoringen** op de maatschappij ligt primair bij de veiligheidsregio's. De veiligheidsregio's bereiden zich vanuit van hun wettelijke taak voor op het verkleinen van effecten van verstoringen van het maatschappelijk leven. Dit is een rol die veiligheidsregio's vervullen voor allerlei soorten crises en hier zit expertise omtrent maatschappelijke continuïteit. Bij de afdelingen OOV van de gemeenten is daarnaast expertise aanwezig over de specifieke maatschappelijke vraagstukken in de betreffende gemeente en wijken. Ook deze expertise is noodzakelijk voor een goede impactanalyse van de verstoring op het maatschappelijk leven en zal in de analyse een plek moeten krijgen.

Voor cybercrises in de gemeentelijke organisatie kan de gemeentelijke calamiteitenorganisatie ondersteuning vragen aan de IBD als het gaat om de inschatting van de aard, omvang en ernst van de situatie. De IBD adviseert over te nemen maatregelen en acties en heeft een directe verbinding met onder andere belangrijke ICT-leveranciers, Computer Emergency Response Teams (CERT's) van andere organisaties, het NCSC en internationale CERT's. Zie hoofdstuk 4 voor een nadere toelichting.

De politie zal adviseren vanuit het oogpunt van opsporing en vervolging. Binnen de politie zijn verschillende cyberteams actief, waaronder het cybercrimeteam vanuit de regionale eenheid, die een mogelijk opzettelijke cybercrisis technisch kunnen duiden op oorzaak en bron en de mogelijkheden van opsporing en vervolging.

3.3 Voorbeelden ter illustratie

Hoewel het bijna onmogelijk is om alle soorten cybercrises te vatten in een paar voorbeelden (er zijn talloze varianten te bedenken), kunnen deze voorbeelden wel dienen om een gevoel te krijgen bij verschillende type crises en bijbehorende respons. Hiernavolgend zijn enkele voorbeelden uitgewerkt. Hierbij is per scenario (S1-S4) uit de cirkel één voorbeeld opgenomen. Ook is een voorbeeld van een dreigingsscenario opgenomen. In de voorbeelden wordt duidelijk dat er verschil is tussen de waardes van de bouwstenen en dat deze in gezamenlijkheid moeten worden gewogen en dan leiden tot een bepaald scenario. Of het een klein, gemiddeld, groot of nationaal scenario is, wordt bepaald door een afweging van alle beschikbare bouwstenen. En dat betekent bijvoorbeeld dat in een klein scenario ook elementen van een hoger scenario kunnen zitten.

Calamiteiten in de interne bedrijfsvoering van de gemeente zonder effecten op de openbare orde, veiligheid en maatschappij worden buiten beschouwing gelaten, aangezien deze buiten de definitie vallen. Denk bijvoorbeeld aan een storing in een koelinstallatie in een datacenter van een gemeente, waardoor dienstverlening wordt verstoord. Dergelijke crises worden intern binnen de organisatie afgehandeld.

In de volgende scenario's ligt de focus op situaties waarbij de 'maatschappelijke continuïteit, openbare orde en veiligheid wordt bedreigd of verstoord'. Per scenario wordt aangegeven hoe de cirkel is gebruikt.

Dreiging van een cyberincident

Onderzoekers hebben een ernstig beveiligingslek gevonden in een type processor dat in driekwart van alle computersystemen in de wereld wordt gebruikt.[11] Het gaat om verschillende gerelateerde kwetsbaarheden, die technisch uiterst complex zijn. Uit onderzoek blijkt dat een aanval moeilijk te detecteren is en bovendien geen sporen achterlaat. De onderzoekers hebben hun bevindingen gepubliceerd op verschillende websites en in enkele whitepapers. Het nieuws is met veel ophef naar buiten gebracht, mede omdat het probleem niet simpel is op te lossen. Diverse fabrikanten van besturingssystemen hebben inmiddels updates (patches) uitgebracht, maar de werking daarvan is beperkt. Er zijn veelal ook configuratieaanpassingen nodig die door beheerders van geraakte systemen zelf moeten worden uitgevoerd. Het CERT heeft de kwetsbaarheid ingeschaald met hoge kans op misbruik en hoge ernst van de schade (een zogenaamd high/high beveiligingsadvies).

Omdat de kwetsbaarheid prominent in de media aan bod komt, krijgt het lek ook flink wat bestuurlijke aandacht. CERT's worden gevraagd om de mogelijke impact op de eigen organisaties zo snel mogelijk in kaart te brengen. Veel organisaties kiezen ervoor om preventief op te schalen naar een hogere alarmfase en hebben draaiboeken paraat voor de situatie dat er daadwerkelijk systemen en diensten uitvallen. Organisaties vragen ook aan ketenpartners om uitsluitsel te geven over de mogelijke impact. Binnen de 'Information Sharing and Analysis Centers' (ISAC's) wordt informatie uitgewisseld over mogelijke maatregelen en technische oplossingen. Het NCSC organiseert een informatiebijeenkomst voor vertegenwoordigers van vitale sectoren en roept de ISAC's op dit ook regionaal te doen voor de eigen sectoren.

Dit scenario is een voorbeeld van een dreigende cybercrisis. Het scenario illustreert dat een cybercrisis acuut kan ontstaan en in potentie een enorme impact en omvang kan hebben: internationaal karakter, snelle verspreiding, ketenafhankelijkheid, ontbreken van een direct passende oplossing, etc. Hoewel er in dit scenario nog geen sprake is van een crisis is preventieve actie nodig, onder meer om de mogelijke impact te bepalen en preventieve maatregelen te treffen. Manifestatie van het beveiligingslek kan in potentie de digitale wereld platleggen op wereldwijde schaal.

11) Dit scenario is fictief, maar gebaseerd op kwetsbaarheden die zich daadwerkelijk hebben voorgedaan.

S1. Gemeente is geraakt met beperkt maatschappelijke impact (klein scenario)

Een medewerker van de sociale dienst is slachtoffer van phishing en heeft een besmet bestand in een e-mailbijlage geopend. Hierdoor is zogenaamde ransomware actief geworden. Deze malware versleutelt willekeurig bestanden waar de medewerker toegang tot heeft. De malware verspreidt zich snel binnen de organisatie en daarbuiten. Het is nog onduidelijk welke andere onderdelen van het gemeentelijk systeem zijn besmet. Er komen signalen van besmetting van belangrijke ketenpartners. Klantdossiers zijn niet meer toegankelijk en sommige werkzaamheden moeten tijdelijk worden gestaakt, waardoor de dienstverlening op het gebied van bijvoorbeeld werk en financiële bijstand acuut in gevaar komt. Berichtgeving hierover in de lokale media zorgt voor (politieke) onrust.

Na een eerste onderzoek blijkt dat ook de back-up besmet is, waardoor er niet direct een handelingsperspectief aanwezig is. Vooralsnog weigert de gemeente losgeld te betalen voor het ontsleutelen van bestanden om de afpersers niet in de kaart te spelen.[12] Bij de gemeente treedt ondertussen het Continuïteitsplan in werking. De sociale dienst schakelt over op het noodplan. De dienstverlening moet grotendeels handmatig worden uitgevoerd. Dit betreft onder meer het verlenen van financiële bijstand aan burgers. Bij de gemeentelijke loketten ontstaan langere wachtrijen, de dienstverlening kan in aangepaste vorm doorgaan. Grote zorg van het crisisteam is mogelijke escalatie door uitval/besmetting van andere systemen binnen de gemeente en de eventuele maatschappelijke consequenties.

De politie verzoekt het OM om inzet extra opsporingsmiddelen om een verdachte hacker uit de gemeente nader te monitoren. Dit verzoek wordt ook in de driehoek besproken. Na goedkeuring en inzet extra opsporingsmiddelen blijkt dit inderdaad de vermoedelijke dader. De politie bereidt een arrestatie voor.

Dit is een voorbeeld van cybercriminaliteit waarbij een gemeente wordt geraakt en de effecten zich beperkt uitspreiden naar het maatschappelijk domein. Dit scenario illustreert onder meer dat een verstoring niet altijd direct wordt opgemerkt (de back-up is al in een eerder stadium besmet), dat er effecten zijn buiten de organisatie en dat die niet gelijk gevolgen (hoeven) te hebben voor openbare orde en veiligheid.

Bouwsteenwaarden: opzettelijk, in de gemeente, maatschappelijke impact klein, geraakt systeem ketengevoelig, eigen responscapaciteit van de gemeente geraakt, effecten binnen de gemeente, (technisch) oplossingsperspectief ontstaat door mogelijke arrestatie actor.

12) Hoe realistisch dit scenario is, blijkt onder meer uit het feit dat diverse Amerikaanse steden openlijk losgeld betalen aan criminelen om weer toegang te krijgen tot hun informatie.

S2. Niet-vitale (lokale) sectoren geraakt, enige maatschappelijke impact (gemiddeld scenario)

In de afgelopen jaren zijn basisscholen veelvuldig digitaal aangevallen. Een stichting van middelbare scholen in een bepaalde gemeente is deze keer slachtoffer van een digitale aanval door een hacker. Hierdoor zijn vele bestanden versleuteld met ransomware. De hacker wil geld ontvangen in ruil voor het toegankelijk maken van de bestanden.
Uit de eerste onderzoeken blijkt dat de versleutelde bestanden belangrijke persoonsgegevens en cijfers van studenten, en functioneringsgegevens van docenten bevatten. De hacker dreigt de gegevens op korte termijn te publiceren wanneer er niet wordt betaald. De aanval is ook bekend bij de landelijke politiek. Enkele Kamerleden hebben vragen gesteld aan de minister van OCW.

Op sociale media circuleren berichten van scholieren die voor hun examen zitten en de school willen aanklagen als gevolg van de aanval. Het is onduidelijk wat hiervan waar is, maar het zorgt publiekelijk voor grote verontwaardiging. Er wordt ook getwijfeld aan de effectiviteit van de respons.

Dit is een voorbeeld van cybercriminaliteit. Dit scenario illustreert de complexiteit van een cyberaanval en ook het feit dat niet altijd direct een (technisch) oplossingsperspectief aanwezig is, bijvoorbeeld als gegevens daadwerkelijk zijn versleuteld of gelekt. Bovendien moet nagedacht worden over het al dan niet betalen aan de hacker en het nadrukkelijker inzetten op opsporen.

Bouwsteenwaarden: opzettelijk, in de gemeente, geraakt systeem ketengevoelig, maatschappelijke impact middel, geraakt gebied eigen gemeente, impact uitval systeem middel, (technisch) oplossingsperspectief ontbreekt.

S3. Vitale sectoren geraakt, lange maatschappelijke verstoring (groot scenario)

In de regio is er een grote stroomstoring. De oorzaak is nog onduidelijk, maar er gaan geruchten dat het zou gaan om een cyberaanval op de energievoorziening. Naast vitale sectoren zijn ook andere sectoren geraakt. Chaos dreigt.

Veel GSM-masten beschikken niet of beperkt over een noodstroomvoorziening, waardoor mobiel internet en telecom in grote delen van de regio niet beschikbaar is. Hierdoor vallen ook betaalsystemen uit. Naarmate de storing langer aanhoudt, ontstaan nieuwe problemen. Bejaardentehuizen en scholen zitten zonder stroom, supermarkten kampen met een tekort aan producten. Er ontstaat een run op schaarse goederen. Omdat ook veiligheidssystemen zijn uitgevallen, stijgt kleine criminaliteit. In het centrum sluiten veel winkels hun deuren, waardoor grote schade wordt geleden. Door de stroomuitval ervaart ook het openbaar vervoer overlast (treinen rijden niet meer).

De aanpak van het cyberprobleem gaat moeizaam omdat aanvankelijk niet duidelijk is wat precies de oorzaak is. Er wordt gedacht aan een digitale aanval, maar later wordt duidelijk dat het gaat om een storing. Hierdoor worden niet direct de juiste stakeholders betrokken.

Dit is een voorbeeld van storing en uitval, waarbij de vitale infrastructuur op verschillende onderdelen (vooralsnog binnen één regio) is geraakt. Dit scenario illustreert cascade-effecten van een cybercrisis. Bij dit type crisis is niet direct duidelijk wat de oorzaak is waardoor de opschaling naar de juiste stakeholders vertraging oploopt.

Bouwsteenwaarden: niet-opzettelijk, buiten de gemeente, meerdere systemen geraakt, vitale infrastructuur geraakt, meerdere gemeenten in Nederland, maatschappelijke impact groot, (technisch) oplossingsperspectief ontbreekt.

S4. Landelijk cyberincident (groot scenario)

Nederland heeft te maken met een reeks digitale aanvallen op grote industriële controlesystemen binnen de vitale infrastructuur. Eerder deed de Algemene Rekenkamer al onderzoek naar de kwetsbaarheid van soortgelijke systemen binnen de vitale waterwerken, waaruit bleek dat de beveiliging op onderdelen te kort schiet. Bij één object werd ongeautoriseerde toegang tot het systeem zelfs niet gedetecteerd.[13] In dit geval is de drinkwatervoorziening geraakt in meerdere regio's. Omdat meerdere regio's en voorzieningen geraakt zijn, is er een acuut tekort aan technische expertise. Enkele drinkwaterbedrijven schakelen daarom externe deskundigen van private partijen in voor (forensisch) onderzoek en gevolgbestrijding. De watervoorziening wordt binnen 48 uur hersteld, maar de verstoring veroorzaakt grote maatschappelijke onrust en een landelijke discussie over de kwetsbaarheid en afhankelijkheid van de vitale infrastructuur.

In dit scenario is de vitale infrastructuur geraakt, waarbij de impact nadrukkelijk in verschillende regio's wordt gevoeld. In dit scenario treedt de landelijke crisisstructuur in werking. Dit scenario illustreert onder meer de afhankelijkheid van de private sector (schaarste van expertise) bij een grootschalige crisissituatie.

Bouwsteenwaarden: opzettelijk, buiten de gemeente, geraakt systeem meerdere systemen, vitale infrastructuur geraakt, meerdere gemeenten/regio's in Nederland, impact groot, (technisch) oplossingsperspectief ontbreekt.

13) Het scenario is fictief, maar dit specifieke voorbeeld is echt. Zie daarvoor de publicatie van de Rekenkamer *Digitale dijkverzwaring: cybersecurity en vitale waterwerken*.

Respons van de crisisorganisatie

Hoofdstuk 4

Na introductie van de bouwsteenmethodiek voor de oordeelsvorming in het crisisteam stappen we nu over naar de crisisrespons. In de volgende paragraaf beschrijven we kort hoe de crisisresponsorganisatie eruitziet, waarbij we onderscheid maken tussen de interne gemeentelijke calamiteitenorganisatie (bedrijfscontinuïteit), de driehoek en de GRIP-structuur[14]).

Daarna onderscheiden we in paragraaf 4.2 de essentiële crisisprocessen zoals die binnen de crisisstructuur worden gehanteerd. Bij elk proces geven we aan wat de aandachtspunten zijn zodat bij een cybercrisis snel zichtbaar is waar het crisisteam extra aandacht aan moet besteden.

14) GRIP-structuur staat voor Gecoördineerde Regionale Incidentbestrijdingsprocedure en beschrijft de manier waarop de veiligheidsregio's opschalen.

4.1 Crisisbeheersingsstructuur

Als binnen de gemeente zich een crisis voordoet die vooral de interne organisatie raakt, wordt deze afgehandeld langs de lijnen zoals beschreven in de bedrijfscontinuïteitsplannen van de betreffende gemeente. Globaal gezegd gebeurt dit door een intern calamiteitenteam onder aansturing van de gemeentesecretaris en verantwoordelijkheid van het college. De CISO heeft daarin een belangrijke coördinerende rol voor de continuïteit van het digitale domein. Daarnaast geldt als uitgangspunt dat bij elke opzettelijke activiteit aangifte wordt gedaan door de gemeente. Niet elke gemeente heeft de beschikking over actuele bedrijfscontinuïteitsplannen. Dit is iets waar in de komende jaren aan gewerkt wordt.

Indien blijkt dat de crisis ook (grote) effecten heeft op de openbare orde en veiligheid, of dat er behoefte is aan extra opsporingsbevoegdheden om de actor te achterhalen, komt de driehoek bij elkaar. Mochten de hulpverleningsdiensten worden ingezet en daarbij (multidisciplinaire) afstemming nodig zijn, of is er sprake van crisisbeheersing of rampenbestrijding, dan kan gebruik worden gemaakt van de GRIP-structuur, waarbij heldere besluitvormings- en informatielijnen zijn afgesproken met multidisciplinaire crisisteams in het veld (CoPI) op tactisch

niveau (ROT) en op bestuurlijk niveau (BT). In geval van een dreigende situatie, er is nog geen sprake van daadwerkelijke inzet van de hulpverleningsdiensten, wordt deze dreiging geanalyseerd in een informele ROT-setting. De naam hiervan verschilt per veiligheidsregio, denk daarbij aan 'voorbereidend ROT' of 'planningsstaf'.

Het kan zijn dat er wel sprake is van een cybercrisis en dat de effecten zichtbaar zijn in domeinen waar de hulpdiensten nog geen rol hebben. Vaak zal dan het informele ROT wel bij elkaar komen om de situatie te analyseren en scenario's te bespreken. Ook zal indien nodig het gemeentelijk crisisteam worden ingericht. Dit wordt in 4.1.4 verder toegelicht.

In theorie kunnen de teams tegelijkertijd actief zijn in hun eigen rol waarbij de focus van het gemeentelijke team zich richt op de eigen organisatie, de focus van ROT en BT zich richt op het bestrijden van de effecten in het fysieke domein, het gemeentelijk crisisteam zich richt op de effecten in het niet-fysieke domein en de driehoek zich richt op opsporingsvraagstukken. Hiernavolgend worden deze teams kort beschreven.

4.1.1 Gemeentelijk calamiteitenteam

Bij een cyberincident binnen de gemeentelijke organisatie kan het gemeentelijk calamiteitenteam, onder verantwoordelijkheid van de gemeentesecretaris, worden ingesteld. Naast de gemeentesecretaris nemen aan dit calamiteitenteam functionarissen deel binnen de gemeente met expertise op het gebied van facilitaire zaken (zoals ICT inclusief telefonie/andere communicatiemiddelen, gebouwbeheer en beveiliging) en crisiscommunicatie. In het continuïteitsplan van iedere gemeente staat onder andere beschreven welke functionarissen bij ICT-storingen of -uitval belast zijn met het reduceren van de effecten van een calamiteit en het continueren van de bedrijfsprocessen van de gemeente. In de meeste gemeenten heeft de CISO hierin een coördinerende rol. Zie voor nadere uitwerking de bedrijfscontinuïteitsplannen van de betreffende gemeente. Samenvattend: dit team houdt zich bezig met het borgen van de gemeentelijk organisatiecontinuïteit en effectbestrijding bij gevolgen binnen de gemeentelijke beleidsdomeinen.

4.1.2 De driehoek

Driehoeksoverleg (artikel 13 Politiewet 2012)[15]: De politie staat onder duaal gezag: voor de handhaving van de openbare orde en voor de hulpverlening ligt het gezag bij de burgemeester en voor de strafrechtelijke handhaving ligt het gezag bij de officier van justitie. Dit overleg tussen politie, burgemeester en OM is de lokale gezagsdriehoek. De burgemeester is meestal de voorzitter van het driehoeksoverleg.[16] In het geval van een cybercrisis kan het zijn dat de politie extra opsporingsmiddelen vraagt om zo de actor op te sporen. Dit moet in overleg met het OM vanuit strafrechtelijk oogpunt, maar ook overleg met de burgemeester is relevant omdat de uitkomst invloed kan hebben voor een snelle(re) afhandeling van de crisis. Er is dan zowel een strafrechtelijke afweging als een afweging in het kader van openbare orde. De driehoek neemt hier in gezamenlijkheid een besluit over zodat de politie altijd kan blijven voldoen aan haar gezagsrelatie met zowel OM als burgemeester. De informatie uit het driehoeksoverleg wordt waar relevant voor de crisisbeheersing gedeeld met het beleidsteam op basis van *need to know*.

Het driehoeksoverleg is daarmee een ander type crisisoverleg dan dat van het interne calamiteitenteam en dat van het beleidsteam.

4.1.3 De GRIP-structuur

Bij een cybercrisis in het geografisch gebied van de gemeente kan de gemeente als bevoegd gezag gebruik maken van de crisisbeheersingsstructuur. Er wordt dan via de GRIP-structuur opgeschaald en de burgemeester laat zich in het GBT adviseren over de consequenties van de digitale verstoring op het maatschappelijk leven en de te nemen maatregelen omtrent de effectbestrijding. Deze opschaling vindt plaats als de effecten van deze cybercrisis leiden tot (grootschalige) inzet van de hulpverleningsdiensten. Er wordt dan binnen de GRIP-structuur opgeschaald om snel een crisisteam te formeren en heldere informatie-besluitvormingslijnen te creëren.

De GRIP-structuur is ontwikkeld om bij crises die één of meerdere gemeenten treffen de crisisbeheersing te structureren. Binnen deze structuur overleggen de hulpverleningsdiensten (brandweer, politie, geneeskundige zorg en bevolkingszorg) onder gezag van de burgemeester of voorzitter veiligheidsregio om de crisis zo effectief mogelijk te bestrijden en de effecten te beperken. Afhankelijk van de omvang van een incident vallen deze diensten onder het bevoegd gezag van de burgemeester van de getroffen gemeente (GRIP-1 tot en met 3) óf van de voorzitter van de veiligheidsregio (GRIP-4).[17] Ten behoeve van effectieve afhandeling is er een aantal ondersteunende secties ingericht:

15) Overheid.nl. *Politiewet 2012*.

16) Tekst deels overgenomen van burgemeesters.nl, voor meer informatie zie burgemeester.nl, Politiewet 2012.

17) IFV (2017). *GRIP en de flexibele toepassing ervan.*

informatiemanagement, operationele leiding en crisiscommunicatie. Deze zijn onafhankelijk van het soort crisis te gebruiken.

De crisisplannen van de veiligheidsregio's beschrijven de concrete invulling van de crisisorganisatie in die betreffende regio.

4.1.4 Gemeentelijke crisisorganisatie

Er zijn cybercrises denkbaar waar het lokaal bestuur effecten van ondervindt, maar die buiten het traditionele domein van de veiligheidsregio vallen en ook de eigen gemeentelijke dienstverlening niet direct raken. Een recent voorbeeld is de hack van de universiteit Maastricht in december 2019 waardoor studenten en medewerkers van de universiteit lange tijd niet konden inloggen en waardoor ook bij de gemeente Maastricht vragen binnen kwamen over de afhandeling en effecten. Denk bijvoorbeeld ook aan het uitvallen van diensten die door een gemeenschappelijke regeling worden geleverd. Voor dit type (cyber)crisis is gemeente ook aan zet om zich met de gevolgen bezig te houden. De structuur waarbinnen dit gebeurt verschilt per gemeente en is niet overal formeel beschreven.

Landelijk speelt de discussie over de flexibilisering van de GRIP-structuur, waarbij de binnen deze structuur ontwikkelde processen ook voor andere crisistypen zouden kunnen worden gebruikt. Ook zouden elementen van de regionale crisisorganisatie daarmee ter beschikking kunnen worden gesteld aan de lokale crisisorganisatie.

Het is aan de gemeenten en de veiligheidsregio samen om te bepalen of onderdelen van de regionale crisisorganisatie ingezet kunnen worden binnen de gemeentelijke crisisorganisatie. Mocht deze wens er zijn dan moet dat formeel op regionaal niveau onder verantwoordelijkheid van het bestuur van de veiligheidsregio's worden besloten.

Enkele aandachtspunten omdat de gemeentelijke crisisorganisatie niet overal formeel beschreven is:

- Kennis van de technische kant van de verstoring zit primair bij de leverancier van het geraakte systeem. Deze informatie is vooral relevant voor de teams die zich met het oplossen van de verstoring bezighouden.

- Kennis van impact van de technische verstoring op organisatieprocessen zit primair bij de CISO van de geraakte organisatie. Het betrekken van een CISO in het crisisteam kan daarmee beeld- en oordeelsvorming vergemakkelijken.

- Kennis van impact van verstoringen op het maatschappelijk leven zit bij de veiligheidsregio's en de afdelingen OOV van de gemeenten.

- Per crisis moet worden gekeken welk domein en systemen geraakt zijn om zo de juiste inhoudelijk adviseurs aan tafel te krijgen. Dit is nog niet in planvorming vastgelegd.

- Het zal voor deelnemers die standaard aan tafel zitten onwennig zijn als ze bij een ander type crisis geen rol hebben. Het helpt om dit vooraf goed af te spreken en tijdens de crisis op te blijven reflecteren.

- Zorg dat de processen informatiemanagement, crisiscommunicatie en leiding- en coördinatie georganiseerd zijn.

4.1.5 Nationaal versus regionaal

In het Nationaal Crisisplan Digitaal wordt de landelijke reactie op een cybercrisis beschreven. Tegelijkertijd is er ook een regionale rol bij het bestrijden van een landelijke cybercrisis. Vanzelfsprekend blijft het lokale of regionale gezag verantwoordelijk voor effectbestrijding conform de Wet veiligheidsregio's (Wvr).

Wanneer er sprake is van een cybercrisis binnen de gemeentelijke crisisorganisatie is de IBD de partij die informatie over het cybercomponent en de oplossingsstrategie kan delen met de getroffen gemeenten. Ook is de IBD de liaison namens de gemeenten richting het NCSC om eventuele lokale oplossingen en vraagstukken te delen.

Politie en OM zijn landelijk georganiseerd, daarmee wordt de opsporingstaak bij een landelijke cybercrisis ook vanuit die partijen landelijk gecoördineerd. Het staat niet specifiek beschreven hoe dit zich verhoudt tot de getroffen lokale partijen en de driehoeken. Lokale bestuurders zullen zich bij een crisis op landelijke schaal vooral laten informeren vanuit OM en politie voor wat betreft de opsporingstaak en afweging.

Indien de cybercrisis beperkt blijft tot een gemeente of regio is het nationale niveau vooral ondersteunend. Indien de gemeente zelf getroffen wordt zal de IBD ondersteunen en de link vormen naar het NCSC. Indien de gemeentelijke organisatie niet zelf getroffen is zal de informatie van het NCSC via de politie en het OM (indien mogelijk) ingebracht worden binnen de crisisbeheersingsteams. In de volgende paragraaf worden de taken

en verantwoordelijkheden van de verschillende (nationale) partijen verder toegelicht.

Indien de effecten zodanig bovenregionaal zijn dat er landelijk wordt opgeschaald (meerdere veiligheidsregio's zijn geraakt) zullen het NCC en het LOCC-bovenregionaal zich vooral richten op informatiedeling en het landelijk informatiebeeld. De informatiemanagers vanuit het ROT hebben inzicht in het landelijk beeld zoals dat binnen het Landelijk Crisismanagement Systeem (LCMS) wordt bijgehouden.

In de volgende tabel is een overzicht te vinden van de verschillende teams die bij een cybercrisis ingezet kunnen worden.

Tabel 1. In te zetten team(s) cybergevolgbestrijding per type cybercrisis

In te zetten team(s)	Type cybercrisis
Driehoeksoverleg.	Indien opzettelijkheid niet uit te sluiten is.
Gemeentelijk calamiteitenteam/ gemeentelijk crisisteam.	Indien gemeente geraakt wordt, effecten in het gemeentelijk domein plaatsvinden.
GRIP-structuur (ROT/BT).	Indien maatschappelijk leven verstoord.
Nationale crisisbeheersingsstructuur.	Indien landelijke verstoring.

4.1.6 Relevante partijen bij cybergevolgbestrijding

In deze paragraaf volgt een overzicht van de belangrijkste partijen bij cybergevolgbestrijding, hun rol en relatie met de G4/gemeentelijke crisisorganisaties. Zie ook de netwerkkaart in bijlage 5. Voor een uitgebreide beschrijving van de nationale crisisbesluitvorming, zie ook het Nationaal Handboek Crisisbesluitvorming van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).[18)]

4.1.6.1 Nationaal Crisis Centrum (NCC)

Het NCC maakt onderdeel uit van de NCTV en beheert het stelsel van de (rijks)crisisstructuur en faciliteert informatiemanagement en crisiscommunicatie op rijksniveau. Het NCC ondersteunt de landelijke besluitvorming bij een (dreigende) crisis. De minister van Justitie en Veiligheid is coördinerend minister voor crisisbeheersing. Het NCC bestaat uit de Eenheid Crisiscoördinatie (ECR, 24/7 (inter)nationaal single point of contact) en de Eenheid Communicatie (ECO, verantwoordelijk voor rijksbrede risico- en crisiscommunicatie). Indien er een landelijke cybercrisis is, wordt gewerkt volgens het Nationaal Handboek Crisisbesluitvorming en specifiek volgens het NCP-Digitaal[19)].

Het is niet gebruikelijk dat (kleinere) gemeenten direct contact opnemen met het NCC. Als er een cybercrisis speelt in een kleine gemeente, kan dit een regionaal karakter krijgen. In dat geval neemt de veiligheidsregio contact op met het NCC. De vier grote gemeenten hebben doorgaans nauwer contact met het NCC en zullen in het geval van een cybercrisis eerder direct schakelen met het NCC via (in)formele lijnen. In het NCP-Digitaal staat wel vermeld dat, indien nodig, het NCC kan ondersteunen op het gebied van crisiscommunicatie.

4.1.6.2 Nationaal Cyber Security Centrum (NCSC)

Voor vitale aanbieders en aanbieders van essentiële diensten (AED's) is het NCSC op grond van de Wet beveiliging netwerk- en informatiesystemen (Wbni) het aangewezen Computer Security Incident Response Team (CSIRT[20)]). Aangewezen AED's hebben onder meer een meldplicht voor cyberincidenten bij het NCSC.

De belangrijkste taken van het NCSC zijn: reageren op incidenten die vrijwillig of verplicht worden gemeld; incidenten op nationaal niveau monitoren, aanbieders vroegtijdig waarschuwen en informatie over risico's en incidenten verspreiden; deelnemen aan het internationale netwerk van CSIRT's en op samenwerking gerichte contacten onderhouden met de private sector. Het NCSC activeert bij een crisis de ICT Response Board (IRB) die de nationale crisisteams adviseert op het gebied van cyber. Het NCSC is tevens nationaal contactpunt namens Nederland voor EU-lidstaten.

Het NCSC geeft aan dat zij in praktijk weinig betrokken zijn bij cyberincidenten in een gemeente tenzij het om meerdere gemeenten gaat en mogelijk een landelijke cybercrisis wordt. De G4 en lokale crisisorganisaties communiceren, als het gaat om cyberverstoringen binnen de interne gemeentelijke organisatie, in principe via de IBD. Het NCSC kan echter een melding van een incident door een organisatie die niet behoort tot vitale aanbieders of onderdelen van het Rijk in behandeling nemen. Zij kunnen dan ondersteuning bieden en advies geven over het betrekken van de juiste expertise.

18) NCTV (2016). *Nationaal Handboek Crisisbesluitvorming.*

19) NCSC (2020). *Nationaal Crisisplan Digitaal.*
20) Zie ook 4.1.6.9

Advisering omtrent de duiding van de oorzaak is een taak van het NCSC binnen het voor hen aangegeven werkgebied.

4.1.6.3 Informatiebeveiligingsdienst voor gemeenten (IBD)

De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger plan te tillen. De IBD is hét aanspreekpunt voor gemeenten in geval van een incident dat te maken heeft met informatiebeveiliging. De rol die het NCSC heeft voor de vitale sectoren heeft de IBD voor de gemeenten. Volgens landelijke afspraken zal de G4 in geval van een cybercrisis met een hoog risico contact opnemen met de IBD[21)].

De IBD levert onder meer 'integrale coördinatie en concrete ondersteuning op gemeente-specifieke aspecten in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging'. De IBD beschikt daarvoor over een computer security incident response team (CSIRT)-functie om zo preventie, detectie en coördinatie van informatiebeveiligingsincidenten binnen de gemeentelijke overheid mogelijk te maken.

De IBD monitort op algemene dreigingen die relevant zijn voor gemeenten en informeert gemeenten wanneer nodig met gericht advies om deze dreigingen tegen te gaan. Op basis van informatie van gemeenten stuurt de IBD dagelijks actuele kwetsbaarheidswaarschuwingen over de hardware, software en systemen die de gemeente in gebruik heeft. De IBD controleert waar mogelijk of IP-adressen, e-mailadressen en overige gegevens van gemeenten die voorkomen in datasets met gelekte gegevens of logbestanden van in beslag genomen servers.

De IBD werkt nauw samen met het NCSC en verkrijgt en verwerkt onder meer beveiligingsadviezen vanuit het NCSC specifiek voor de gemeentelijke sector. De IBD monitort met name op dreigingen die relevant zijn voor gemeenten en informeert gemeenten wanneer nodig met gericht advies om deze dreigingen tegen te gaan.

De IBD richt zich met name op interne crisisbeheersing van gemeenten (contact via CISO), maar kan ook benaderd worden voor externe crisisbeheersing voor gemeenten. Op dit moment is de lijn dat informatie vanuit de IBD via de CISO in het crisisteam wordt ingebracht.

21) Afspraak is niet formeel vastgelegd. Er is ook geen formele meldingsplicht. Beschreven informatie is op basis van de uitgevoerde interviews.

4.1.6.4 CISO

De CISO is een staffunctie binnen een organisatie die verantwoordelijk is voor de ontwikkeling en implementatie van informatiebeveiliging. De CISO is een belangrijk aanspreekpunt wanneer de organisatie waar deze persoon werkzaam is, wordt getroffen door een cyberverstoring. De CISO is in veel gevallen het eerste aanspreekpunt voor afstemming over het oplossen van de cybercrisis. Ook kan de CISO de impact van de digitale verstoring op de eigen organisatieprocessen duiden.

De CISO binnen het gemeentelijk domein houdt zich conform zijn/haar functieprofiel onder andere bezig met het coördineren van de reactie op ernstige informatiebeveiligings- of ICT-incidenten en het informeren van bestuur en management over de status van informatiebeveiliging en afhandeling van dergelijke incidenten.[22)] Deze coördinatie rol en adviserende taak richting het bestuur hebben betrekken op cyberincidenten die de gemeentelijke dienstverlening/systeem raken (scenario 1 en 2). In de praktijk wordt van CISO's vaak verwacht dat zij vanuit hun technische kennis en beveiligingsblik meedenken en bestuurlijk advies geven over de impact van een ICT-incident dat impact heeft op de gemeentelijke dienstverlening en aanpalende sectoren, waaronder de openbare orde en veiligheid. Vanuit deze rol kan het dus ook meerwaarde hebben een CISO aan te laten sluiten als adviseur bij bijvoorbeeld een ROT.

Een belangrijk aandachtspunt in het kader van informatiedeling is dat de aansluiting van de CISO bij de IBD kan plaatsvinden als vertrouwde contactpersoon (VCIB) of als algemeen contactpersoon (ACIB)[23)]. De IBD communiceert uitsluitend met de VCIB over vertrouwelijke beveiligingsincidenten. Een VCIB kan naast de CISO ook een andere functionaris zijn.

4.1.6.5 Politie

De politie is verantwoordelijk voor handhaving van de rechtsorde (dit omvat tevens de opsporing) en hulp aan hen die dat behoeven. Indien noodzakelijk kan de politie haar (crisis) organisatie opschalen bij incidenten met grote impact volgens het (N)SGBO-model: (Nationale) Staf Grootschalig Bijzonder Optreden. Op het niveau van de veiligheidsregio fungeert een SGBO als actiecentrum van de politie en richt zij zich op crisisbeheersing, gevolgbestrijding en het wegnemen van de bron van het incident. Voor de landelijke informatievoorziening en -inschatting, het contact en de coördinatie met de landelijke en

22) IBD (2020). *Handreiking functieprofiel Chief Information Security Officer.*
23) IBD. *Factsheet Verantwoordelijkheden van de VCIB.*

internationale partners als NCSC, INTERPOL en Europol kan een SGBO-ondersteuning krijgen van de Landelijke Eenheid (Dienst Landelijke Informatie Organisatie). De Nationale Politie is vertegenwoordigd in bijna alle ISAC's. Tevens is het mogelijk om een nationaal SGBO (NSGBO) op te starten, met als taak richting te geven of te sturen op de politieoperaties. Deze wordt via de reguliere bestuurlijke lijnen aangehaakt aan de nationale en regionale crisisstructuur. Het niveau van opschaling hangt af van de impact van de maatschappelijke ontwrichting, zowel qua ernst als regionale spreiding.

Het gezag over politie-inzet is in beginsel territoriaal georiënteerd (burgemeester, bij crisis opschalend via GRIP-model). Voor de opsporing na een strafbaar feit vallen de politie en ook de Koninklijke Marechaussee onder het bevoegd gezag van het OM. Bijzondere opsporingsbevoegdheden kunnen ingezet worden om eventuele verdachten van cybercrime te traceren, strafbare feiten te stoppen en criminele infrastructuren te ontmantelen. Dit kan leiden tot het verhinderen van de criminele activiteiten en/of het aanhouden van verdachten in binnen- of buitenland. Op die manier kan de dreiging en verstoring mogelijk worden weggenomen en controle over de situatie verkregen worden. Aanvankelijk zal onzekerheid bestaan over het type dader. Reden waarom vanaf het begin van een onderzoek de nadruk ook ligt op het beperken van schade en het identificeren en notificeren van (potentiele) slachtoffers en/of benadeelden (dit kan ook plaatsvinden op basis van de hulpverleningstaak).

4.1.6.6 Openbaar Ministerie (OM)

Het OM is bij een (dreigend) ICT-incident verantwoordelijk voor de strafrechtelijke handhaving van de rechtsorde. Dit betekent dat het OM:

- leiding geeft aan het opsporingsonderzoek naar de toedracht van de calamiteit of crisis
- de rechtsorde handhaaft door het laten aanhouden (en vervolgen) van burgers of rechtspersonen die zich schuldig maken aan het overtreden van wet- en regelgeving tijdens een calamiteit of crisis.

4.1.6.7 Inlichtingendiensten (AIVD, MIVD)

De Joint Sigint Cyber Unit (JSCU) is een gezamenlijk onderdeel van de AIVD en de MIVD. Deze unit biedt expertise en ondersteuning op het gebied van sigint (signals intelligence) en cyber en verschaft inlichtingendiensten toegang tot (dreigings) informatie uit technische bronnen.

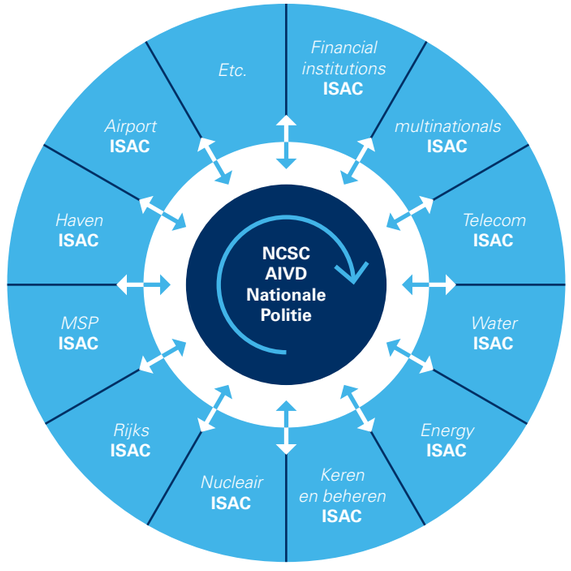
G4 en regionale crisisorganisaties schakelen in een crisissituatie in principe niet rechtstreeks met inlichtingendiensten, maar deze spelen wel een belangrijke rol bij detectie onder meer via het Nationaal Detectie Netwerk (NDN) en deelname Information Sharing and Analysis Centres (ISAC's). De gemeenten zijn nog niet aan het NDN gekoppeld. Deze wens is er wel vanuit de gemeenten. Inlichtingendiensten beschikken over eigen informatiebronnen die in de regel niet of zeer beperkt worden gedeeld. Als deze al gedeeld worden dan loopt dat via de NCTV.

4.1.6.8 Information Sharing and Analysis Centers (ISAC's)

Een ISAC is een sectoraal overleg over cybersecurity. Een ISAC voorziet in een vertrouwde omgeving met organisaties uit dezelfde sector waarin gevoelige en vertrouwelijke informatie over incidenten, dreigingen, kwetsbaarheden, maatregelen en leerpunten op het gebied van cybersecurity worden gedeeld.

De verschillende ISAC's hebben in principe geen actieve rol ten tijde van een cybercrisis Dit is meer de taak en rol van een CSIRT (zie hiernavolgend). De focus in een ISAC ligt meer op kennisdeling en informatie-uitwisseling. ISAC's vormen echter een belangrijk (kennis)netwerk van waaruit mogelijk expertise kan worden betrokken en waarin crisisrespons kan worden geëvalueerd.

Zie figuur 3 voor een overzicht van ISAC's die actief zijn in Nederland. Standaard is in elke ISAC een drietal verschillende publieke organisaties aangesloten: het NCSC, de AIVD en de Nationale Politie. Het is voor organisaties mogelijk om een ISAC te starten of aan te sluiten bij en ISAC in een bepaalde sector.



Figuur 3 Overzicht ISAC's Nederland. Bron: NCSC

4.1.6.9 Computer Security Incident Response Teams (CSIRT's) en Computer Emergency Response Teams (CERT's)

Een collectieve CSIRT[24] is een samenwerkingsvorm die kan ontstaan vanuit een reeds bestaande samenwerking, bijvoorbeeld een ISAC. In een CSIRT worden diensten voor meerdere organisaties uitgevoerd. In het algemeen zijn CSIRT's verantwoordelijk voor het voorkomen, isoleren en mitigeren van computer- en informatiebeveiligingsincidenten om de beschikbaarheid van diensten of informatiestromen te garanderen. Hiervoor zijn technische en niet-technische werkzaamheden nodig. Tijdens incidenten worden er handelingen verricht in systemen om het incident of voorval te isoleren of te mitigeren. In de nasleep van een incident draagt het CSIRT ook zorg voor de evaluatie om herhaling van het incident te voorkomen. Hiervoor is informatie uit systemen en personen (logbestanden, geautomatiseerde detectiemeldingen, meldinganalyse) vereist.[25] Collectieve CSIRT's fungeren als coördinator in de 'warme' fase, wanneer een incident of crisis bij een of meerdere deelnemende partijen speelt. De G4 (CISO's) en lokale crisisorganisaties kunnen direct schakelen met een CSIRT, zoals Z-CERT het response team voor de zorg.

24) CSIRT is de moderne benaming voor wat decennialang bekend stond als CERT. De benamingen worden in praktijk door elkaar gebruikt.
25) NCSC (2018) *Start een CSIRT: collectief samenwerken.*

4.1.6.10 Private CSIRT's en expertise

Externe deskundigen spelen een belangrijke rol bij cybergevolgbestrijding, in het bijzonder voor het leveren van specialistische kennis ten tijde van een crisis. Denk met name aan digitaal forensisch onderzoek en analyse. Private partijen leveren ook zogenaamde managed services zoals Security Operation Centers (SOC) en monitoring diensten voor detectie van dreigingen en kwetsbaarheden. Dergelijke monitoring is vergelijkbaar met dat van het Nationaal Detectie Netwerk, maar dan uitgebreider en veelal ook geavanceerder.

Externe partijen leveren ook vertrouwensdiensten zoals certificaten voor beveiligde websites. Tijdens de DigiNotar-crisis (2011) moesten veel organisatie met spoed hun certificaten vervangen waardoor er een enorme schaarste ontstond. Externe partijen kunnen ook een rol spelen bij preventie van mogelijke aanvallen of het beperken van de impact daarvan. Denk daarbij bijvoorbeeld aan het initiatief van nomoreransom.org. Een ander goed voorbeeld waar ondersteund bij kan worden is DDoS-mitigatie, waarbij legitiem internetverkeer wordt gescheiden van de aanval, waardoor (data)netwerken beschikbaar blijven.[26] De G4 en lokale crisisorganisaties zullen bij een crisis (maar ook in de koude fase) zeer waarschijnlijk een beroep doen op private partijen voor de hiervoor genoemde diensten.

Indien externe partijen worden ingezet voor forensisch onderzoek en analyse is het van groot belang dat het resultaat ook gebruikt kan worden door het OM bij eventuele vervolging. Om te voorkomen dat per casus aparte afspraken moeten worden gemaakt over de voorwaarden en eisen waaraan het onderzoek dan moet voldoen onderzoekt het OM of hierover niet vooraf afspraken gemaakt kunnen worden met partijen. Een optie zou kunnen zijn om dit bijvoorbeeld met certificering te formaliseren. Op deze manier kan marktcapaciteit maximaal worden benut op een moment dat de overheidspartijen piekbelasting ervaren vanwege een grote cyberaanval. Ook voor het monitoren van dreigingen en kwetsbaarheden zouden bijvoorbeeld afspraken gemaakt kunnen worden met externe deskundigen over de inzet van hun capaciteit om te monitoren op nieuwe aanvallen binnen het maatschappelijk domein. Dit sluit aan bij het WRR-advies in haar nieuwste rapport 'Voorbereiden op digitale ontwrichting, (09-09-2019)' voor een wettelijke bevoegdheid van digitale hulptroepen.

4.1.6.11 Overige partijen

26) Zie bijlage 2 voor een uitleg van dit aanvalstype.

Er zijn nog andere partijen in het cybersecurity speelveld die geen directe rol spelen in de crisisgevolgbestrijding, maar mogelijk indirect betrokken zijn via (keten)partners van de gemeente of bijvoorbeeld in verband met de toezichthoudende rol.

- Cyber Security Raad (CSR), adviesorgaan van het kabinet.
- Digital Trust Center (DTC), programma van het Ministerie van Economische Zaken en Klimaat gericht op de cyberweerbaarheid van het bedrijfsleven.
- Toezichthouders zoals Autoriteit Consument en Markt (ACM) en Autoriteit Persoonsgegevens (AP) relevant met het oog op diverse meldplichten.

In bijlage 5 worden alle in deze pararaaf genoemde partijen in een netwerkkaart getoond.

4.2 Kritische crisisbeheersingsprocessen

Los van welk crisisteam de crisis aanpakt is er een aantal kritische crisisbeheersingsprocessen te onderscheiden dat altijd goed geregeld moet zijn voor een goede afhandeling van een (cyber) crisis. Het uitgangspunt is daarbij steeds dat de processen voor 'traditionele' crises goed ingericht zijn en alleen de specifieke aandachtspunten vanuit de cybergevolgbestrijding worden benoemd.

4.2.1 Melding & alarmering

Bij een (cyber)crisis is het van groot belang dat betrokken partijen zo snel als mogelijk op de hoogte raken van de situatie. Dit geldt zowel voor crises die door opzettelijk handelen zijn veroorzaakt als voor andere verstoringen. Vanwege de snelheid waarmee een cybercrisis zich kan verspreiden, kan het aantal betrokken partijen snel veranderen. Daarom is het belangrijk om heel snel de partijen te informeren die als informatieknooppunt fungeren zoals de IBD en het NCSC.

Melding: Crisisbeheersing start pas als de getroffen organisatie weet dat er een crisis is. Er moet een melding plaatsvinden bij de partij die de crisis kan aanpakken. Dat kan een interne (cyber)crisisorganisatie zijn, maar ook een externe partij die daarbij ondersteunt. Naast de reguliere meldingsprocessen gelden de volgende aandachtspunten in het geval van een cybercrisis. Deze aandachtspunten verschillen per domein dat geraakt wordt.

Indien een interne gemeentelijke organisatie is geraakt (zowel ICT-domein als gemeentelijke dienstverlening):

- **Aandachtspunt 1:** draag zorg voor een intern meldingsprotocol en opvolging zodat werknemers snel melden en weten waar ze moeten melden en dat de interne organisatie snel opvolgt met acties en delen van informatie. Beschrijf ook het proces van melding in geval het normale meldingskanaal niet meer beschikbaar is.
- **Aandachtspunt 2:** draag zorg voor snelle informatiedeling met IBD zodat deze eventueel kunnen adviseren en ook overzicht houden over eventuele verdere verspreiding. Neem dit op in protocol.
- **Aandachtspunt 3:** tenzij duidelijk is dat het geen bewuste actie is gelijk de politie informeren zodat deze geen tijd verliest voor mogelijke aanpak van de bron. Neem dit op in het protocol.

Indien de maatschappij is geraakt:

- **Aandachtspunt 1:** Inventariseer voor jouw specifieke gemeente/regio welke organisaties cruciaal zijn voor maatschappelijke continuïteit. Maak met deze organisaties afspraken over het delen van informatie omtrent cyberincidenten/crisis. Doe dit vanuit het perspectief dat de overheid gevolgbestrijding moet organiseren bij uitval van de organisatie en dat er mogelijk escalatierisico is. Indien de organisatie aangesloten is bij een SOC, dan kunnen ze het daar melden. Het SOC zet deze melding vervolgens door aan ketenpartners in het ISAC/CERT/CSIRT waarin zij deelnemen.
- **Aandachtspunt 2:** maak afspraken over (informatie met betrekking tot voortgang van) de aanpak van het cyberincident. De politie/OM is hier goed voor gepositioneerd, zowel vanuit haar rol in de ISACs als in het kader van afspraken met mogelijke externe deskundigen omtrent forensisch onderzoek en analyse.

Indien vitale infrastructuur is geraakt:

- **Aandachtspunt 1:** in het geval dat een organisatie in een vitale sector of een AED getroffen wordt door een cyberverstoring, heeft deze organisatie in het kader van de Wbni een meldplicht bij het NCSC. Organisaties in vitale sectoren en AED's zijn verplicht om ernstige digitale veiligheidsincidenten te melden bij het NCSC, die als CSIRT voor vitale aanbieders en AED's fungeert. De gemeenten zien graag dat deze meldingen naar de betreffende gemeente worden doorgezet, eventueel via de IBD. In artikel 20 van de Wbni is vastgelegd dat het NCSC vertrouwelijke informatie die herleidbaar is tot een aanbieder in beginsel niet mag delen met derden. Delen is alleen toegestaan wanneer dat dienstig is aan het bevorderen van maatregelen ter voorkoming of beperking van een verstoring van het maatschappelijk verkeer, met CSIRT's, onder de Wbni aangewezen computercrisisteams en inlichtingen- en veiligheidsdiensten. Ook is het toegestaan om informatie te delen wanneer de betrokken aanbieder daarvoor toestemming geeft. Gemeenten zijn geen doelgroep van het NCSC. Het NCSC zal de gemeenten daarom niet zelf informeren. Wel hebben gemeenten een eigen CERT, de IBD. De IBD is een aangewezen computercrisisdienst. Het NCSC kan dus wel informatie met de IBD delen, mocht die informatie nuttig voor ze zijn.

- **Aandachtspunt 2:** maak afspraken via IBD met NCSC over informatie-uitwisseling naar de crisisorganisatie waar betreffende vitale infrastructuur gelegen is. Dit punt is relevant voor zowel de preparatieve fase als voor de responsfase. Zoals al eerder gezegd, blijft lokale/regionale gezag verantwoordelijk voor crisisbeheersing in dat gebied naast eventueel optreden van de landelijke overheid.

Alarmering: Zolang er geen overtuiging is dat er geen opzet in het spel is, is alarmering van politie een belangrijke stap die snel gezet moet worden zodat deze zich op de opsporing van de (mogelijke) actor kan richten. Omdat bij een cybercrisis extra en andere expertise nodig is, zijn er voor alarmering enkele aandachtspunten:

- **Aandachtspunt 1:** alarmeer het crisisteam dat verantwoordelijk is voor het herstel van bedrijfsprocessen.

- **Aandachtspunt 2:** indien het een verstoring van de eigen processen betreft: alarmeer de partij waarmee afspraken zijn gemaakt om te helpen de cyberverstoring op te lossen. Het is raadzaam om als gemeente een partnerschap aan te gaan met externe deskundigen die de middelen hebben om een cyberverstoring op te lossen waarbij intern vooraf afspraken zijn gemaakt over de financiering. Het kan raadzaam zijn hiervoor een 'retainer' af te sluiten met een leverancier. Op het moment dat een melding van een cyberverstoring binnenkomt, kunnen deze deskundigen van vaak private partijen direct gealarmeerd worden.

- **Aandachtspunt 3:** direct de politie alarmeren in verband met starten opsporingsproces.

- **Aandachtspunt 4:** alarmeer ook bij cybercrises die de gemeentelijke organisatie nog niet getroffen hebben: alarmeer intern bij de gemeente deskundigheid om het risico voor de eigen bedrijfsvoering in kaart te brengen.

4.2.2 Opschaling (en afschaling)

Na melding en alarmering van de juiste betrokken partijen, is het zaak om te bepalen of en hoe opschaling nodig is naar de crisisorganisatie. Het uitgangspunt is dat ook bij cybercrises wordt aangesloten bij de bestaande crisisstructuren en opschalingsniveaus. Hieronder wordt aangegeven welke opschaling logischerwijs bij welk scenario past.

Opschalingstructuur	Type cybercrisis	Toelichting en aandachtspunten opschaling
Gemeentelijk calamiteitenteam	Indien gemeente zelf geraakt is.	In het geval van een cyberverstoring binnen de gemeentelijke organisatie, vindt opschaling plaats op basis van het interne continuïteitsplan van de gemeente. Iedere gemeente heeft zelf vastgesteld hoe dit wordt vormgegeven. In de gemeente Den Haag kan bijvoorbeeld worden opgeschaald naar respectievelijk een Cluster calamiteitenteam (IDC/A) en Dienst calamiteitenteam (IDC). Indien er sprake is van opzet zal de gemeente aangifte doen. De gemeente is verder verantwoordelijk voor het weer op orde brengen van (de dienstverlening van) haar eigen systemen en publiekscommunicatie over de dienstverlening.
Driehoeksoverleg	Indien opzettelijkheid niet uit te sluiten is.	Indien er een afweging moet worden gemaakt over de inzet van extra opsporingsmiddelen wordt de driehoek bij elkaar geroepen. Dit ter afweging van politie en OM.
Gemeentelijk crisisteam	Indien crisis maatschappelijke effecten heeft in beleidsdomein gemeente.	Een cybercrises met effect op de samenleving, maar zich afspelend bij een andere partij en (nog) geen effecten op fysieke veiligheid/ openbare orde. Bij zo'n soort scenario kan zowel op tactisch als strategisch niveau binnen de gemeente een crisisteam worden ingericht. **Aandachtspunt 1:** Indien de cybercrisis zich buiten de gemeentelijke organisatie bevindt of uitstrekt, maar (nog) geen effecten heeft in de maatschappelijke omgeving, is er geen bestaande structuur om de crisis te managen. **Aandachtspunt 2:** Het is van belang dat inzichtelijk is welke informatie van welke partijen nodig is.
GRIP-structuur	Indien sprake is van maatschappelijke verstoring.	Indien de cyberverstoring effecten heeft (of dreigt te hebben) op de maatschappelijk omgeving wordt opgeschaald volgens de GRIP-structuur om met de hulpdiensten de effecten te managen. Zoals eerder gesteld, zal dit een opschaling naar GRIP 2 of hoger zijn vanwege de cyberspecifieke problematiek die in het ROT/BT wordt besproken. Bij een dreiging kan een voorbereidend ROT bij elkaar komen om scenario's uit te werken.
Nationale crisisbeheersingsstructuur	Indien vitale infrastructuur is geraakt of (een deel van) Nederland treft.	Indien de cyberverstoring bovenregionale impact heeft of de vitale infrastructuur raakt wordt opgeschaald via het Nationaal Handboek Crisisbesluitvorming en het NCP-Digitaal.

Tabel 2 Toelichting en aandachtspunten per opschalingsstructuur en type cybercrisis

Opschalingscriteria

Bij cybercrises wordt indien mogelijk vastgehouden aan de bestaande opschalingscriteria voor opschaling naar de interne gemeentelijke calamiteitenorganisatie, de driehoek of de GRIP-structuur. Deze criteria zijn te vinden in respectievelijk de continuïteitsplannen van de gemeenten en de regionale crisisplannen van de veiligheidsregio's.

De Cyber-Crisis-Cirkel (figuur 2) is bedoeld om tot een eerste duiding van het cyberincident te komen. Hieruit volgt onder andere ook advies voor opschaling. Indien de waarde niet bekend is, is het aan het team in hoeverre deze onduidelijkheid meeweegt in de inschatting van de zwaarte van het scenario.

Denk daarbij aan:

- maatschappelijke impact middel of groot; overweeg GRIP 2 of hoger en gemeentelijk crisisteam.

- maatschappelijke omgeving geraakt; overweeg opschalen naar GRIP 2 of hoger en gemeentelijk crisisteam.

- eigen gemeente geraakt (i.c.m. maatschappelijke omgeving); overweeg GRIP 2/3 en gemeentelijk crisisteam.

- eigen regio geraakt (i.c.m. maatschappelijke omgeving); overweeg GRIP 4.

- oorzaak opzettelijk; overweeg om op te opschalen naar de driehoek indien meer opsporingsbevoegdheden nodig zijn.

- crisis in een niet-maatschappelijke omgeving; binnen gemeente, ketengevoelig, impact middel, overweeg opschaling gemeentelijk crisisteam.

- vitale infrastructuur geraakt; overweeg opschalen NCC.

- Nederland of internationaal geraakt; overweeg opschalen NCC.

- geraakt domein eigen ICT; overweeg opschalen intern calamiteitenteam.

4.2.3 Leiding en coördinatie

Op het moment dat is opgeschaald naar de crisisorganisatie, is het van belang dat voor iedereen helder is hoe de rollen en taken verdeeld zijn en door wie waarover besluiten moeten worden genomen.

Voor de bronbestrijding geldt dat de getroffen organisatie in principe zelf verantwoordelijk is voor het oplossen van digitale verstoring. Bij een crisis binnen het gemeentelijk ICT-systeem is dit de gemeentelijke calamiteitenorganisatie onder voorzitterschap van de gemeentesecretaris.

Voor de effectbestrijding van een cybercrisis is hiervoor vastgesteld dat dit binnen de GRIP-structuur kan; dan is namelijk leiding en coördinatie helder vormgegeven. Ook kan het zijn dat de problematiek in de driehoek wordt besproken. Hierbij hebben burgemeester en officier van justitie beiden het gezag en voert de politie de gezamenlijk genomen besluiten uit.

Zoals eerder geconstateerd bestaat de mogelijkheid van een serieuze cybercrisis die (nog) geen directe effecten heeft op de maatschappelijke omgeving. In deze gevallen wordt het gemeentelijk crisisteam bij elkaar geroepen. Dit staat onder leiding van de gemeentesecretaris.

Op basis hiervan identificeren we een aantal aandachtspunten.

- **Aandachtspunt 1:** identificeer vooraf welke inhoudelijke adviseurs in het ROT/BT bij cybercrises aanwezig moeten zijn en maak hierover afspraken.

- **Aandachtspunt 2:** leidt de Operationeel Leiders en informatiemanagers verder op om ook op deze beleidsterreinen heldere besluitvorming te faciliteren. Versterk in algemene zin de cyberkennis bij crisisteams om impact en maatregelen voldoende te kunnen duiden.

- **Aandachtspunt 3:** omdat men van tevoren het incidentverloop niet weet is het belangrijk om vanuit verschillende expertisegebieden (tactiek, intel en digitaal) het probleem te analyseren. Daarbij is het belangrijk om partijen te betrekken die de consequenties van een digitale verstoring begrijpen en de vertaling naar maatschappelijke impact kunnen geven.

Sleutelbesluiten

Enkele bestuurlijke dilemma's die tijdens de oordeelsvorming aan bod kunnen komen zijn in de volgende tabel samengevat.

Thema's	Dilemma
Maatschappelijke impact en stakeholdermanagement	Welke rol heb je als bestuurder richting maatschappelijke partijen waar de oorzaak van de verstoring ligt, terwijl het openbaar bestuur de maatschappelijk impact moet managen?
Dreiging van escalatie en duiding en communicatie	Cyberincidenten kunnen razendsnel escaleren van dreiging naar crisis. Tegelijkertijd kan een dreiging ook een dreiging blijven. Communiceer je over die dreiging of niet?
Techniek en maatschappij	Welke onderdelen van een systeem worden geïsoleerd of uitgeschakeld terwijl ze nog niet geraakt zijn, maar die mogelijk wel geraakt zouden kunnen worden?
Betrouwbare overheid	Wie communiceert er over de crisis en wat is de belangrijkste boodschap? Op welke manier wordt communicatie afgestemd met de direct getroffen organisatie en op welke manier wordt afgestemd met het NKC?
Ketenbetrouwbaarheid	Op welk moment, door wie en wanneer kan worden besloten om systemen weer op te starten zonder 100% garantie dat de keten of het systeem veilig is?
Continuïteit crisisbeheersing (lokaal, regionaal, landelijk)	I. Rolverdeling lokaal bestuur versus driehoek versus veiligheidsregio. II. Rolverdeling tussen lokaal/regionaal versus landelijk.
Continuïteit dienstverlening	Duur van monitoring van het systeem ten opzichte van vrijgeven van het systeem. Hoe langer je monitort, hoe kleiner de kans op infectie maar hoe hoger de kosten van de verstoring.
Opsporing en vervolging en continuïteit dienstverlening	Vanuit algemeen belang is het onwenselijk om te betalen. Indien opsporing realistisch is zou hier nadruk op moeten liggen. Hiermee wordt het criminele verdienmodel verstoort. Tegelijkertijd ligt er ook een maatschappelijke verantwoordelijkheid bij het openbaar bestuur voor de dienstverlening die het levert.

Tabel 3 Strategische/bestuurlijke dilemma's

Vanuit de hiervoor genoemde dilemma's kunnen enkele sleutelbesluiten worden geïdentificeerd. Hierbij kan onderscheid gemaakt worden tussen inhoudelijke besluiten en procesbesluiten. Inhoudelijke besluiten zijn gericht op het effect van de crisisbeheersing. Procesbesluiten zorgen ervoor dat de crisisbeheersing niet hapert.

Mogelijk inhoudelijke besluiten:

- Bij ransomware: wel of niet betalen van het losgeld (kan onder andere effect en effectduur beïnvloeden).
- Inhuur: inschakelen forensische experts en digitale experts van buiten (kostenpost, capaciteit beperkt).
- Vrijgeven systeem: duur van monitoring van het systeem na infectie ten opzichte van het vrijgeven van het systeem. Dit speelt niet als de organisatie 24-uurs monitoring al heeft ingeregeld via SOC-SIEM.
- Uitschakelen (nog niet getroffen) systemen: uitschakelen van systemen en/of applicaties waardoor bepaalde bedrijfsprocessen stilvallen met als doel isolatie, maar met als gevolg onduidelijke keteneffecten (het uitschakelen van bijvoorbeeld al het mailverkeer van een organisatie kan consequenties hebben voor lopende onderhandelingen met leveranciers of afnemers binnen het normale bedrijfsproces).
- Voortgang dienstverlening: dienstverlening vanuit nog niet getroffen systemen stilleggen.
- Crisiscommunicatie: communiceren over (dreiging van) aanval of escalatie.

Mogelijke proces besluiten:

- Op- en afschaling: wordt de crisis door het meest effectieve team met de juiste bevoegdheid bestreden?
- Aflossing: zorg dat bij langer durende crises het team wordt afgelost en draag zorg voor een goede overdracht.
- Liaisons: naar welke partijen of teams gaat een liaison/ van welke partijen of teams vragen we liaisons.
- Informeren stakeholders: welke bestuurders en ketenpartners willen/moeten dit weten en wie informeert ze.

4.2.4 Informatiemanagement

Tijdens een crisis is het van groot belang om in alle betrokken teams een eenduidig beeld te hebben van de situatie en de uitgezette acties. Hiervoor wordt het begrip 'netcentrisch werken' gebruikt. Kort gezegd is het de bedoeling dat dezelfde informatie over de crisis op hetzelfde moment zichtbaar is in elk betrokken team.

Binnen GRIP-opschaling is dit voor traditionele crises in de veiligheidsregio's vormgegeven en zijn de processen van de hulpverleningsdiensten hierop aangesloten. De veiligheidsregio gebruikt het LCMS als systeem om netcentrisch te werken.[27] Ook de watersector en geneeskundige sector werken op deze manier. De Driehoek en gemeentelijke calamiteitenteams worden niet op deze manier ondersteund. Binnen de G4 wordt verschillend gedacht over het inzetten van het netcentrisch werken van de veiligheidsregio buiten de GRIP-opschaling. Voor het crisisbeheersingsproces heeft het meerwaarde om het informatiemanagement zo professioneel mogelijk te organiseren en gebruik te maken van bestaande structuren en processen.

Bij een cybercrisis kan de bron liggen bij een partij en een sector waarmee (nog) geen informatie- uitwisselingsafspraken zijn gemaakt. Daarmee is de eerste prioriteit voor de informatiemanager niet alleen het maken van een beeld op basis van beschikbare informatie, maar meer nog een stakeholderanalyse van partijen die bevraagd moeten worden op informatie. Uiteraard verdient het de voorkeur dat met de relevante organisaties hier vooraf afspraken over worden gemaakt op basis van een analyse van de veiligheidsregio.

Bovendien is het raadzaam om een liaison van de partij die is geraakt door de cyberverstoring uit te nodigen voor het crisisoverleg. Van belang is hierbij om specifiek die persoon uit te nodigen die toelichting kan geven over de cyberverstoring (en de technische duiding daarvan). Indien er meerdere (overheids) crisisteams actief zijn is het raadzaam onderling af te stemmen waar deze expert de meeste meerwaarde heeft.

Het is de verwachting dat de drempel om ook informatie te delen vanuit de betreffende organisatie lager wordt vanwege de GRIP-opschaling door de overheid. Dit ligt ingewikkelder voor landelijk of internationaal opererende partijen. Bij deze partijen hebben de lokale vestigingen vaak geen zeggenschap over het cybercrisismanagement en de informatie-uitwisseling naar buiten. Dit heeft mede te maken met soms grote commerciële belangen. De burgemeester en/of het OM kunnen medewerking vorderen indien het algemeen belang dit vereist.

Het is niet uitgesloten dat deze partijen wel informatie willen delen met landelijke gesprekspartners zoals NCC of het NCSC. Het is de uitdaging om deze informatiedeling dienend te laten zijn aan de lokale/regionale crisisbeheersingsorganisatie. Hierover zou het veiligheidsberaad afspraken kunnen maken met het Rijk.

Indien de cybercrisis van dien aard is dat de landelijke crisisbeheersingsstructuur in werking treedt, dan zal een nationaal beeld worden opgesteld door het NCC. De gemeentelijke crisisbeheersingsorganisatie sluit hier dan op aan via het LOCC.

Een laatste punt van aandacht bij informatiemanagement op dit thema is de taal. De woorden die worden gebruikt om over dreigingen, aanvallen en oplossingen te spreken, zijn niet voor iedereen in de crisisbeheersing direct betekenisvol en kunnen onnodig verwarring veroorzaken. Dit is een van de redenen dat in deze handreiking relatief veel achtergrondinformatie is opgenomen en dat een aantal termen uitvoeriger wordt uitgelegd. Om te begrijpen wat het probleem is, wat de consequenties zijn en wat de oplossing betekent, is het belangrijk dat betrokkenen minimaal een basiskennis cybersecurity bezitten. Voor informatiemanagers, crisiscommunicatieadviseurs en operationeel leiders zou dit nog een niveau dieper mogen zijn omdat deze functionarissen de betreffende informatie moeten vertalen in adviezen en besluiten voor anderen. Tegelijkertijd vraagt dit van de partij die de cyberinformatie zal duiden in het crisisteam aandacht voor het vertellen van het verhaal in begrijpelijke termen voor niet-specialisten.

4.2.5 Crisiscommunicatie

Tijdens een (cyber)crisis is het van belang om de medewerkers, media, het algemene publiek en andere belanghebbenden te informeren over de crisissituatie. Als belangrijkste uitgangspunt geldt dat de algemene aandachtspunten van (de organisatie van) crisiscommunicatie ook gelden bij een cybercrisis. Een cybercrisis brengt daarnaast ook (nieuwe) uitdagingen met zich mee ook op het gebied van crisiscommunicatie.

In het NCP-Digitaal staan de richtlijnen op nationaal niveau voor crisiscommunicatie bij digitale verstoringen. Daarnaast biedt het Instituut Fysieke Veiligheid de factsheet Crisiscommunicatie tips voor incidenten met een

27) IFV. *Netcentrisch Werken.*

cybercomponent (digitale verstoring).[28)]
Hierin staat de rolverdeling bij crisiscommunicatie beschreven tussen het NCSC, NCTV/NCC, veiligheidsregio, gemeente/burgemeester, de Informatie Beveiligingsdienst, politie, Openbaar Ministerie, Vitale partners en Autoriteit Persoonsgegevens. Ook wordt ingegaan op doelgroepen, communicatiepartners, crisiscommunicatiemiddelen, doelstellingen voor crisiscommunicatie, handelingsperspectieven en interessante casus en links.

Dit hoofdstuk benoemt enkele aandachtspunten aanvullend op hiervoor genoemde NCP-digitaal en factsheet.

Rolverdeling

Binnen het (verlengd) lokaal bestuur wordt tijdens een cyberincident of cybercrisis de geldende opschalingsstructuren voor crisiscommunicatie gevolgd. De burgemeester van de getroffen gemeente of voorzitter van de veiligheidsregio is op lokaal/regionaal niveau verantwoordelijk voor informatievoorziening aan burgers over rampen en crises en over de maatregelen die de overheid heeft getroffen ter voorkomen en bestrijding ervan. Daartoe behoort de communicatie over de aanpak van de effecten van de verstoring op de openbare orde, veiligheid en maatschappij. Wanneer is opgeschaald binnen de GRIP-structuur vindt nauwe afstemming plaats tussen de getroffen gemeente en veiligheidsregio. Wanneer de nationale crisisorganisatie is geactiveerd, coördineert het Nationaal Kernteam Crisiscommunicatie (NKC) de pers- en publieksvoorlichting vanuit de rijksoverheid.

Aandachtspunten

- Er is afstemming nodig over wie in welke situatie regie heeft op monitoring, ontwikkelen van omgevingsanalyses, en op het communiceren zelf. Effecten van een cybercrises kennen vaak geen duidelijke fysiek grenzen en er is meestal geen duidelijke 'bron' waardoor al snel meerdere partijen zouden willen/moeten communiceren zonder dat ze zich binnen bestaande afspraken met elkaar hierover verhouden. De plek waar alle crisiscommunicatielijnen bij elkaar komen is het NKC. In het NCP-Digitaal staat 'Indien nodig ondersteunt de Eenheid Communicatie van het NCC (onderdeel NKC) het lokaal of regionaal bevoegd gezag met adviezen, middelen en een netwerk van ervaringsdeskundigen'. Het lijkt voorstelbaar dat bij een cybercrisis gebruik wordt gemaakt van deze mogelijkheid. Vanuit het NCC kan dan geadviseerd worden over het communicatieproces bij betreffende crisis (waar deze niet past binnen de bestaande afspraken) en ondersteunt worden met capaciteit. Indien nationale opschaling volgt, is de stap naar coördinatie vanuit het NKC relatief klein.

- De IBD kan de gemeente ondersteunen bij woordvoering en communicatieadvies indien de gemeente zelf getroffen is en is hiervoor 24/7 bereikbaar. De VNG heeft op haar website verschillende documenten ter beschikking gesteld waaronder de factsheet Incidentcoördinatie Crisiswoordvoering. Op landelijk niveau zijn het CSIRT DSP, NCSC en NCTV-NCC betrokken voor de duiding en maatregelen op technisch operationeel gebied. De communicatiecapaciteit van deze partijen is beperkt.

- Investeer in stakeholdermanagement. Regelmatig heb je als lokale overheid in de afhandeling van een cybercrisis te maken met private organisaties die getroffen zijn. Afstemming over crisiscommunicatie met deze organisaties is een extra uitdaging aangezien deze vaak (nog) niet in het directe netwerk zitten en er sprake kan zijn van conflicterende belangen.

Inhoudelijke aspecten crisiscommunicatie

Ook voor crisiscommunicatie over cybercrisis gelden de gebruikelijke uitgangspunten met betrekking tot de drie kerndoelen van crisiscommunicatie: duiden, informatievoorziening en bieden van een handelingsperspectief. Cyberincidenten zijn op bepaalde elementen specifiek waarvoor een aantal aandachtspunten kunnen worden geformuleerd:

- Duiding van een cyberincident kent specifieke elementen. Ook voor de duiding ten behoeve van het bepalen van de communicatiestrategie kan gebruik worden gemaakt van de Cyber-Crisis-Cirkel waarmee de zwaarte van de verstoring en effecten in kaart gebracht kunnen worden. De uitkomsten corresponderen ook met de vijf illustratieve scenario's die zijn opgenomen in deze handreiking.

- Veel crisisprofessionals, communicatiedeskundigen en bestuurders staan voor de opgave de complexiteit van crises in begrijpelijke termen te communiceren om zo betrokkenen begrijpelijke informatie te bieden zodat deze effectiever kunnen handelen. Enkele tips hiervoor zijn:
  - Betrek een communicatie adviseur met digitale expertise bij het opstellen van de communicatiestrategie en vertaling naar communicatieberichten (eventueel kan hiervoor ondersteuning worden gezocht bij: CISO's, IBD, NCSC).
  - Bijlagen 1 tot en met 3 van deze handreiking voorzien in een toelichting op veel voorkomende oorzaken en impact van cybercrises, specifieke aspecten van een (dreigende) cybercrisis en een overzicht van mogelijke aanvalstechnieken.
  - Cybersecurity woordenboek van Cyberveilig Nederland maakt lastige terminologie begrijpelijk.[29)]
  - Borg kennisniveau crisiscommunicatieprofessionals op het gebied van cybergevolgbestrijding door hen bij te scholen.

- Houd rekening bij communicatie met het beperkte kennisniveau van burgers op het gebied van cybercrises.[30)] Investeer in cyberkennis bij inwoners en bijbehorende risicocommunicatie om de kans op cyberincidenten te verkleinen.

- Bereid alternatieve communicatiemiddelen voor die ook inzetbaar zijn als de eigen organisatie wordt getroffen door een cyberincident waardoor (intern en extern) communiceren wordt bemoeilijkt. Crisisteams maken vaak gebruik van whatsapp. Een veilig alternatief is bijvoorbeeld Signal.

- Bereid communicatieproducten voor zoals woordvoeringslijnen, Q&A's en stem deze af met betrokken partijen.

- Ontwikkel een aantal basisscenario's voor communicatie voor verschillende typen cyberincidenten. Breng hierbinnen de verschillende communicatiepartners in beeld en maak afspraken over wie, wanneer en waarover communiceert. Bijvoorbeeld welke afspraken gelden wanneer een ziekenhuis is getroffen? Of als de gemeentelijke organisatie zelf is getroffen? Gebruik kan worden gemaakt van de scenario's ter illustratie (zie paragraaf 3.3).

28) IFV (2019). *Crisiscommunicatietips voor incidenten met een cybercomponent (digitale verstoring).*

29) Cyberveilig Nederland (2019). *Cybersecurity Woordenboek. Van cybersecurity naar Nederlands.*

30) Het algemene kennisniveau wordt wel steeds hoger naarmate er meer incidenten in de media zijn en er toegankelijke publicaties verschijnen zoals Huib Modderkolk, het is oorlog en niemand die het ziet, Podium, 2019.

4.3 Capaciteitsvraagstukken

Een van de grote uitdagingen bij een cybercrisis is het vinden van de (forensische) expertise om onderzoek te doen en het probleem op te lossen.

Het lijkt verstandig dat de G4-gemeenten of de veiligheidsregio's met deze partijen in gesprek gaan over beschikbare ondersteuning en onder welke omstandigheden die beschikbaar is. De IBD kan daar mogelijk ook een rol in vervullen. OM en politie verzorgen de digitale ondersteuning gericht op het opsporingsproces.

Het is het onderzoeken waard of ook op het gebied van cybergevolgbestrijding burgerparticipatie een zinvolle optie is. Door middel van afspraken vooraf met betrekking tot monitoringscapaciteit van externe deskundigen in geval van een crisis, vooraf gestelde eisen aan partijen voor forensisch onderzoek en analyse en het instellen van bijvoorbeeld een meldpunt cyberhulpverlening door burgers kan de overheid optimaal gebruik maken van de in de samenleving aanwezige kennis. Op het gebied van bijvoorbeeld reanimatie (hartslag.nu), dijkwachten, watervoorziening bij natuurbrand en andere hulpverlening is het geaccepteerd dat burgers assisteren bij het aanpakken van een crisis.

4.4 Uitdagingen in de nafase

Het aspect cyber brengt verschillende uitdagingen met zich mee. Zo zal het lastig te duiden zijn wanneer een cyberverstoring echt over is; het is wellicht niet helder of alles weer ‘schoon’ is en daarnaast is het lastig te bepalen of en wanneer systemen weer naar behoren en verantwoord werken. Dit maakt het in de nafase extra ingewikkeld om te toetsen of alle problemen (en bijbehorende effecten) verholpen zijn en welke kosten gemaakt zijn en te verhalen zijn. Wat we zien is dat een goed communicatietraject naar medewerkers en getroffenen vanuit de organisatie tijdens de crisis het makkelijker maakt om in de nafase problemen op te lossen. Het is voor iedereen helder bij wie ze zich kunnen melden en er is dan ook vertrouwen in de organisatie om de problemen op te lossen.[31)]

Enkele belangrijke aandachtspunten om in de nafase rekening mee te houden zijn:

- Investeer per gemeente in het ontwikkelen en up-to-date houden van een continuïteitsplan. In dit plan staat beschreven wat nodig is om de continuïteit van de gemeentelijke processen te borgen. Zorg daarbij dat het continuïteitsplan en de crisisplannen zo goed als mogelijk op elkaar aansluiten.

- Draag zorg voor het evalueren van zowel de (technische) aanpak van de verstoring als de procesmatige aanpak van crisismanagement (kritische processen van crisismanagement).

- Borg de leerpunten in planvorming (crisisplannen, handreiking en continuïteitsplannen).

- Beoefen jaarlijks een cyberscenario binnen de organisatie op teamniveau. Dilemmasessies en brown paper sessies zijn daarnaast goede instrumenten om inzicht te krijgen in de focus van de verschillende teams die actief zijn bij een cyberscenario. Gezamenlijk oefenen van teams heeft vooral pas zin als de teams zelf goed zicht hebben in rol, taken en verantwoordelijkheden en als team getraind zijn.

31) Zie bijvoorbeeld de reactie van studenten en medewerkers na de hack van de UM in december 2019 in Volkskrant (2020). Universiteit Maastricht krabbelt voorzichtig op na cyberaanval.

Bijlagen

Bijlagen behorende bij de Handreiking Cybergevolgbestrijding G4

Bijlage 1 Cybercrises: oorzaken en impact

Oorzaken	Toelichting	Impact
Cyberspionage	Cyberaanvallen door statelijke actoren gericht op het verkrijgen van waardevolle informatie en verzamelen van inlichtingen. Aanvallen zijn gericht op computers en complete netwerken, waaronder in toenemende mate social media. De doelen lopen uiteen: politiek, ondermijnend en zelfs sabotage (zie hiernavolgend). *Voorbeeld: de vermeende Russische inmenging met verkiezingen, in het bijzonder de verkiezingen in de Verenigde Staten van 2016.32) Of de spionage bij ASML waardoor ASML belangrijk concurrentievoordeel verloor.*[33]	Cyberspionage blijft veelal lang onopgemerkt en leidt als zodanig niet direct tot een crisis, maar kan wel grote impact hebben en escaleren: onrust, politieke spanning.
Cybersabotage	Cyberaanvallen gericht op verstoring of zelfs sabotage van de vitale infrastructuur, zoals de energievoorziening. Bij dit crisistype wordt veelal zeer destructieve malware (kwaadaardige software) verspreid door veelal statelijke actoren of daaraan gelieerde groepen. *Voorbeeld: GreyEnergy malware, gericht op saboteren van kritieke infrastructuur, zoals energienetwerken.*[34]	Dergelijke aanvallen kunnen een langdurig ontwrichtend effect hebben op de maatschappij en vormen een bedreiging voor de nationale veiligheid.
Cybercriminaliteit	Het opzettelijk (tijdelijk) aantasten van de beschikbaarheid, integriteit of vertrouwelijkheid van gedigitaliseerde processen of systemen voor financieel gewin. Bij dit crisistype wordt ook malware ingezet, maar ook bijvoorbeeld DDoS, een aanval waarbij online diensten zwaar worden overbelast en daardoor niet meer beschikbaar zijn. *Voorbeeld: DDoS-aanvallen op de Belastingdienst, douane en DigiD, waardoor deze niet meer beschikbaar zijn.*[35]	De levering van producten of diensten wordt verstoord met maatschappelijke schade tot gevolg. Het vertrouwen in de digitale samenleving wordt geschaad.
Cyberterrorisme	Het opzettelijk en langdurig aantasten van gedigitaliseerde processen of systemen mogelijk leidend tot vernietiging daarvan (vergelijkbaar met sabotage). *Er zijn geen recente voorbeelden van cyberterrorisme, maar dit is wel een bron van zorg voor de nabije toekomst.*[36]	Dergelijke aanvallen kunnen een langdurig ontwrichtend effect hebben op de maatschappij.
Cyberactivisme (cybervandalisme)	Het opzettelijk aantasten van de beschikbaarheid en integriteit van informatie en systemen. Bij dit crisistype wordt bijvoorbeeld digitaal ingebroken (*hacken*). *Voorbeelden: informatiediefstal (datalekken) en manipulatie van (informatie op) websites.*	Bij dit crisistype wordt de levering van producten of diensten verstoord, waardoor maatschappelijke schade ontstaat.
Fake nieuws	Het opzettelijk verspreiden van onjuiste informatie om een (politiek) doel te bereiken via (sociale) media. *Voorbeelden: Amerikaanse verkiezingen, MH17-toedracht.*[37]	Bij dit crisistype wordt de publieke opinie beïnvloed waardoor mogelijk berichten van de overheid niet worden geaccepteerd.
Storing en uitval	Niet-opzettelijke storing of uitval van gedigitaliseerde processen of systemen door menselijk falen, technisch falen, natuurgeweld (hitte, droogte, vocht). Dit crisistype wordt versterkt door de toenemende mate van complexiteit en koppeling van systemen: uitval van één systeem kan uitval veroorzaken op andere plekken. *Voorbeeld: een softwarefout in de treinverkeersleiding zorgt in augustus 2018 voor chaos in het treinverkeer rondom Amsterdam.*[38]	Dit crisistype heeft een grote potentiële impact, in het bijzonder wanneer een centraal informatieknooppunt of vitaal proces wordt geraakt (energie, transport, telecom, etc.).

32) Wikipedia.nl. *Russische cyberaanval tijdens de Amerikaanse verkiezingen.*
33) NOS (2019). *Chinese cyberaanval op ASML.*
34) Welivesecurity (2018). *Updated arsenal of one of the most dangerous threat actors.*
35) Beveiligingnieuws (2019). *Stijging DDoS aanvallen.*
36) NCSC (2019). *Cybersecuritybeeld Nederland.*
37) Modderkolk (2019). *Het is oorlog en niemand die het ziet.*
38) ProRail (2018). *Oorzaak computerstoring treinverkeersleiding gevonden.*

Bijlage 2 Specifieke aspecten van een (dreigende) cybercrisis

Een cybercrisis verschilt ten opzichte van een traditionele crisis door de technologische component (digitale processen, ICT, internet, etc.). Cybergevolgbestrijding kent een aantal specifieke uitdagingen ten opzichte van de traditionele crisisbestrijding. Anders gezegd: wat maakt een cybercrisis anders dan een traditionele ramp of crisis?

We onderscheiden de volgende zes cyber-specifieke aspecten.

Aspect	Kenmerken	Toelichting
Onopgemerkte crisis.	• Niet altijd direct een (technische) oplossing aanwezig na ontdekking. • Kan worden veroorzaakt door een tot op dat moment onbekende kwetsbaarheid. • Aanzienlijke (potentiële) schade. • Aanhoudende dreiging.	Een cybercrisis wordt niet altijd direct opgemerkt. Een (dreigende) cybercrisis is daardoor veelal een *crisis in wording*. Gemiddeld hebben organisaties in Europa, Midden-Oosten en Afrika (EMEA) zo'n 175 dagen nodig om aanvallers in hun netwerk te detecteren.[39] Hierdoor neemt de kans op schade aanzienlijk toe, in het bijzonder bij exploitatie van kwetsbaarheden waarvoor nog geen oplossing beschikbaar is.[40] De trend is bovendien zorgelijk: de gemiddelde detectietijd is 40% toegenomen ten opzichte van de meting uit 2017. Uit de resultaten blijkt eveneens dat organisaties die het slachtoffer zijn geworden van een aanval waarschijnlijk opnieuw worden aangevallen.
Snelle (geografische) verspreiding.	• Snelle verspreiding • Snelle escalatie. • Verspreiding niet geografisch beperkt. • Acute alarmering (nog) niet getroffen organisaties.	Een cybercrisis kan zich dankzij het internet in een *hoog tempo verspreiden*, ook over landsgrenzen heen. De WannaCry-cyberaanval is een goed voorbeeld daarvan.[41] De aanval begon op vrijdagochtend 12 mei 2017. Diezelfde dag had de malware meer dan 230.000 computers in meer dan 150 landen besmet. Onder de getroffen organisaties bevonden zich onder meer ziekenhuizen, oliemaatschappijen, transportbedrijven en banken. Dit betekent ook dat een cybercrisis bij een ander kan leiden tot mogelijke gevolgbestrijdingsmaatregelen bij nog niet getroffen instanties.
Hoge (informatie)keten afhankelijkheid.	• Ketenafhankelijkheid. • Cascade effecten. • Niet regio gebonden effecten.	Organisaties werken veelal in *(informatie)ketens* en zijn in hoge mate *verbonden en afhankelijk* van elkaar (hyperconnectiviteit). Dat betekent dat een cybercrisis een kettingreactie kan veroorzaken, waardoor andere systemen in de keten niet goed meer functioneren. Een organisatie kan nadelige effecten ondervinden zonder dat het zelf direct geraakt is (cascade effect). De negatieve effecten zijn bovendien niet-regiogebonden.
Publiek private samenwerking.	• Afhankelijkheid private sector ICT-infrastructuur. • Capaciteit en expertise veelal bij private partijen aanwezig. • Technische complexiteit.	Voor het managen van bronbestrijding (oplossen van de technische problematiek) en cybergevolgbestrijding is de overheid in grote mate *afhankelijk van private partijen en shared service centers*. Vrijwel de gehele ICT-infrastructuur in de wereld is in handen van de private sector. De technologie wordt geleverd door private partijen. Daarnaast beschikt de private sector over grotere expertise en capaciteit op het gebied van cybersecurity dan de publieke sector.
Taalverschil bestuurders en digitaal specialisten.	• Bestuurlijke communicatie • Bestuurders kunnen de ernst niet goed duiden. • Urgentiebesef op bestuurlijk niveau. • Cyberincident als 'nieuw' fenomeen voor een organisatie.	De technologie component in een cybercrisis introduceert *grote taalverschillen* tussen de bestuurders en de digitaal specialisten. Dit kan tijdens een cybercrisis leiden tot vertragingen in de besluitvorming of zelfs verkeerde besluiten. Ook de bronbestrijding kan lastiger zijn omdat technische expertise binnen de traditionele crisisteams ontbreekt of de oorzaken simpelweg niet goed herkend worden. Wat daarbij meespeelt is dat veel organisaties niet eerder geconfronteerd zijn met een cyberincident. Een goed voorbeeld is de DigiNotar-crisis. Gemeenten en andere organisaties waren destijds niet voorbereid en hadden bijvoorbeeld niets geregeld voor het met spoed vervangen van beveiligingscertificaten, waardoor bij veel gemeenten de dienstverlening langer niet beschikbaar was dan nodig.
(Inter)nationaal karakter.	• Samenwerken op (inter) nationaal niveau. • Rekening houden met verschillende jurisdicties. • Betrokkenheid statelijke actoren. • Taalverschillen.	Cybercrises kunnen van nature een *(inter)nationaal karakter* hebben waardoor deze zich op hetzelfde moment in meerdere landen kunnen manifesteren. Dit vereist samenwerking en coördinatie op internationaal niveau, waarbij het opereren onder verschillende jurisdicties een grote uitdaging is. Wat de complexiteit vergroot is dat statelijke actoren mogelijk zelf betrokken zijn bij het veroorzaken van een cybercrisis (cyberspionage, cybersabotage).

39) Fireeye (2020). *M-trends 2020.*
40) Wikipedia.nl. *Zerodayattack.*
41) Wikipedia.nl. *WannaCry ransomware attack.*

Bijlage 3 Digitale aanvalstechnieken

In de volgende tabel staan de meest voorkomende digitale aanvalstechnieken. Het overzicht bevat met name technieken die kunnen worden ingezet voor aanvallen op (vitale) digitale processen en systemen. Er worden voortdurend nieuwe aanvalstechnieken ontwikkeld (veelal varianten op bestaande methoden). Dergelijke aanvalstechnieken blijven vaak lang onopgemerkt omdat ze technisch geavanceerd zijn en moeilijk traceerbaar. Hoewel deze geavanceerde aanvalstechnieken grote schade kunnen aanrichten, stelt het CSBN 2019 dat ook eenvoudige aanvalstechnieken succesvol kunnen worden ingezet.

De aanvalstechnieken staan veelal niet op zichzelf. Verschillende technieken worden in combinatie of achtereenvolgend ingezet. Dit vergroot de kans van slagen voor kwaadwillenden.

Aanvalstechniek	Toelichting
Denial-of-Service-aanval (DDoS).	Een Distributed-Denial-of-Service-aanval (DDoS) heeft tot doel om een specifieke dienst (veelal een website) van een organisatie onbruikbaar te maken door deze over te belasten. Hiervoor wordt gebruik gemaakt van een groot aantal verschillende bronnen, zoals geïnfecteerde computers en IoT-apparatuur. Deze zijn vaak onderdeel van een zogenaamd Botnet, een netwerk van besmette systemen die centraal kan worden bestuurd. Door een groot aantal systemen tegelijk grote hoeveelheden data te laten versturen naar één systeem, server of netwerk raakt deze overbelast, waardoor digitale processen en systemen voor een bepaalde tijd niet meer beschikbaar zijn. *Voorbeelden DDoS-aanvallen: Dyn-aanval, GitHub-aanval, DigiD-aanval*
Computer worm.	Een computerworm is eveneens een type malware. Een worm verspreidt zich (zonder tussenkomst) naar andere systemen en besmet zo complete netwerken. Een worm hoeft ook geen bestaande applicatie (host file) binnen te dringen om schade aan te richten en is daardoor zeer schadelijk. Wormen worden veelal verspreid via e-mails in bijlagen. Zodra de worm is geactiveerd zal deze het systeem kunnen binnendringen zonder dat de gebruiker dat merkt. Een worm kan zich via een adressenbestand verspreiden naar andere gebruikers. Een worm is vaak ontworpen met als doel om beveiligingslekken te exploiteren en zo schade aan te richten. Voorbeelden computer worm: Stuxnet, ILOVEYOU, The Morris Worm
Malware aanval.	Malware (malicious software) is een verzamelnaam voor kwaadaardige software. Een malware-aanval wordt gebruikt om een toegang te krijgen tot systemen, waarna deze kunnen worden verstoord, overgenomen of belangrijke informatie kan worden verkregen. Malware kan systemen virtueel infecteren (via bijvoorbeeld een internetverbinding) of fysiek (via bijvoorbeeld een USB-stick). Virtuele en fysieke methoden worden vaak gezamenlijk gebruikt om een groter effect te sorteren. Onder een malware-aanval kan een groot aantal verschillende aanvallen worden verstaan. Veel aanvalstechnieken die hier worden beschreven, vallen onder de noemer malware-aanval. *Voorbeelden malware: virussen, ransomware, wipermalware, trojans en worms (zie hiernavolgend)*
Man-in-the-middle (MITM)-aanval.	Een man-in-the-middle (MITM)-aanval is een aanval waarbij een kwaadwillende de (data)communicatie tussen twee partijen ongemerkt onderschept. Met dit type aanval kan belangrijke informatie worden verkregen en zelfs worden gemanipuleerd. Aangezien de versturende en ontvangende partij niet weten dat er een kwaadwillende tussen hen in zit, blijft de onderschepping vaak lang onopgemerkt. Om de datacommunicatie tussen twee of meerdere systemen te infiltreren maken kwaadwillenden gebruik van verschillende technieken, die veelal bekende zwakke plekken van internetcommunicatie exploiteren (bijvoorbeeld DHCP of DNS aanvallen). *Voorbeelden MITM: e-mail hijacks, Wi-Fi MITM, Man-In-The-Browser Attack*
Phishing-aanval.	Phishing is een vorm van social engineering (manipulatie van menselijk gedrag) waarbij een kwaadwillende slachtoffers gericht e-mails verstuurt of telefonisch benadert om zo gevoelige informatie te achterhalen of om malware te installeren op hun systemen. Het slachtoffer van een phising-aanval is veelal in de veronderstelling dat de persoon die contact legt een bekende is of een vertrouwde organisatie vertegenwoordigt. Phishing wordt onder meer ingezet voor het achterhalen van bank- of andere inloggegevens. Een agressieve vorm van phishing is spear phishing. Hierbij wordt eerst persoonlijke informatie van het slachtoffer achterhaald om de aanval nog persoonlijker en effectiever te maken. Andere voorbeelden Phishing: CEO fraud, Dropbox phising, Deceptive phishing
Ransomware-aanval.	Ransomware is een specifiek type malware-aanval waarbij bestanden worden versleuteld en zo onbruikbaar worden gemaakt. Getroffen systemen worden pas vrijgegeven na betaling van losgeld (veelal in de vorm van Bitcoins). Deze vorm van digitale afpersing maakt gebruik van encryptie-technieken. De malware wordt veelal geïnstalleerd en geactiveerd na het klikken op een misleidende hyperlink in een e-mailbericht of op een website. Het is vrijwel onmogelijk om zelf de bestanden te ontsleutelen zonder te beschikken over de encryptiesleutel. Na betaling van losgeld wordt de sleutel verstrekt, maar dit is niet altijd het geval. Ransomware is een zeer effectieve methode van afpersing. Getroffen organisaties staan voor een groot dilemma: wel of niet betalen. Systemen kunnen veelal worden hersteld door middel van het terugzetten van een back-up. Zonder externe afgekoppelde back-up zullen vrijwel zeker bestanden verloren gaan. Voor meer informatie zie ook www.nomoreransom.org *Voorbeelden ransomware: GandCrab, Wannacry, Scareware*
SQL injection-aanval.	SQL injection (SQLi) is een aanvalstechniek waarbij webapplicaties worden gemanipuleerd. SQL is een computertaal om met databases te communiceren. Door middel van een SQLi kan een kwaadwillende inzicht krijgen in de inhoud van een database, wijzigingen doorvoeren of bestanden naar de database schrijven. Hierdoor kan de database ernstig worden beschadigd of zelfs vernietigd. SQLi is daarom vooral gevaarlijk voor digitale processen die data gedreven zijn (en een database bevatten). Denk hierbij aan webapplicaties. Het voorkomen van een SQLi is in principe niet ingewikkeld. Tegenwoordig is deze aanvalstechniek daarom voornamelijk gericht op kleinere webapplicaties. Toch hebben ook grotere websites te maken gehad met een SQLi aanval (Yahoo, The Pirate Bay en Sony).
Trojans.	Een Trojan, of Trojan Horse, is een type malware waarbij social engineering wordt gebruikt om onoplettende gebruikers te misleiden. Een Trojan is legitiem lijkende, maar in werkelijkheid malafide software. Wanneer deze wordt geactiveerd kan de kwaadwillende beschikken over vertrouwelijke gegevens, deze wijzigen of zelf stelen. Tevens kunnen de prestaties van systemen worden gecompromitteerd. Er bestaan verschillende soorten Trojans, die worden geclassificeerd op basis van de acties die na activatie kunnen worden uitgevoerd op een systeem. Een Trojan kan bijvoorbeeld beschikken over een backdoor waarmee kwaadwillenden een systeem op een later moment kunnen misbruiken. *Voorbeelden Trojan: Backdoor, Rootkit, Exploit*

Bijlage 4 Relevante wet- en regelgeving

Rondom het thema cybergevolgbestrijding heeft de gemeente specifieke kenmerken en handelingsperspectieven. In de koude fase zijn de verantwoordelijkheden van gemeenten en partners voldoende beschreven. Zo kennen we voor de informatieveiligheid inmiddels de landelijke Baseline Overheid (BIO)[42] die sinds 1 januari 2020 van kracht. De BIO vervangt de BIG, BIR, BIR2017, IBI en BIWA. Ook in de strafrechtketen raakt men inmiddels steeds meer bekend met het handhaven in de online wereld. Voor de bestrijding van digitale criminaliteit kennen we Europese en nationale wetgeving (bijvoorbeeld computercriminaliteit III).

Met betrekking tot de daadwerkelijke gevolgbestrijding van een incident of crisis zijn de bevoegdheden en verantwoordelijkheden echter minder goed beschreven. Er is nauwelijks een overzicht van handelingsperspectieven voor de gemeenten en veiligheidsregio's die specifiek voor cyber gelden.[43] Afhankelijk van het soort cybercrisis zijn er ook verschillende juridische kaders waarbinnen gehandeld moet worden. In deze bijlage proberen we daarom volgens de bestaande juridische kaders de verschillende taken en bevoegdheden in de cybergevolgbestrijding in kaart te brengen.

Wanneer een cybercrisis op grote schaal plaatsvindt, kan dit in korte tijd leiden tot chaos met gevolgen voor de openbare orde en veiligheid of voor de maatschappij. Denk bijvoorbeeld aan de gerichte sabotage van ziekenhuizen, het verstoren van het openbaar vervoer of wanneer vitale voorzieningen in Nederland worden geraakt.

Wet veiligheidsregio's en gemeentewet

Indien zich een cybercrisis voordoet met fysieke effecten op de openbare orde en veiligheid, is er voor de burgemeester een centrale rol weggelegd. Artikel 172, eerste lid, van de Gemeentewet bepaalt namelijk dat de burgemeester belast is met de handhaving van de openbare orde.[44] Een burgemeester kan vanuit zijn rol verschillende verantwoordelijkheden hebben, waaronder als burgemeester van een gemeente en als voorzitter van de veiligheidsregio. Volgens de Wet veiligheidsregio's heeft de burgemeester een aantal bevoegdheden[45]:

- De burgemeester heeft het gezag bij brand alsmede bij ongevallen anders dan bij brand voor zover de brandweer daarbij een taak heeft (artikel 4).
- De burgemeester heeft het opperbevel in geval van een ramp of van ernstige vrees voor het ontstaan daarvan (artikel 5).
- De burgemeester kan de leiding van het ambulancevervoer aanwijzingen geven ten behoeve van de openbare orde (artikel 6).
- De burgemeester is belast met de informatievoorziening tijdens de ramp of crisis (crisiscommunicatie) naar bevolking en hulpverleners (artikel 7).

In het veiligheidsberaad is daarnaast ook gesproken over de rol van de veiligheidsregio's bij digitale ontwrichting. Dit is nog geen vastgestelde landelijke beleidslijn, maar geeft wel een indicatie hoe hier in de veiligheidsregio's naar gekeken kan worden. Met het toenemen van het aantal digitale verstoringen zal deze beleidslijn zich steeds verder uitkristalliseren. 'Aangezien de oorzaak van branden, rampen en crises ook in de digitale omgeving kan liggen, zullen de veiligheidsregio's moeten anticiperen op het voorkomen van digitale ontwrichting dan wel het verkleinen van de kans erop.'[46] De burgemeester heeft een verantwoordelijkheid als het gaat om de verschillende aspecten van de digitale veiligheid van een gemeente of de regio:

- Informatieveiligheid (eigen organisatie).
- Risicoanalyse en -beheersing.
- Openbare orde en veiligheid.
- Bestrijding van digitale criminaliteit.
- Cybergevolgbestrijding.

De gemeente en veiligheidsregio (onder gezag van de burgemeester) hebben bij een digitale verstoring ook de verantwoordelijkheid om burgers te beschermen en voor te lichten. Een burgemeester is echter niet verantwoordelijk voor de verlening van continuïteit binnen vitale sectoren of de aanpak van een cyberincident zelf.

Wet beveiliging netwerk- en informatiesystemen (Wbni)

De Wet beveiliging netwerk- en informatiesystemen (Wbni), ook wel de Cybersecuritywet genoemd, en het besluit Bbni is in essentie de Nederlandse implementatie van de Europese richtlijn over netwerk- en informatiebeveiliging (NIB-richtlijn), die een hoger niveau van cybersecurity binnen de EU beoogt.[47)-48)] De Wbni en bijbehorend besluit regelen onder meer een meldplicht voor vitale sectoren en is dus relevant in het geval een organisatie in één van de aangewezen vitale sectoren geraakt is. Onder de Wbni vallen als (andere aangewezen) vitale aanbieder (AED of AAVA) of digitale dienstverlener (DSP). NCSC geldt volgens de Wbni als het CSIRT voor vitale diensten, de minister van EZK als CSIRT voor de DSP's. Omdat gemeenten en veiligheidsregio's vooralsnog geen vitale aanbieder zijn, kunnen zij tijdens een cybercrisis niet direct gebruik maken van de kennis en expertise van het NCSC. Ook zal de ICT Response Board niet direct worden geactiveerd als er sprake is van een (dreigende) cybercrisis. De gemeente of veiligheidsregio valt volgens het besluit onder de Wbni. Het NCSC attendeert veiligheidsregio's en gemeenten niet direct op risico's en dreigingen, terwijl ze hier vanuit hun wettelijke taak wel een verantwoordelijkheid in hebben. De gemeente kan wel indirect te maken krijgen met de werking ervan, als een organisatie in de vitale sector binnen de gemeente of regio geraakt is. Dan geldt het NCSC als aanspreekpunt.

Omdat het NCSC niet direct verbonden is aan gemeenten, bestaat er de IBD. De IBD is de sectorale CERT/CSIRT voor alle Nederlandse gemeenten en daarmee ook het aanspreekpunt voor cyberincidenten die plaatsenvinden binnen de bedrijfscontinuïteit van gemeenten. De IBD zorgt er daarnaast voor dat kennis over cybersecurity bij de gemeenten onderling wordt gedeeld, maar ook met leveranciers en vitale sectoren. Dit doen zij als schakelpunt naar het NCSC.

Politiewet

Volgens de politiewet wordt de taak van de politie als volgt omschreven[49]:

'De politie heeft tot taak in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.'

De politie heeft, ter uitvoering van zijn taak, de bevoegdheid om geweldsmiddelen en vrijheidsbeperkende middelen toe te passen (Politiewet 2012, artikel 7). Cybercrime kan de openbare orde en veiligheid verstoren en valt daardoor onder de reguliere opsporingsverantwoordelijkheid van politie en OM. De politie voert deze taak uit middels cybercrimeteams in de eenheden en het THTC. Dit team richt zich op de meest geavanceerde vormen van cybercrime. Daarnaast bestaat er binnen de politie het Landelijk Meldpunt Internet Oplichting en een samenwerkingsverband met banken. De politie voert, vanwege de aard van cybercrime, zijn opsporingstaak uit in samenwerking met andere internationale politie-organisaties (onder andere Europol). Dit doen zij ook in samenwerking met de nationale inlichten- en veiligheidsdiensten.

Voor gemeenten en veiligheidsregio's geldt dat hierin een belemmering bestaat om te handhaven in de online wereld. Het gemeenterecht is geschreven vanuit een offline oogpunt en is dus niet direct toepasbaar in de online wereld. Politie en Openbaar Ministerie zijn de bevoegde organen als het gaat om optreden achteraf. 'Voor bestuursrechtelijk optreden door de burgemeester in zijn hoedanigheid van handhaver van de openbare orde is dan geen ruimte. Wel kan de burgemeester op de hoogte worden gesteld van dergelijke zaken in het driehoeksoverleg, zeker indien de uitingen gepaard gaan met een bedreiging van de openbare orde.'[50]

Wet op de inlichtingen- en veiligheidsdiensten (WIV)

Op 1 mei 2018 is de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) ingegaan, die geldt voor de AIVD en MIVD.[51] De Wiv is een belangrijk instrument om de toenemende dreigingen rondom cyber tegen te gaan. De gemoderniseerde wet

42) IBD (2020). *Baseline Informatiebeveiliging Overheid (BIO).*
43) IFV (2018). *De rol van de veiligheidsregio's bij digitale ontwrichting.*
44) Overheid.nl. *Gemeentewet.*
45) Overheid.nl. *Wet veiligheidsregio's.*
46) Overheid.nl. *Wet veiligheidsregio's.*
47) Overheid.nl. *Wet beveiliging netwerk- en informatiesystemen.*
48) Overheid.nl. *Besluit beveiliging netwerk- en informatiesystemen.*
49) Overheid.nl. *Politiewet 2012.*
50) Bantema, Twickler, Munneke, Duchateau & Stol (2018). *Burgemeesters in Cyberspace*
51) Overheid.nl. *Wet Inlichtingen- en Veiligheidsdiensten.*

vergemakkelijkt onderzoek naar cyberdreigingen en dreigingsbeelden in het cyberdomein. De Wiv maakt het mogelijk om de volgende acties uit te voeren: onderzoeksopdrachtgerichte interceptie (art. 48-50), (2) de hackbevoegdheid (art. 45), (3) het stelselmatig vergaren van gegevens omtrent personen uit open bronnen (art. 38) en (4) de informantenbevoegdheid (art. 39).

'Voor de AIVD en de MIVD is een belangrijke taak weggelegd deze vorm van spionage vroegtijdig te detecteren en waar mogelijk te voorkomen. Om dat mogelijk te maken wordt gezocht naar de kenmerken van ongewenste activiteiten (bijv. signatures van kwaadaardige software) en naar verkeer dat ongebruikelijke afwijkingen vertoont (anomaliedetectie).'[52)]

Algemene Verordening Gegevensbescherming (AVG)

De Europese Algemene Verordening Gegevensbescherming (AVG) regelt de bescherming van persoonsgegevens en het vrije verkeer van persoonsgegevens binnen de Europese Unie.[53)] De AVG versterkt rechten en plichten rondom privacy en regelt onder meer een meldplicht in geval van datalekken. De verordening geldt voor alle bedrijven en organisaties die zich met persoonsgegevens bezighouden. De AVG is bij een cybercrisis relevant in het geval persoonsgegevens zijn gelekt of gestolen, in het bijzonder de meldplicht datalekken. De getroffen gemeente meldt de datalek bij de Autoriteit Persoonsgegevens.

Telecommunicatiewet

Telecommunicatie is momenteel niet meer weg te denken. Iedereen moet tegenwoordig toegang kunnen hebben tot betrouwbare en moderne telecommunicatie. Om deze groeiende markt te reguleren bestaat de Telecommunicatiewet. Deze wet is gebaseerd op regels van Europese verordeningen en Nederlandse wetten.

De Telecommunicatiewet regelt onder andere:

- frequentiebeleid
- beleid van telefoonnummers
- consumentenbescherming
- privacybescherming.

Voor crisisbeheersing in telecommunicatie speelt de Telecommunicatiewet een belangrijke rol.[54)] 'Voor crisisbeheersing ten aanzien van het internet gelden geen bijzondere bepalingen in aanvulling op de algemene regeling in de Telecommunicatiewet. Het aanbieden van internettoegang valt onder 'het aanbieden van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten' in de zin van die wet'.[55)]

De Telecommunicatiewet regelt het bevoegd gezag. De minister van EZK is bevoegd om maatregelen jegens de telecomsector te nemen, de minister van J&V jegens computercriminaliteit en persoonlijke levenssfeer en de burgemeester of voorzitter veiligheidsregio alleen ten aanzien van de gevolgen van onbereikbaarheid. De Telecommunicatiewet regelt ook de continuïteit van telecommunicatie. Om de continuïteit van telecommunicatie veilig te stellen stelt artikel 11a. 1 uit de Telecommunicatiewet dat aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten passende technische en organisatorische maatregelen nemen om de risico's voor de veiligheid en de integriteit van hun netwerken en diensten te beheersen. Indien de continuïteit van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten wordt onderbroken geldt dat bij een inbreuk op de veiligheid en/of een verlies van integriteit de minister in kennis wordt gesteld.

De Telecommunicatiewet (artikel 14) regelt ook dat in bijzondere omstandigheden de minister van EZK aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten aanwijzingen kan geven om de telecommunicatie van en naar het buitenland te verzorgen (in overeenstemming met de minister van BZ). Ook regelt de wet dat in bijzondere omstandigheden aanwijzingen kunnen worden gegeven aan aanbieders om bij mededelingen van overheidsinstanties om het publiek te waarschuwen voor dreigende rampen of noodsituaties en om de gevolgen van rampen of noodsituaties te verzachten, gebruik te maken van de diensten.

52) Oerlemans & Hagens (2018). *De Wet op de inlichtingen- en veiligheidsdiensten 2017: Een technologisch gedreven wet*
53) Overheid.nl. *Uitvoeringswet Algemene verordening gegevensbescherming*
54) Overheid.nl. *Telecommunicatiewet.*
55) IFV (2015). *Bestuurlijke Netwerkkaarten Crisisbeheersing. Netwerkkaart 21: Telecommunicatie & internet.*

Wet computercriminaliteit

Per 1 maart 2019 is de Wet computercriminaliteit III in werking getreden.[56)] Deze wet versterkt de opsporing en vervolging van computercriminaliteit. Hier zijn wijzigingen in het Wetboek van Strafrecht en het Wetboek van Strafvordering aan vooraf gegaan. Politie en Justitie kunnen middels deze wet heimelijk en online onderzoek doen in computers (pc, mobiele telefoon of server). Ook zijn er meer handelingen beschikbaar om onderzoek te doen naar ernstige delicten. Ambtenaren kunnen bij een zeer ernstig misdrijf gegevens ontoegankelijk maken of kopiëren en als het gaat om een ernstig misdrijf communicatie aftappen of observeren.

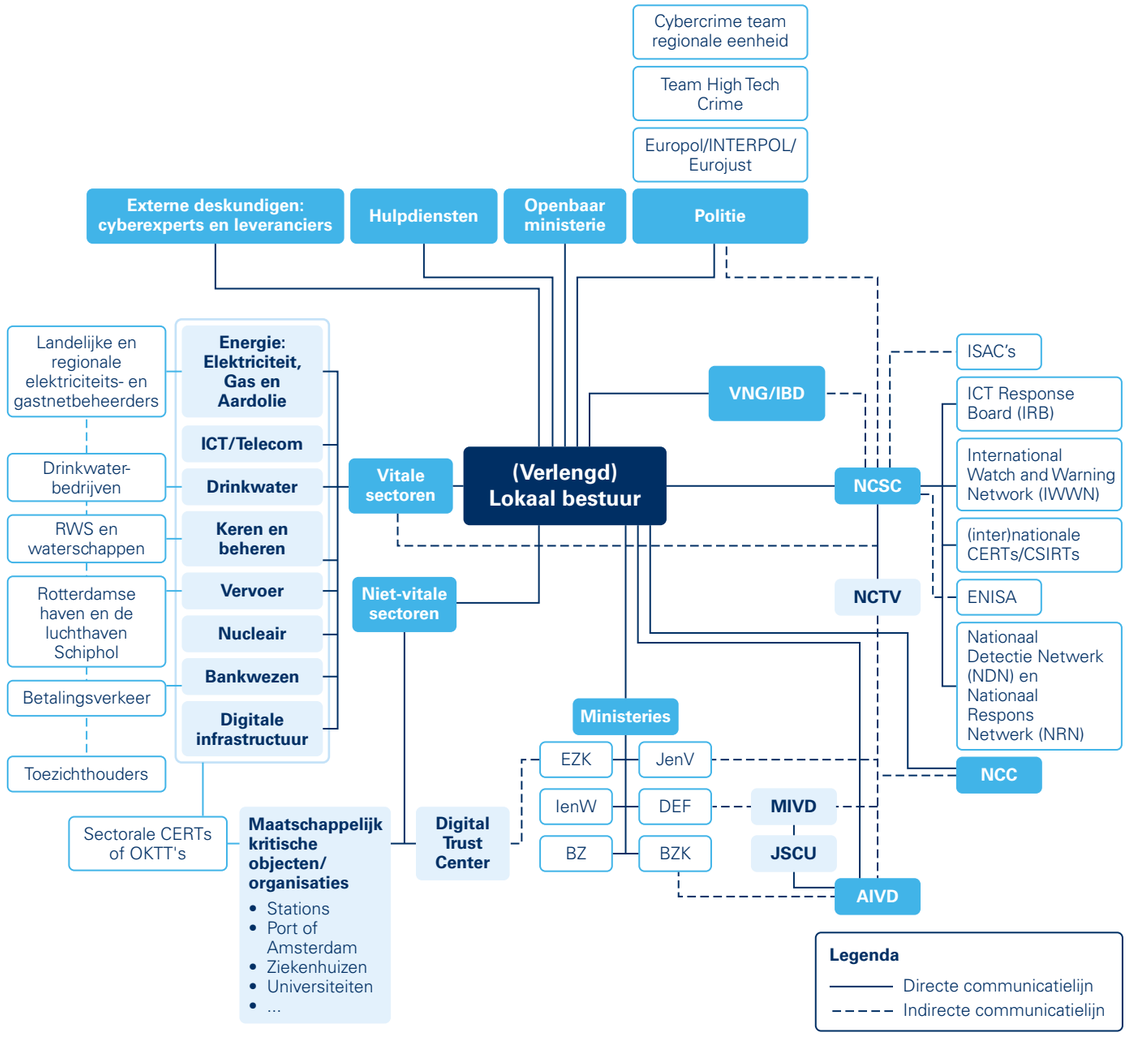
Coordinated vulnerability disclosure beleid

Een Coordinated Vulnerability Disclosure (CVD), eerder bekend als Responsible Disclosure, is 'het op een gecoördineerde wijze bekend maken van een kwetsbaarheid'[57)] en wordt opgesteld door een organisatie zelf. Een melder maakt in gezamenlijkheid met een organisatie ICT-kwetsbaarheden openbaar. De organisatie waar de kwetsbaarheden zijn aangetroffen hebben in zo een geval tijd om de kwetsbaarheid op te lossen. Het beleid stelt dat er bijvoorbeeld geen aangifte wordt gedaan van inbreuk indien de melder zich aan de spelregels heeft gehouden. Een CVD helpt de veiligheid van ICT-systemen te vergroten en ICT-kwetsbaarheden eerder te melden om de kans op schade zoveel mogelijk te beperken. Voor meer informatie over het CVD-beleid adviseren wij de Leidraad Coordinated Vulnerability Disclosure van het NCSC te raad plegen.[58)]

56) Overheid.nl. *Wijzigingswet Wetboek van Strafrecht, enz. (verbetering en versterking opsporing [...] computercriminaliteit (computercriminaliteit III))*
57) NCSC (2018). *Leidraad Coordinated Vulnerability Disclosure.*
58) NCSC (2018). *Leidraad Coordinated Vulnerability Disclosure.*

Bijlage 5 Netwerkkaart

Deze netwerkkaart geeft de verschillende communicatielijnen in het gemeentelijke landschap weer voor cybergevolgbestrijding. Het biedt een overzicht van alle crisispartners die betrokken kunnen zijn tijdens een cybercrisis en daarmee ook de complexiteit die hiermee gepaard gaat.



Bijlage 6 Vitale processen

Om als maatschappij te kunnen functioneren, is het onderhouden van een aantal specifieke processen cruciaal. Het gaat om systemen en middelen, die fysiek of virtueel, zo belangrijk zijn voor Nederland dat een verstoring enorme impact kan hebben op de nationale veiligheid, ons economisch welzijn, de gezondheid of een combinatie daarvan. Deze processen noemen we vitale processen, de vitale infrastructuur of vitale systemen. In deze handreiking spreken we regelmatig over deze vitale processen waardoor een korte toelichting noodzakelijk is.

In het besluit meldplicht cybersecurity is vastgesteld wat de vitale processen in Nederland zijn en een melding bij het NCSC verplicht is.[59] Deze processen zijn gecategoriseerd naar categorie A en B, waarbij uitval van A-vitale processen grotere potentiële gevolgen op de samenleving heeft dan uitval van B-vitale processen en A-vitale processen voldoen aan het criterium van cascade/domino-effecten.[60]

Categorie A

In het geval van uitval, aantasting of verstoring van een A-vitaal proces wordt rekening gehouden met de volgende gevolgen[61]:

- Economische gevolgen: > circa €50 miljard schade of circa 5,0 % daling reëel inkomen.
- Fysieke gevolgen: meer dan 10.000 personen dood, ernstig gewond of chronisch ziek.
- Sociaal maatschappelijke gevolgen: meer dan 1 miljoen personen ondervinden emotionele problemen of ernstig maatschappelijke overlevingsproblemen.
- Cascade gevolgen: Uitval heeft als gevolg dat minimaal twee andere sectoren uitvallen.

Vitaal proces	Sector	Ministerie
Landelijk transport en distributie elektriciteit	Energie	EZK
Gasproductie, landelijk transport en distributie gas		
Olievoorziening		
Drinkwatervoorziening	Drinkwater	IenW
Keren en beheren waterkwantiteit	Water	IenW
Opslag, productie en verwerking nucleair materiaal	Nucleair	IenW

Categorie B

In deze categorie staat de infrastructuur die bij verstoring, aantasting of uitval de ondergrenzen van minstens één van de drie impactcriteria voor categorie B raakt:

- Economische gevolgen: > circa € 5 miljard schade of ca. 1,0 % daling reëel inkomen.
- Fysieke gevolgen: meer dan 1.000 personen dood, ernstig gewond of chronisch ziek.
- Sociaal maatschappelijke gevolgen: meer dan 100.000 personen ondervinden emotionele problemen of ernstig maatschappelijke overlevingsproblemen

Vitaal proces	Sector	Ministerie
Regionale distributie elektriciteit	Energie	EZK
Regionale distributie gas		
Internet en datadiensten	ICT/Telecom	EZK
Internettoegang en dataverkeer		
Spraakdienst en SMS		
Plaats- en tijdsbepaling GNSS		EZK
Vlucht- en vliegtuigafhandeling	Transport	IenW
Scheepsvaartafwikkeling		
Grootschalige productie/verwerking en/of opslag (petro) chemische stoffen	Chemie	IenW
Toonbankbetalingsverkeer	Financieel	FIN
Massaal giraal betalingsverkeer		
Hoogwaardig betalingsverkeer tussen banken		
Effectenverkeer		
Communicatie met en tussen hulpdiensten middels 112 en C2000	OOV	JenV
Inzet politie		
Basisregistraties personen en organisaties	Digitale overheids-processen	BZK
Interconnectiviteit (transactie-infrastructuur voor informatie uit basisregistraties)		
Elektronisch berichtenverkeer en informatie-verschaffing aan burgers		
Identificatie en authenticatie van burgers en bedrijven		
Inzet defensie	Defensie	DEF

59) Overheid.nl. *Besluit beveiliging netwerk- en informatiesystemen.*
60) Overheid.nl. *Besluit tot aanwijzing van aanbieders, producten en diensten ten aanzien waarvan een plicht geldt om ernstige ICT-incidenten te melden.*
61) NCSC (2020). *Nationaal Crisisplan Digitaal.*

Bijlage 7 Documentatie

Algemene Rekenkamer (2019). *Digitale dijkverzwaring: cybersecurity en vitale waterwerken.* https://www.rekenkamer.nl/publicaties/rapporten/2019/03/28/digitale-dijkverzwaring-cybersecurity-en-vitale-waterwerken

Bantema, W., Twickler, S.M.A., Munneke, S.A.J., Duchateau, M. & Stol, W.Ph. (2018). *Burgemeesters in Cyberspace: Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld.* https://www.burgemeesters.nl/sites/www.burgemeesters.nl/files/File/Rapport%20-%20Burgemeesters%20in%20CS%20-%20definitief.pdf. Politie & Wetenschap: Apeldoorn

Cyberveilig Nederland (2019). *Cybersecurity Woordenboek. Van cybersecurity naar Nederlands.* https://cyberveilignederland.nl/woordenboek-cyberveilig-nederland/

Informatiebeveiligingsdienst (IBD). Verantwoordelijkheden van de VCIB. https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2015/02/15-0205-Factsheet_Verantwoordelijkheden_LR-DEF.pdf

Informatiebeveiligingsdienst (IBD) (2020). *Handreiking IB-functieprofiel Chief Information Security Officer BIO.* https://www.informatiebeveiligingsdienst.nl/product/handreiking-ciso-functieprofiel/

Instituut Fysieke Veiligheid. *Netcentrisch werken.* https://www.ifv.nl/kennisplein/Paginas/Netcentrisch-Werken.aspx

Instituut Fysieke Veiligheid (april 2019). *Bestuurlijke Netwerkkaarten Crisisbeheersing: Netwerkkaart 21b Cybersecurity.* Arnhem: IFV.

Instituut Fysieke Veiligheid (april 2019). *Crisiscommunicatietips voor incidenten met een cybercomponent (digitale verstoring).* Arnhem: IFV.

Instituut Fysieke Veiligheid (2019). *Verbinding tussen werelden. Een verdiepende studie naar de aanpak van zeven bovenregionale crisistypen.* Arnhem: IFV.

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

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2014). *Handreiking terrorismebestrijding voor bedrijven.* Den Haag. https://www.sociaalweb.nl/cms/files/2015-12/handreiking_bedrijven_lr_tcm126_573578.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2016). *Nationaal Handboek Crisisbesluitvorming.* https://www.nctv.nl/documenten/publicaties/2016/09/13/nationaal-handboek-crisisbesluitvorming

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2017). *Handreiking Terrorismegevolgbestrijding.* Den Haag.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2018). *Handreiking Alerteringssysteem Terrorismebestrijding (ATb): Publiek-Private Samenwerking bij een terroristische dreigingssituatie.* https://www.nctv.nl/binaries/Handreiking%20ATb%20-%20update%20juni%202018_tcm31-335705.pdf

Nationaal Cyber Security Centrum (2018). *Coordinated Vulnerability Disclosure: de Leidraad.* https://www.ncsc.nl/documenten/publicaties/2019/mei/01/cvd-leidraad

Nationaal Cyber Security Centrum (2018). *Nederlandse Cybersecurity agenda: Nederland digitaal veilig.* https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/mei/01/nederlandse-cybersecurity-agenda/CSAgenda_def_web_tcm31-322330.pdf

Nationaal Cyber Security Centrum (2018). *Start een CSIRT: Collectief samenwerken.* https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/mei/01/start-csirt/Handreiking_collectief_CSIRT.pdf

Nationaal Cyber Security Centrum (2019). *Cybersecuritybeeld 2019: Ontwrichting van de maatschappij ligt op de loer.* https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2019.html

Nationaal Cyber Security Centrum (2020). *Nationaal Crisisplan Digitaal (NCP-Digitaal).* https://www.ncsc.nl/documenten/publicaties/2020/februari/21/nationaal-crisisplan-digitaal

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

Wetenschappelijke Raad voor het Regeringsbeleid (2019). *Voorbereiden op digitale ontwrichting.* WRR: Den Haag. https://www.wrr.nl/binaries/wrr/documenten/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting/R101-Voorbereiden-op-digitale-ontwrichting.pdf

Overheid.nl (2019). *Besluit beveiliging netwerk- en informatiesystemen.* https://wetten.overheid.nl/BWBR0041520/2019-01-01

Bijlage 8 Afkortingenlijst

ACM	Autoriteit Consument & Markt
AC-Pol	Algemeen Commandant Politie
AED	Aanbieder van een essentiële dienst
AIVD	Algemene Inlichtingen en Veiligheidsdienst
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BT	Beleidsteam
BZ	Ministerie van Buitenlandse Zaken
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CERT	Computer Emergency Response Team
CGB	Cybergevolgbestrijding
CISO	Chief Information Security Officer
CoPI	Commando Plaats Incident
CSBN	Cybersecuritybeeld Nederland
CSIRT	Computer Security Incident Response Team
CSR	Cyber Security Raad
CVD	Coordinated Vulnerability Disclosure
DDoS	Distributed Denial of Service
DEF	Ministerie van Defensie
DTC	Digital Trust Center
ECO	Eenheid Communicatie
ECR	Eenheid Crisiscoördinatie
ENISA	European Union Agency for Cybersecurity
EZK	Ministerie van Economische Zaken en Klimaat
G4	De vier grootste gemeenten (Amsterdam, Den Haag, Rotterdam en Utrecht)
GBT	Gemeentelijk Beleidsteam
GMS	Geïntegreerd Meldkamer Systeem
GRIP	Gecoördineerde Regionale Incidentbestrijdings Procedure
GSM	Global system for mobile communications
HIN	Hoofd Informatie Politie
HOPEX	Hoofd Opsporingsexpertise Politie
HOPS	Hoofd Opsporing Politie
IBD	Informatiebeveiligingsdienst
IDC	Intern Dienstencentrum
ICT	Informatie- en communicatietechnologie
IenW	Ministerie van Infrastructuur en Waterstaat
IFV	Instituut Fysieke Veiligheid
IoT	Internet of Things
IRB	ICT Response Board
ISAC	Information Sharing and Analysis Center
IWWN	International Watch and Warning Network
JenV	Ministerie van Justitie en Veiligheid
JSCU	Joint Sigint Cyber Unit
LCMS	Landelijk Crisis Management Systeem
LOCC	Landelijk Operationeel Coördinatiecentrum
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
NCC	Nationaal Crisiscentrum
NCP-Digitaal	Nationaal Crisisplan Digitaal
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NDN	Nationaal Detectie Netwerk
NRN	Nationaal Respons Netwerk
OCW	Ministerie van Onderwijs, Cultuur en Wetenschap
OKTT	Organisatie die objectief kenbaar tot taak heeft andere organisaties of het publiek te informeren.
OM	Openbaar Ministerie
OOV	Openbare Orde en Veiligheid
OT	Operationeel Team
RBT	Regionaal Beleidsteam
ROT	Regionaal Operationeel Team
SIEM	Security Information & Event Management
(N)SGBO	(Nationale) Staf Grootschalig en Bijzonder Optreden
SLA	Service Level Agreement
SOC	Security Operations Center
TDO	Team Digitale Opsporing Politie
THTC	Team High Tech Crime Politie
Wbni	Wet Beveiliging Netwerk- en Informatiesystemen
Wiv	Wet op inlichtingen en veiligheidsdiensten
WRR	Wetenschappelijke Raad voor het Regeringsbeleid
VNG	Vereniging Nederlandse Gemeenten

Berenschot

Berenschot is een onafhankelijk organisatieadviesbureau met 350 medewerkers wereldwijd. Al 80 jaar verrassen wij onze opdrachtgevers in de publieke sector en het bedrijfsleven met slimme en nieuwe inzichten. We verwerven ze en maken ze toepasbaar. Dit door innovatie te koppelen aan creativiteit. Steeds opnieuw. Klanten kiezen voor Berenschot omdat onze adviezen hen op een voorsprong zetten.

Ons bureau zit vol inspirerende en eigenwijze individuen die allen dezelfde passie delen: organiseren. Ingewikkelde vraagstukken omzetten in werkbare constructies. Door ons brede werkterrein en onze brede expertise kunnen opdrachtgevers ons inschakelen voor uiteenlopende opdrachten. En zijn we in staat om met multidisciplinaire teams alle aspecten van een vraagstuk aan te pakken.

Berenschot Groep B.V.

Europalaan 40, 3526 KS Utrecht
Postbus 8039, 3503 RA Utrecht
030 2 916 916
www.berenschot.nl
/berenschot