Cybercrisis bij gemeenten: Een verkennend onderzoek naar de voorbereidingen, ervaringen en uitdagingen

01-02-2021

S. (Sander) Ebbers, MSc
J. (Joyce) Koch, MSc MA
dr. J. (Jurjen) Jansen
dr. J. (Jelle) Groenendaal
dr. W. (Willem) Bantema
dr. E.R. (Rutger) Leukfeldt

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

NHL STENDEN hogeschool

Samenvatting

Aanleiding
Gemeenten zijn in hoge mate afhankelijk van digitale systemen. Als deze systemen onbedoeld uitvallen of aangevallen worden, kan dit grote gevolgen hebben voor de dienstverlening aan burgers en/of de interne bedrijfsvoering. Recente gevallen zoals de aanvallen op de gemeente Lochem (2019) en Hof van Twente (2020), en de Citrix-kwetsbaarheid (2019) hebben duidelijk gemaakt dat cyberincidenten grote impact kunnen hebben, niet te voorkomen zijn en zelfs kunnen uitmonden in een cybercrisis. Gemeenten moeten zich voorbereiden op cybercrises waarbij zij zelf het slachtoffer zijn.

Daarnaast kunnen gemeenten geconfronteerd worden met de fysieke gevolgen die ontstaan wanneer een organisatie gevestigd in de gemeente getroffen wordt door een cyberaanval. Denk hierbij aan een ziekenhuis dat door een aanval haar ICT niet meer kan gebruiken en daardoor de deuren moet sluiten. In een dergelijk geval zijn gemeenten betrokkenen en zullen zij samen met de veiligheidsregio('s) moeten acteren om de problemen in het fysieke domein aan te pakken.

In dit verkennende onderzoek gaan we nader in op het fenomeen cybercrisis binnen gemeenten waarbij we onderscheid maken tussen cybercrisis waarbij gemeenten (1) slachtoffer zijn of (2) betrokkene.

Onderzoeksdoelen en vragen
Cybercrises in het algemeen en binnen de gemeentelijke context in het bijzonder zijn nog maar beperkt beschreven in de (wetenschappelijke) literatuur. Het hoofddoel van het onderzoek is om inzicht te verschaffen in de ervaringen die gemeentelijke medewerkers hebben met cybercrisis als 'slachtoffer' en 'betrokkene' en hoe zij kijken naar de rollen en uitdagingen die er zijn.

Het hoofddoel is opgesplitst in twee hoofdvragen: (1) Welke uitdagingen ervaren gemeenten bij (de voorbereiding op) cybercrisis die de gemeentelijke organisatie raken? En (2) Welke uitdagingen ervaren gemeenten bij (de voorbereiding op) cybercrisis die plaatsvinden bij organisaties gevestigd in de gemeente en (kunnen) leiden tot problemen in het fysieke domein?

Methoden van onderzoek
Er is een literatuurstudie uitgevoerd die als basis heeft gediend voor semigestructureerde interviews. In de periode van 1 juli tot 1 december 2020 hebben 22 interviews plaatsgevonden met medewerkers van 18 verschillende gemeenten. Het merendeel van respondenten was werkzaam als Chief Information Security Officer (CISO) (N = 15), Adviseur Openbare orde en Veiligheid (AOV) (N = 9) en Adviseur informatiebeveiliging (N = 6).

Beantwoording hoofdvragen
De grootste uitdagingen voor gemeenten bij (de voorbereiding op) cybercrisis die de gemeentelijke organisatie raken zijn: (1) tijdens de warme fase verwacht men van de CISO soms een leidinggevende rol in plaats van de dagelijkse adviserende rol, (2) informatie gaat veelal sneller via informele kanalen dan via

de formele kanalen, (3) CISOs gebruiken de crisiskennis van AOV-ers onvoldoende (4) (voorbereiding op) cybercrisis is nog te veel een IT-feestje, (5) oefenen is belangrijk maar gebeurt nog te weinig, en (6) kleine gemeenten hebben geen draaiboeken of crisisplannen, grote gemeenten wel. Gemeenten hebben nauwelijks ervaring met cybercrises die de gemeentelijke organisatie raken.

De grootste uitdagingen voor gemeenten bij (de voorbereiding op) cybercrisis die plaatsvinden bij organisaties gevestigd in de gemeente zijn: (1) er is binnen gemeenten en veiligheidsregio's weinig cyber-expertise en kennis van de CISO wordt niet benut, (2) gemeenten worstelen met hun rol bij een dergelijke crisissituatie, (3) de rolverdeling tussen de gemeente en veiligheidsregio is onduidelijk bij een dergelijke crisissituatie, en (4) gemeenten vinden dat organisaties allereerst zelf verantwoordelijk zijn voor respons en mitigatie. Geen van de respondenten heeft ervaring opgedaan met een cybercrisis bij een organisatie gevestigd in de gemeente.

Conclusie

De *eerste* conclusie is dat gemeenten beperkt voorbereid zijn op cybercrisis en onvoldoende zicht hebben in hoeverre bestaande plannen en niet-geformaliseerde werkwijzen voldoende zijn om de impact van cybercrisis te kunnen beperken, mede omdat er niet wordt geoefend. De *tweede* conclusie is dat nog een wereld te winnen is bij een actievere samenwerking tussen CISOs en AOV-ers. De *derde* conclusie is dat deelnemende gemeenten nog geen ervaring hebben met cybercrisis waarbij ze enkel 'betrokkene' zijn.

De belangrijkste theoretische bijdrage is dat we geen aanwijzingen hebben gevonden dat de generieke literatuur over crisisbeheersing niet van toepassing zou kunnen zijn op cybercrisis.

Dit onderzoek is uitgevoerd onder een beperkt aantal gemeenten. Om een rijker en completer beeld te krijgen van cybercrisis bij gemeenten, adviseren we om een vervolgonderzoek uit te zetten bij meer gemeenten, bijvoorbeeld in de vorm van een vragenlijstonderzoek. Ander vervolgonderzoek zou zich kunnen richten op het meten van de mate van voorbereiding van gemeenten op cybercrisis, slimme manieren waarop gemeenten hun voorbereiding kunnen verbeteren en op cyberincident- en cybercrisisevaluaties.

Inhoud

1. Inleiding

1.1 Aanleiding onderzoek

Gemeentelijke organisaties zijn al geruime tijd in transitie naar digitale dienstverlening en bedrijfsvoering. De gemeente heeft een faciliterende rol in de ontwikkeling van zogenoemde *smart cities,* steden waarbij (nieuwe) informatietechnologie en digitalisering een centrale rol spelen in de aanpak van vraagstukken als klimaat, mobiliteit en gezondheid.[1] De coronacrisis heeft deze ontwikkeling versneld. Gemeenten hebben in korte tijd een groot deel van de (kritieke) processen moeten digitaliseren en thuiswerkfaciliteiten moeten uitrollen. De afhankelijkheid van digitale systemen neemt hiermee steeds verder toe en het aanvalsoppervlak voor cybercriminelen wordt groter. De groeiende hoeveelheid privacygevoelige data die de overheid verwerkt, brengt ook digitale dreigingen met zich mee. Deze dreigingen, in combinatie met de toegenomen afhankelijkheid, maakt dat de (potentiële) impact van cyberincidenten toeneemt.

Verstoringen en aanvallen kunnen de digitale dienstverlening en bedrijfsvoering van gemeenten urenlang of zelfs dagenlang platleggen. Gevoelige data van burgers kunnen worden gestolen of bewerkt en op grote schaal worden misbruikt door cybercriminelen. Het blijft echter niet altijd bij alleen dreigingen, dat laten de volgende twee voorbeelden zien.

Voorbeeld 1: Cyberaanval gemeente Lochem
In juni 2019 blijkt de gemeente Lochem getroffen te zijn door een geavanceerde cyberaanval. De gemeente ontdekte vreemde activiteit op het gemeentenetwerk en daarop werd op 13 juni 2019 besloten om alle dienstverlening die afhankelijk is van informatie- en communicatietechnologie (ICT) stil te leggen. De dienstverlening kon de week erna worden hervat, maar het heeft nog veel tijd gekost om te achterhalen wat de schade was. Na digitaal forensisch onderzoek bleek dat de aanvallers ruimschoots de tijd hadden genomen om de gemeente te infiltreren. De uiteindelijke kosten zijn door de gemeente geschat op € 200.000. Zoals uit het rapport van de gemeente Lochem blijkt, vond deze aanval niet doelbewust bij hen plaats, maar is misbruik gemaakt van een algemene kwetsbaarheid in een van de systemen. Dit had dus elke gemeente kunnen overkomen (De Winter, 2019).

Voorbeeld 2: Citrix-kwetsbaarheid
Citrix, een Amerikaans softwareprogramma dat toegang tot interne programma's en applicaties op afstand verschaft voor medewerkers van organisaties, meldde zelf op 17 december 2019 een lek (*exploit*) in de eigen software. Citrix kwam eind december en begin januari met aanbevelingen om het lek te dichten, en op 24 januari met een ronde updates met oplossingen (*patches*). Honderden Nederlandse organisaties maken gebruik van Citrix,

[1] G40 Stedennetwerk (2020). *Rijk en gemeenten moeten samen bouwen aan slimmere steden*. Verkregen via https://www.g40stedennetwerk.nl/nieuws/rijk-en-gemeenten-moeten-samen-bouwen-aan-slimmere-steden

waaronder een groot aantal gemeenten, en zijn kwetsbaar geweest voor cyberaanvallen en cyberspionage gedurende deze periode.[2]

Met andere woorden, de praktijk laat zien dat cyberdreigingen daadwerkelijk kunnen uitmonden in cybercrises. In dit verkennende onderzoek gaan we nader in op de aard en omvang van cybercrises binnen gemeenten, in hoeverre gemeenten zich voorbereiden op cybercrises, en welke uitdagingen gemeenten hierbij ervaren.

Cybercrisis

Een cybercrisis definiëren wij in dit onderzoek als een verstoring, uitval of misbruik van een gedigitaliseerd proces, (informatie)systeem of informatiedienst die de continuïteit, integriteit en/of vertrouwelijkheid bedreigt of ernstig verstoort en waarbij onder (een gevoel van) tijdsdruk en onzekerheid besluiten moeten worden genomen (zie ook par. 2.2).

Een gemeente kan op twee manieren betrokken raken bij een cybercrisis:

- Als **slachtoffer** wanneer door een cybercrisis de gemeentelijke (digitale) processen, systemen of diensten bedreigt of ernstig verstoort worden
- Als **betrokkene** wanneer een (publieke of private) organisatie binnen de gemeente geraakt wordt door een cybercrisis en bijvoorbeeld (fysieke) gevolgen ontstaan waarop de gemeente (en hulpdiensten) moet acteren.

Belang onderzoek

Cybercrisis(-management) is een nog relatief onontgonnen onderzoeksterrein, zeker in de context van gemeenten (VNG, 2019). Er is wel zicht op dreigingen, maar weinig zicht op de potentiële impact van cyberincidenten of cybercrisis op de reputatie van gemeenten. Ook is er geen consensus over een adequate crisisrespons, dan wel communicatiestrategie tijdens en na incidenten (VNG, 2019). Dit terwijl ook voor gemeenten veel op het spel staat. De ransomware-aanvallen op gemeente Lochem in 2019 (zie voorbeeld 1) en gemeente Hof van Twente[3] in 2020 illustreren dat gemeenten evengoed doelwit zijn voor cybercriminelen. Daarnaast trof het Citrix-lek begin 2020 een groot aantal gemeenten.
Het digitale verkeer en de digitale afhankelijkheid neemt toe, zeker ten tijde van het schrijven van dit rapport tijdens de coronapandemie.[4] Gemeenten hebben in korte tijd een groot aantal kritieke diensten moeten digitaliseren (Rathenau Instituut, 2020). Burgers zijn steeds vaker aangewezen op onlinedienstverlening van gemeenten en bewegen zich als consumenten ook vaker in cyberspace. Dit

---

[2] NOS (2020). *Lek bij Citrix actief gebruikt door hackers en spionne*n. Verkregen via https://nos.nl/artikel/2339151-lek-bij-citrix-actief-gebruikt-door-hackers-en-spionnen.html
[3] NOS (2020). *Gemeente Hof van Twente platgelegd door hacker*. Verkregen via https://nos.nl/artikel/2359142-gemeente-hof-van-twente-platgelegd-door-hacker.html
[4] WRR (2020). *Coronacrisis vraagt om debat over digitalisering*. Verkregen via https://www.wrr.nl/wrr-en-corona/artikel-coronacrisis-vraagt-om-debat-over-digitalsering

alles maakt dat het loont dat gemeenten nadenken over welke positie zij hierbij in willen nemen richting het beschermen van burgers en bedrijven, maar ook richting het beschermen van de (continuïteit van de) eigen ICT-infrastructuur.

Onderzoeksdoelen

De doelen van dit verkennende onderzoek zijn om inzicht te verschaffen in:

1) de aard, omvang en gevolgen van cybercrises waarbij gemeenten het primaire slachtoffer zijn en hoe zij zich hierop voorbereiden;
2) hoe gemeenten kijken naar hun rol bij een cybercrisis waarbij ze niet het primaire slachtoffer zijn (dat wil zeggen cybercrises die zich afspelen bij bedrijven of publieke instellingen gevestigd in de gemeente);
3) welke uitdagingen gemeenten ervaren bij de voorbereiding en response op cybercrises.

1.2 Hoofd- en deelvragen

Om de gestelde onderzoeksdoelen te verwezenlijken, hebben wij de volgende hoofdvragen geformuleerd.

Hoofdvragen

1) Welke uitdagingen ervaren gemeenten bij cybercrisis binnen de gemeentelijk organisatie?
2) Welke uitdagingen ervaren gemeenten bij cybercrisis bij organisaties gevestigd in de gemeente?

Om de hoofdvragen te beantwoorden, zijn onderstaande deelvragen geformuleerd.

Deelvragen

1. Wat verstaan gemeenten onder een cybercrisis?
2. In hoeverre en hoe bereiden gemeenten zich voor op cybercrises binnen de gemeentelijk organisatie?
3. Welke ervaringen hebben gemeenten met cybercrises binnen de gemeentelijk organisatie?
4. In hoeverre en hoe ziet de gemeente haar rol bij cybercrises bij organisaties gevestigd in de gemeente?
5. Welke ervaringen hebben gemeenten met cybercrises bij organisaties gevestigd in de gemeente?

1.3 Leeswijzer

In hoofdstuk 2 staat het theoretisch raamwerk voor dit onderzoek centraal. Daarin wordt voornamelijk ingegaan op de definities en vormen van cybercrises en de organisatie ervan. Vervolgens worden in hoofdstuk 3 de onderzoeksmethoden verantwoord. De resultaten worden besproken in hoofdstuk 4. Tot slot worden in hoofdstuk 5 de belangrijkste resultaten bediscussieerd en komen de beperkingen van het onderzoek aan bod. Ook bevat dat hoofdstuk antwoorden op onze onderzoeksvragen.

2. Theoretisch kader

In dit hoofdstuk worden de belangrijkste begrippen van dit onderzoek toegelicht. Allereerst presenteren we definities van crises en cybercrises in paragraaf 2.1 en 2.2. Vervolgens gaan we in op de hoedanigheid waarin crises zich voordoen (par. 2.3). In paragraaf 2.4 gaan we dieper in op de organisatie van cybercrises. Tot slot vatten we de belangrijkste uitkomsten van het theoretisch kader samen in paragraaf 2.5.

2.1 Definitie crisis

Een van de meest gangbare definities van crisis is geformuleerd door Rosenthal. Hij definieerde een crisis als '*een ernstige bedreiging van de basisstructuren of van de fundamentele waarden en normen van een sociaal systeem, welke bij een geringe beslissingstijd en bij een hoge mate van onzekerheid noopt tot het nemen van kritieke beslissingen*' (Rosenthal, 1984, p.25). Deze definitie omvat drie centrale begrippen die we ook bij andere definities in de literatuur hebben teruggevonden, namelijk (be)dreiging, onzekerheid en tijdsdruk (Ansell et al., 2010; Boin et al., 2017, 2020; Pauchant & Mitroff, 1992; Pearson & Clair, 1998; Pearson & Mitroff, 1993).

Een beperking van de definitie van Rosenthal is dat deze niet duidelijk maakt wat precies bedoeld wordt met 'de basisstructuren of fundamentele waarden en normen' in de context van een organisatie, zoals in ons onderzoek een gemeente. Voor dit onderzoek richten we ons daarom op definities van crisis in een organisatiecontext, ofwel organisatiecrisis.
Pearson en Clair (1998) definiëren een organisatiecrisis als *'een uitzonderlijke situatie of gebeurtenis met grote impact die door belanghebbenden wordt gezien als een bedreiging voor de levensvatbaarheid en integriteit van de organisatie'* (p.10). Volgens Pearson en Clair (1998) gaat het bij een organisatiecrisis dus om een dreiging die de levensvatbaarheid en integriteit van de organisatie en haar dienstverlening of producten in gevaar brengen.

2.2 Definitie cybercrises

Uit de literatuur blijkt dat de definitie van cybercrisis mede wordt bepaald door de wijze waarop de gemeente betrokken raakt bij een cybercrisis. Boeke (2018) laat dit terugkomen in een vergelijkend Europees onderzoek naar cybercrisismanagement. In bepaalde definities ligt de focus vooral op de *cyber*-component van crisis, dus dat een cybercrisis als het ware een bijzonder type crisis is, met daarbij de focus op maatschappelijke gevolgen. In deze definitie is gemeente hoofdzakelijk een *betrokkene*. Terwijl in andere definities met name wordt gesteld dat een cybercrisis een gemeentelijk informatiebeveiligingsincident is met potentieel maatschappelijk gevolgen. In dit geval is de gemeente hoofdzakelijk een *slachtoffer*.

Gemeente als betrokkene

Berenschot (2020) heeft in opdracht van de G4-gemeenten (Amsterdam, Rotterdam, Den Haag en Utrecht) een handreiking geschreven over cybercrisismanagement. In hun handreiking sluiten ze aan bij de definitie van cybersecurity zoals die in de Nederlandse Cybersecurity Agenda 2018 (NCTV,

2018, p.9) geformuleerd is: *'Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan'.* Met deze definitie van cybersecurity als basis hanteert Berenschot (2020) de volgende definitie van een cybercrisis: *'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*'.

Deze definitie legt de nadruk op maatschappelijke continuïteit, openbare orde en veiligheid en lijkt daarmee meer van toepassing op cybercrisis waarbij een gemeente betrokkene (in plaats van slachtoffer) is.

Gemeente als slachtoffer

Binnen de definitie waarin een gemeente als slachtoffer wordt getypeerd, staat een ernstige verstoring van de beschikbaarheid, integriteit en/of vertrouwelijkheid centraal.[5,6,7]

De oorsprong van deze definitie ligt in de wijze van afhandeling van informatiebeveiligingsincidenten, zoals bijvoorbeeld beschreven in normenkaders zoals de Baseline Informatiebeveiliging Overheid (BIO, Rijksoverheid, 2019, p78) welke wij in paragraaf 2.3 nader toelichten: *'Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatieverwerkende systemen…'*.

Op basis van deze omschrijving definiëren wij een cybercrisis met de gemeente als slachtoffer als *een verstoring, uitval of misbruik van een gedigitaliseerd proces, (informatie)systeem of informatiedienst die de beschikbaarheid, integriteit en/of vertrouwelijkheid bedreigt of ernstig verstoort en waarbij onder (een gevoel van) tijdsdruk en onzekerheid besluiten moeten worden genomen*.

Een cybercrisis zoals door ons gedefinieerd leidt dus in eerste instantie tot kritieke, urgente problemen binnen de organisatie die getroffen wordt en sluit daarbij aan bij de definitie van Pearson en Clair (1998, zie par. 2.1). Ook hebben wij in onze definitie het aspect van tijdsdruk en onzekerheid van Rosenthal (1984) overgenomen. Opgemerkt moet worden dat volgens onze definitie een cybercrisis al kan plaatsvinden zonder dat het grote maatschappelijke gevolgen heeft. Een interne cybercrisis kan overigens wel maatschappelijke gevolgen hebben en daarmee uitmonden tot een externe cybercrisis in het maatschappelijke domein.

> Voorbeeld: Een groot datalek bij een gemeente kan volgens onze definitie tot een cybercrisis leiden voor de gemeente. Bijvoorbeeld

[5] Beschikbaarheid: De mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers (van Houten, Spruit & Wolters, 2019).

[6] Integriteit: De mate waarin gegevens of functionaliteit juist en volledig zijn (van Houten et al., 2019).

[7] Vertrouwelijkheid: De mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn (van Houten et al., 2019).

doordat het lek leidt tot interne continuïteitsverstoringen. Het lek hoeft echter geen noodzakelijke gevolgen te hebben voor de maatschappelijke continuïteit of openbare orde en veiligheid wanneer (de impact van) het lek niet 'naar buiten slaat' en burgers beïnvloedt. In andere gevallen kan het wel leiden tot een externe cybercrisis, bijvoorbeeld wanneer door een verstoring uitkeringsgerechtigden hun uitkeringen niet ontvangen en massaal verhaal komen halen bij de gemeente.

Operationalisatie cybercrisis
Alles overziend kan een gemeente dus op twee manieren betrokken raken bij een cybercrisis:

- Als **slachtoffer** wanneer door een cybercrisis de gemeentelijke (digitale) processen, systemen of diensten bedreigt of ernstig verstoort worden
- Als **betrokkene** wanneer een (publieke of private) organisatie binnen de gemeente geraakt wordt door een cybercrisis en er bijvoorbeeld (fysieke) gevolgen ontstaan waarop de gemeente (en hulpdiensten) moeten acteren

2.3 Vormen van cybercrises

De gevolgen van een cybercrisis kunnen verschillende vormen aannemen. Het Instituut voor Veiligheids- en Crisismanagement (COT) heeft op pragmatische wijze de verschillende verschijningsvormen van een cybercrisis weergegeven.[8] Het COT maakt hierin een onderscheid tussen vier verschijningsvormen: (1) grootschalige en/of langdurige IT-uitval, (2) datalek persoonsgevoelige gegevens (medewerkers, klanten), (3) datalek bedrijfsgevoelige gegevens, en (4) onbetrouwbaarheid van (data)systemen. Deze verschijningsvormen zijn hieronder nader uitgewerkt.

Grootschalige en/of langdurige IT-uitval

Vrijwel alle vitale processen in Nederland zijn voor een groot deel, of volledig afhankelijk van ICT. Dit betekent dat grootschalige uitval van deze systemen een disruptief effect heeft op de gehele samenleving en dus zal uitmonden in een crisis. Deze problematiek wordt in de meest recente dreigingsbeelden op zowel nationaal (NCTV, 2020b; WRR, 2019) als lokaal niveau erkend (VNG, 2020).

Het is denkbaar dat een cyberaanval zorgt voor grootschalige IT-uitval, bijvoorbeeld als die gericht is op het elektriciteitsnet. Dit heeft te maken met het feit dat het elektriciteitsnet steeds 'slimmer' wordt, oftewel meer sensoren bevat die met het internet zijn verbonden. Deze sensoren zijn veelal ingericht op gebruiksvriendelijkheid (c.q. gemakkelijk gegevens uitlezen), maar minder op veiligheid (Otuoze et al., 2018). Deze dreiging wordt als reëel gezien in het meeste recente Cybersecuritybeeld Nederland (NCTV, 2020a).

[8] Kaouass en Zannoni (2017). *De veiligheidsregio en cyberagenda 2017-2020: voorbereid, betrokken en betrouwbaar.* Verkregen via www.linkedin.com/pulse/de-veiligheidsregio-en-cyberagenda-2017-2020-abderrahman-kaouass/?trk=v-feed

Tot nu toe hebben in Nederland nog geen ontwrichtende IT-verstoringen plaatsgevonden, maar wel hebben diverse gemeenten ervaring met kleinschalige IT-uitval van een aantal uur tot een aantal dagen. In 2019 kampte de gemeenten op Voorne-Putten met een grote ICT-storing en had de gemeente Amsterdam in een paar maanden tijd driemaal een grote ICT-storing. [9,10] Begin november 2020 was de dienstverlening van gemeente Hellendoorn een aantal dagen uit de lucht.[11] In al deze gevallen was de gemeente het slachtoffer van IT-uitval.

Een voorbeeld waarbij gemeenten betrokkene waren was bij de ransomware-aanval bij containerbedrijf Maersk in 2017. Ransomware is een vorm van malware die het voor gebruikers onmogelijk maakt om bij hun eigen data te komen, mits ze een losgeldsom betalen (Metropolitan Police Service, 2019). De cyberaanval op Maersk in de Rotterdamse haven zorgde voor grootschalige, langdurige IT-uitval bij Maersk, maar maakte de gemeente Rotterdam ook een betrokkene. Het containertransport kwam grotendeels stil te liggen en dit zorgde voor opstopping en lange files rondom de Rotterdamse haven. De gemeente Rotterdam had op dat moment geen goed beeld van de crisis bij Maersk en wist dus bijvoorbeeld ook niet hoe ernstig de situatie nog kon worden of wanneer het opgelost zou zijn (WRR, 2019).

Datalek persoonsgevoelige gegevens

Sinds de invoer van de Algemene Verordening Gegevensbescherming (hierna: AVG) in mei 2018 is een sterk groeiende aandacht voor datalekken van persoonsgegevens. Dit heeft grotendeels te maken met de 'meldplicht datalekken' die de AVG met zich meebrengt. Periodiek rapporteert de Autoriteit Persoonsgegevens (de toezichthoudende autoriteit voor verwerking van persoonsgegevens, hierna: AP) over de hoeveelheid gemelde datalekken. In 2019 zijn bij de AP 26.956 meldingen gedaan van potentiële datalekken. De top drie van sectoren die de meeste datalekken meldt bestaat uit (1) de financiële sector (30%), (2) de zorgsector (28%), en (3) het openbaar bestuur (17%).

Veelal gaat hierbij om een relatief onschuldig datalek waarbij een medewerker per ongeluk persoonsgegevens naar een verkeerde ontvanger stuurt. In ongeveer 3% van de gevallen gaat het om een datalek door hacking, malware (zoals ransomware), of phishing (AP, 2020).

Naast dat een datalek met persoonsgegevens financiële gevolgen kan hebben doordat de AP een boete kan opleggen, zorgen datalekken ook regelmatig voor reputatieschade. Dit lijkt zeker het geval wanneer het gaat over gevoelige

---

[9] Algemeen Dagblad (24 juni 2019). *Grote ict-storing bij gemeenten op Voorne-Putten verholpen*. Verkregen via https://www.ad.nl/voorne-putten/grote-ict-storing-bij-gemeenten-op-voorne-putten-verholpen~a2d99c64/

[10] Algemeen Dagblad (25 maart 2019). *Gemeente kampt opnieuw met ict-storing*. Verkregen via https://www.ad.nl/amsterdam/gemeente-kampt-opnieuw-met-ict-storing~a949a8c2/

[11] Tubantia (9 november 2020). *ICT-storing bij gemeente Hellendoorn, afdeling burgerzaken kan niets meer doen*. Verkregen via https://www.tubantia.nl/hellendoorn/ict-storing-bij-gemeente-hellendoorn-afdeling-burgerzaken-kan-niets-meer-doen~a0f44da5/

gegevens of gegevens over kwetsbare groepen burgers. Dit bleek bijvoorbeeld recent bij gemeente Apeldoorn, waar een datalek voor woede zorgde bij de betrokkenen. Bezwaarschriften rondom een woningbouwproject waren integraal doorgestuurd naar de projectontwikkelaar, inclusief namen en adressen. [12]

Een datalek bij gemeente Raalte in 2019 zorgde bij de betrokkene zelfs voor een vermeende mishandeling en diverse bedreigingen. De betrokkene tipte de gemeente in 2019 middels een brief op een mogelijk gevaar, waarbij hij de gemeente vroeg de tip vertrouwelijk te behandelen. Deze tip werd per ongeluk op het openbare deel van de website van de gemeente geplaatst. De briefschrijver stelde dat hij daardoor mishandeld en bedreigd werd.[13]

Datalek bedrijfsgevoelige gegevens

Het Nationaal Cyber Security Centrum (NCSC) spreekt in het Cybersecuritybeeld Nederland 2020 (NCTV, 2020a) van een grote dreiging en toename in digitale bedrijfsspionage die zich toespitst op overheidsorganen. Dit gebeurt steeds vaker door statelijke actoren; een actor die handelt uit naam van een nationale overheid. De doelen hierbij zijn onder andere om bedrijfsgevoelige gegevens te gebruiken om politiek voordeel te behalen, de eigen economische ontwikkeling te verbeteren, of om eventuele sancties te omzeilen. De Militaire Inlichtingen- en Veiligheidsdienst (MIVD) adviseerde medio oktober 2020 om smartphones niet in de buurt te hebben wanneer gevoelige zaken worden besproken. Zij adviseren dit omdat het als een reële kans wordt gezien dat Russen of Chinezen via smartphones spioneren.[14] Deze spionage kan veelal plaatsvinden omdat software bewust dan wel onbewust kwetsbaarheden bevat.

Het is niet bekend of dergelijke zaken zich bij gemeenten hebben voorgedaan, oftewel dat zij slachtoffer zijn geweest van bedrijfsspionage. Wel neemt de Vereniging Nederlands Gemeenten (VNG) de positie in van betrokkene. Dit blijkt bijvoorbeeld uit de Inventarisatie Cyberveiligheid die de VNG samen met het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) in 2017 publiceerde.[15] Deze inventarisatie moet gemeenten helpen om na te denken over hoe zij op gemeenteniveau en binnen gemeentegrenzen om willen gaan met deze dreigingen. De inventarisatie erkent de groeiende rol van cyberveiligheid in het veiligheidsdomein en benoemt daarbij ook digitale spionage (en de verkoop van

---

[12] De Stentor (27 Oktober 2020). *Woede in Ugchelen over datalek: gemeente Apeldoorn mailt namen bezwaarmakers naar projectontwikkelaar*. Verkregen via https://www.destentor.nl/apeldoorn/woede-in-ugchelen-over-datalek-gemeente-apeldoorn-mailt-namen-bezwaarmakers-naar-projectontwikkelaar~a771527f/

[13] RTV Oost (7 februari 202*0). Tipgever: 'Ik ben mishandeld na datalek gemeente Raalte*'. Verkregen via https://www.rtvoost.nl/nieuws/325522/Tipgever-Ik-ben-mishandeld-na-datalek-gemeente-Raalte

[14] BNR (12 oktober 2020). *MIVD: Leg je telefoon weg als je gevoelige zaken bespreekt*. Verkregen via https://www.bnr.nl/nieuws/technologie/10423500/mivd-leg-je-telefoon-weg-als-je-gevoelige-zaken-bespreekt

[15] VNG (22 december 2017). *Inventarisatie Cyberveiligheid geeft overzicht*. Verkregen via https://vng.nl/nieuws/inventarisatie-cyberveiligheid-geeft-overzicht

buitgemaakte [bedrijfs]informatie) als een voorbeeld waar gemeenten een visie op moeten ontwikkelen.

Onbetrouwbaarheid van (data)systemen

Sinds 1 januari 2019 is de Baseline Informatiebeveiliging Overheid (hierna: BIO) van kracht. Dit is een eenduidig informatiebeveiligingsnormenkader voor de gehele overheid. Betrouwbaarheid wordt binnen de BIO vertaald als 'integriteit'. Onbetrouwbaarheid is dus een inbreuk op de integriteit. Praktisch betekent dat een ongeoorloofde of onopzettelijke wijziging van gegevens heeft plaatsgevonden. Om toe te lichten wat dit betekent volgt nu een voorbeeld.

Het beste voorbeeld van een cybercrimevorm die veelal leidt tot een inbreuk op de integriteit is *malware*. Malware is kwaadaardige software die ervoor zorgt dat apparatuur of een systeem niet meer functioneert zoals het hoort te functioneren en waarbij mogelijk de data in het systeem niet meer correct zijn, gemanipuleerd zijn en daarmee onbetrouwbaar kunnen zijn (Domenie et al., 2013; Metropolitan Police Service, 2019). Bij de eerder genoemde cyberaanval op gemeente Lochem (zie par. 1.1) hebben cybercriminelen meerdere soorten malware geprobeerd te installeren die, gelukkig, niet succesvol waren, omdat de cybercriminelen onvoldoende rechten hadden (De Winter, 2019). Wanneer de acties wel succesvol waren geweest dan zou het in potentie mogelijk zijn geweest om uitkeringsinformatie of andere vertrouwelijke informatie van burgers te veranderen.

Een ander voorbeeld is een aanval waarbij cybercriminelen berichten onderscheppen en vervolgens aanpassen, de zogeheten man-in-the-middle-aanval (hierna: MITM; NCTV, 2020b). De bekendste MITM-aanval is de DigiNotar-hack in de zomer van 2011.[16] DigiNotar (een Nederlandse certificaatautoriteit) was daarbij gehackt en werd door de hacker gebruikt om valse SSL-certificaten uit te geven. SSL-certificaten zijn een beveiligingslaag op een website, die alleen uitgegeven mogen worden door een erkende autoriteit en die moet waarborgen dat gegevens die ingevoerd worden op een website niet (of met meer moeite) onderschept kunnen worden. Wanneer deze certificaten vals zijn is het mogelijk om een website te maken die legitiem lijkt, maar in feite malafide is.

2.4 De organisatie van cybercrisis

Nu gaan we in op de (cyber)crisisorganisatie. Kovoor-Misra (2009) stelt vijf fasen van crisismanagement vast; *prevention*, *preparation*, *containment*, *recovery* en *learning* (vrij vertaald: preventie, voorbereiding, inperking, herstel en leren). Pearson en Clair (1998) stellen dat crises en crisismanagement geen op zichzelf staande evenementen zijn, maar eerder langdurige processen met een lange aanloopfase en nazorgfase. Hiermee zien zij in feite preventie én voorbereiding als de voorbereidingsfase en herstellen én leren als de nazorgfase. Wij vatten de discussie daarom samen in drie fasen: (1) de voorbereidingsfase, (2) de acute

[16] Slate (21 december 2016). *How a 2011hack you've never heard of changed the internet's infrastructure*. Verkregen via https://slate.com/technology/2016/12/how-the-2011-hack-of-diginotar-changed-the-internets-infrastructure.html

responsfase, en (3) de nazorgfase. Deze zijn in de navolgende secties nader uitgewerkt.

2.4.1 Voorbereiden op (cyber)crises

Bij voorbereiding op (cyber)crises kijken we met name naar de maatregelen die organisaties nemen om voorbereid te zijn op een cybercrisis. Ansell et al. (2010), evenals Boin et al. (2016, 2020), stellen dat organisaties vaak noodprotocollen en crisisplannen hebben, maar dat in een werkelijke crisis wordt afgeweken van deze plannen, bijvoorbeeld omdat deze verouderd zijn of omdat er niet mee geoefend is. Ten tijde van een crisis moeten onder hoge tijdsdruk geld, goederen en middelen worden gemobiliseerd, en moet deze mobilisatie worden gecoördineerd. Organisationele wendbaarheid tijdens crisis is volgens Ansell et al. (2010) de heilige graal. Crisisresponsteams moeten worden getraind om wendbaar en dynamisch te kunnen reageren. Publieke organisaties zijn echter eerder geneigd tot regulatie en controle, en zijn daarmee minder wendbaar en dynamisch. Dat maakt waarschijnlijk dat publieke organisaties minder effectief een cybercrisis afhandelen (Pauchant & Mitroff, 1993; Smith & Elliott, 2007).

We weten dat digitale veiligheid een geprioriteerd thema is bij gemeenten (Stol & Bantema, 2020; VNG, 2019). De eerdergenoemde BIO biedt daarvoor een belangrijke basis. In de BIO wordt onder andere aandacht besteedt aan het voorbereiden op (interne) incidenten. In de BIO is benoemd welke acties, taken en verantwoordelijkheden de gemeente heeft in het geval van een incident (Rijksoverheid, 2019). In hoofdstuk 16 van de BIO wordt gesproken over de verantwoordelijkheden bij, rapportage van, beoordeling van, respons op en lering uit informatiebeveiligingsincidenten.[17] De doelstelling van de BIO hierbij is '*een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging*' (Rijksoverheid, 2019, p.63). In de BIO wordt overigens niet expliciet ingegaan op cybercrises. In het geval een incident leidt tot een crisis kan hulp worden ingeschakeld van het Computer Emergency Response Team (CERT[18]) van de Informatiebeveiligingsdienst (IBD; NCTV, 2020a). Daarnaast geven gemeenten handen en voeten aan de verantwoordelijkheid die voortvloeit uit de BIO door in beleid te benoemen zich voor te bereiden op cybercrises, noodplannen te schrijven en aan te geven te oefenen met cybercrisissimulaties (Stol & Bantema, 2020).

Wat betreft cybercrises die buiten een gemeentelijke organisatie maar binnen gemeentelijke grenzen plaatsvinden, waarbij de gemeente dus betrokkene zou kunnen zijn, zijn de verantwoordelijkheid en de daaruit voortvloeiende maatregelen onduidelijk. Het CCV heeft recent samen met de VNG een overzicht gemaakt van voorbeelden van veiligheidsproblemen met een digitale

[17] Dit is dus breder dan (cyber)crises.

[18] Een Computer Emergency Response Team (CERT) is een speciaal voor ernstige incidenten ingericht team dat werkt als een soort 'digitale brandweer' (Van Houten et al., 2019). Zie ook https://www.informatiebeveiligingsdienst.nl/ibd-cert/

component.[19] Dit geeft gemeenten inzicht in verschillende vormen van crises, maar geeft nog geen handvatten hoe hiermee om te gaan. Het is onduidelijk in hoeverre en op welke wijze de gemeente hierin een verantwoordelijkheid heeft. Op het niveau van veiligheidsregio's is deze verantwoordelijkheid beter geduid (Veiligheidsberaad, 2018).[20] Het is de vraag waar de verantwoordelijkheid van de gemeente eindigt en waar de verantwoordelijkheid van de veiligheidsregio begint bij een cybercrisis. Het is onduidelijk in hoeverre gemeenten bevoegd zijn te acteren bij cybercrises die zich voordoen bij organisaties gevestigd in de gemeente.

De meeste literatuur over cybercrisismanagement gaat over strategie op nationaal (Boeke, 2018; Collier, 2017; NCTV, 2019, 2020b) of regionaal niveau (IFV, 2020; Veiligheidsberaad, 2018). De inzichten van Collier (2017) zijn nog het beste toe te passen op strategisch keuzes op gemeentelijk niveau en zijn vanwege deze reden noemenswaardig. In die studie is een vergelijking gemaakt tussen de cybercrisis-aanpak van Estland en die van het Verenigd Koninkrijk. Vanuit deze vergelijking zijn een vijftal variabelen geformuleerd die invloed lijken te hebben op welke cybercrisisstrategie wordt gekozen. We benoemen in onderstaande opsomming deze variabelen en passen ze toe op gemeenten.

- Grootte: Is het een relatief grote gemeente en/of heeft het veel beschikbare financiële middelen? Hoe minder inwoners een gemeente heeft, hoe wendbaarder bij een crisis, maar ook hoe groter de afhankelijkheid van externe partners omdat de beschikbare middelen kleiner zijn.
- Geschiedenis: Heeft de gemeente ervaring met een cybercrisis? Hoe recenter de ervaring hoe groter de kans dat voorbereiding op een cybercrisis beleidsprioriteit heeft.
- Dreigingslandschap: Hoe evident zijn de cyberrisico's voor de gemeente of voor organisaties gevestigd in de gemeente? Hoe meer organisaties gevestigd in de gemeente behoren tot de vitale infrastructuur, hoe meer dreigingen er (waarschijnlijk) zijn.
- Politieke filosofie: in hoeverre ervaart de gemeente een zorgplicht voor de voorbereiding op een cybercrisis? En in hoeverre laat de gemeente dit over aan de markt? Hoe groter de ervaren zorgplicht bij cybercrisis, hoe groter de kans dat gemeente een proactieve rol inneemt als betrokkene bij cybercrisis.
- Digitale afhankelijkheid: In hoeverre zijn de diensten van de gemeente gedigitaliseerd? Hoe groter de digitalisering hoe groter de kans dat gemeenten ook een proactief cybercrisisstrategie hebben.

2.4.2 (Cyber)crisisrespons

Bij de responsfase kijken we naar de manier waarop een organisatie reageert op een cybercrisis. We kijken hierbij naar twee aspecten, namelijk: de organisatie van de crisisrespons en crisiscommunicatie.

---

[19] Het CCV (z.d.). *Cyberweerbaarheid gemeenten*. Verkregen via www.hetccv.nl/onderwerpen/cybercrime/cyberweerbaarheid-gemeenten

[20] Een veiligheidsregio zet zich in voor de veiligheid van de inwoners en bezoekers van de betreffende regio. Nederland kent 25 veiligheidsregio's (https://www.rijksoverheid.nl/onderwerpen/veiligheidsregios-en-crisisbeheersing/veiligheidsregios).

Organisatie van de crisisrespons

Uit de literatuur blijkt dat veel organisaties traditioneel een crisisorganisatie hebben die bestaat uit twee lagen: (1) de operationele laag en (2) de strategische laag. De *operationele laag* bestaat uit teams in de 'controlekamer' die te maken hebben met de directe bestrijding van een crisis vanuit hun specialisme; ook wel *first responders* genoemd die snel ter plaatse zijn en moeten (en kunnen) improviseren (Ansell et al., 2010; Boin et al., 2020). De *strategische laag* bestaat uit teams of personen in de 'bestuurskamer' die verder van de crisis staan maar verantwoordelijk zijn voor de crisisrespons en belangrijke beslissingen moeten nemen (Boin et al., 2020). Tijdens de responsfase dient te worden samenwerkt tussen beide lagen, maar aan deze wijze van organiseren zitten inherente problemen (Boin et al., 2020; Groenendaal et al., 2013; Smith & Elliott, 2007). Boin et al. (2020, p.21) spreken over een breukvlak tussen het operationele en strategische niveau, een *weeffout*:

'Beide niveaus hebben belangrijke maar heel verschillende taken, die alleen goed kunnen worden uitgevoerd wanneer iedereen samenwerkt. De samenwerking tussen het operationele en strategische niveau is een kritieke maar veelal onderschatte factor die de kwaliteit van grootschalige crisisrespons in hoge mate bepaalt. Het gaat hier om twee heel verschillende werelden waarin verschillende assumpties en prioriteiten domineren, de achtergronden van actoren sterk verschillen, evenals de taal en omgangsvormen'.

Volgens Boin et al. (2020) resulteert dit in een actieprobleem en een informatieprobleem. Het *actieprobleem* houdt in dat bestuurders vaak wel een idee hebben wat zij willen bereiken, maar niet weten hoe ze dit moeten doen. Om toch iets te doen storten zij zich op operationele werkzaamheden. Dit is een controlereflex en zorgt voor micromanagement. Tegelijkertijd zorgt dit voor frustratie bij de operatie. Het *informatieprobleem* houdt in dat de bestuurders vaak operationele informatie krijgen, terwijl zij met name behoefte hebben aan tactische/strategische informatie waarop zij strategische beslissingen baseren. De gedetailleerde operationele informatie is niet geschikt voor het nemen van strategische beslissingen. Zowel op strategisch als operationeel niveau wordt dit gegeven in stand gehouden, en dat gaat ten koste van de crisisrespons (Boin et al., 2020). Groenendaal et al. (2013) omschrijven dat gecentraliseerde aansturing tijdens noodsituaties vanuit het management moeilijk te bewerkstelligen is omdat het management de noodzakelijke en betrouwbare informatie over de situatie mist.

Zoals eerder aangegeven is digitale veiligheid een prioriteit bij gemeenten (VNG, 2019), maar het is de vraag in hoeverre dit leidt tot een gedegen gemeentelijke responsstrategie. Tot op heden is weinig bekend over *good practices* bij de respons op een cybercrisis op gemeentelijk niveau, zowel binnen de gemeentelijke organisatie als bij organisaties gevestigd in de gemeente. Een uitzondering hierop is een recente Noorse case-studie naar de organisatie van cybercrisismanagement bij incidenten die plaatsvinden bij organisaties gevestigd in de gemeente (Østby & Katt, 2020). In deze studie wordt gesteld dat het een vereiste is dat in de strategische, tactische en operationele cybercrisisorganisatie ICT-expertise aanwezig is, omdat reguliere crisismanagementrollen niet goed aansluiten bij de expertise die benodigd is. De suggestie van Østby en Katt (2020)

is om de gemeentelijke ICT-manager onderdeel te laten zijn van de responsorganisatie. Hoe deze ICT-rol specifiek moet worden vormgegeven wordt niet verder verduidelijkt in deze studie.

(Cyber)crisiscommunicatie

Een belangrijk onderdeel van crisisrespons is interne en externe crisiscommunicatie. Kim et al. (2017) stellen dat in de literatuur weinig aandacht is voor *cyber*crisiscommunicatie. Daarom putten we uit algemene literatuur over crisiscommunicatie.

Beldad et al. (2018) definiëren crisiscommunicatie als het verzamelen, verwerken en verspreiden van informatie die nodig is om een crisissituatie aan te pakken. Hierbij zijn verzamelen, verwerken en intern verspreiden van informatie onderdeel van de interne crisiscommunicatie, en het verspreiden van informatie naar derde partijen onderdeel van de externe crisiscommunicatie.

De externe communicatiestrategie als onderdeel van de crisisrespons speelt een belangrijke rol in het beschermen van stakeholders tegen schade en het beschermen van de reputatie van de organisatie (Coombs, 2007). Of zoals Regtvoort en Siepel (2014) het verwoorden: enerzijds communicatie als relatiemanagement en anderzijds communicatie als reputatiemanagement. Na een negatieve gebeurtenis gaan mensen op zoek naar oorzaken (Coombs, 2007). Wanneer een organisatie als schuldig wordt gezien heeft dit een negatieve impact op de reputatie van de organisatie, met alle gevolgen van dien. Smith en Elliott (2007) noemen dit de legitimiteitscrisis (*Crisis of Legitimation).* Volgens de situationele crisiscommunicatie theorie (*Situational Crisis Communication Theory)* van Coombs (2007) hangt de dreigende reputatieschade af van drie factoren: (1) de initiële verantwoordelijkheid voor de crisis, (2) de geschiedenis van crises bij de organisatie, en (3) de relationele reputatie van de organisatie voorafgaand aan de crisis. Organisaties moeten hun communicatiestrategie laten afhangen van die drie factoren. Jong (2019), in navolging van Coombs en Holladay (2010), en Coombs (2007) stellen dat organisaties in de crisisresponsfase drie externe crisiscommunicatiestrategieën volgen, soms in combinatie met elkaar; (1) ontkennen, (2) verzachten, en (3) accepteren.

Literatuur wijst uit dat de keuze voor acceptatie de minst schadelijke gevolgen heeft, mits een organisatie dit tijdig doet. Organisaties die deze strategie hanteren worden na crises hoger gewaardeerd op reputatie en vertrouwen dan organisaties die kozen voor het afwachten van berichtgeving van derden (Beldad et al., 2018; Boin et al., 2020). Bij deze proactieve communicatiestrategie *(stealing thunder)* beoogt de organisatie stakeholders snel te informeren en zelf het narratief van de crisis te bepalen (*framing).* Dat wil zeggen dat de organisatie zelf invloed wil hebben op het verhaal wat van binnen naar buiten de organisatie wordt gecommuniceerd over de crisis. Ook Østby en Katt (2020) raden op basis van hun onderzoek aan om deze proactieve communicatiestrategie te hanteren.

Organisaties kiezen er soms ook voor om te wachten met informatie delen, tot een derde partij de informatie naar buiten brengt. Deze reactieve strategie *(thunder)* geeft de media de kans om het narratief van de crisis te bepalen (Arpan & Pompper, 2003; Beldad et al., 2018; Boin et al., 2020; Coombs, 2014). Sociale media zorgen daarnaast voor dat informatie razendsnel kan verspreiden waarbij

iedere bron het narratief van de crisis kan beïnvloeden (Jong, 2019). Kim et al. (2017) ontkrachten de *thunder* en *stealing thunder* theorie enigszins in hun onderzoek naar cybercrises door datalekken. Zij stellen dat alhoewel tijdige communicatie vanuit de organisatie helpt bij het *framen* van crises, media niet altijd het narratief van de organisatie overnemen.

De gewenste strategie voor crisiscommunicatie (*stealing thunder*/proactief) wordt in de praktijk niet altijd gebruikt. Alhoewel bestuurders graag tijdig informatie willen delen met burgers en de media, moeten zij vaak wachten op informatie van onderzoeksteams of de Onderzoeksraad voor Veiligheid (OvV). Een te vroege of onjuiste boodschap kan volgens Jong (2019) het verschil betekenen tussen 'wachtgeld of een lintje' voor de desbetreffende bestuurder.

2.4.3 Herstel en nazorg na (cyber)crisis

Herstel en nazorg na een cybercrisis is een onderbelicht thema in de *cyber*crisisliteratuur. Ahmad et al. (2015) geven aan dat uit eerdere onderzoeken naar voren komt dat organisaties niet lijken te leren van cybercrisis. Een argument wat hier regelmatig wordt genoemd is het feit dat organisaties niet graag informatie delen over cybergerelateerde thema's, veelal vanwege de angst voor reputatieschade (Crossler et al., 2013; Enocson & Söderholm, 2018).
Omdat weinig onderzoek is gedaan naar 'leren van cybercrisis' richten we ons tot de algemene 'leren van crisis'-literatuur. Hierbij richten we ons op het lerend vermogen van organisaties na afloop van een crisis.

Leren van crises

Het uiteindelijke doel van het leren van crises is het doorgronden van de oorzaken van de crisis, en als organisatie voorbereid zijn om de impact van een volgende crisis te minimaliseren; van vatbaar voor crisis (*crisis-prone)* naar voorbereid op crisis (*crisis-prepared).* Ofwel om de (digitale) weerbaarheid van de eigen organisatie te verbeteren. Om dit te bewerkstellingen is een verandering nodig in zowel het gedrag als de opvattingen van mensen binnen de organisatie (Boin et al., 2020; Deverell & Hansén, 2009; Elliott, 2009; Pauchant & Mitroff, 1992).

Smith en Elliott (2007) beargumenteren dat alhoewel veel literatuur de veronderstelling bevat dat organisaties leren van crises, organisaties resistent lijken voor het leren van crises. Dit komt door een drietal barrières voor en misvattingen over (organisationeel) leren van crises. Allereerst worden crises aangegrepen als kansen (*windows of opportunity*) om beleidshervorming te bewerkstellingen waarvoor eerder geen urgentie was. Daarnaast hebben beleidstukken die worden gepresenteerd na een crisis weinig impact, omdat het vaak onduidelijk is op welke manier beleidstukken worden gecommuniceerd naar rest van de organisatie. Deze kennis blijft vaak op de oppervlakte. Het blijft dan bij 'eerste-orde leren' *(first order learning / single-loop learning)*, waarbij betrokken afdelingen leren van de ervaringen maar de rest van de organisatie daaruit geen lering trekt. Tot slot dient de nasleep van crises veelal tot het attribueren van schuld. Beleid dat volgt op dit proces heeft een 'geleerde lessen' karakter maar het doel is veelal niet organisationeel leren. Birkland (2009) noemt deze beleidstukken fantasiedocumenten (*fantasy documents*) en stelt dat deze veelal genegeerd worden en weinig leerzaam zijn.

Er wordt steeds meer opgeroepen om cybercrisiservaring te delen in vertrouwelijke context. In het meest recente Dreigingsbeeld Informatiebeveiliging van de VNG wordt bijvoorbeeld opgeroepen om *'beveiligingsincidenten en incidentenrapportage te delen met de Informatiebeveiligingsdienst (IBD), zodat de andere gemeenten hier ook van kunnen leren'* (VNG, 2018, p. 17). Dit is ook waartoe wordt opgeroepen in hoofdstuk 16 van de BIO 'Lering uit Informatiebeveiligingsincidenten' (Rijksoverheid, 2019). De VNG geeft op haar website ook handreikingen om invulling te geven aan deze norm uit de BIO. In deze handreiking valt op dat 'lering trekken uit' slechts beperkt blijft tot een interne evaluatie van een incident, met een evaluatierapport te gevolg. Binnen de openbaar beschikbare informatie van de VNG is geen leidraad gevonden voor het borgen van deze crisiskennis binnen de organisatie of het delen van deze kennis met andere gemeenten.

2.5 Resumé

Hieronder vatten we de kernpunten van het theoretisch kader samen. Deze kernpunten vormen de basis van het interviewprotocol dat werd gebruikt om medewerkers van gemeenten te interviewen. Daarnaast zijn de kernpunten ook startpunten voor vervolgonderzoek.

Definiëren cybercrisis

Het definiëren van een *cyber*crisis blijkt moeilijk, omdat dit onontgonnen terrein is binnen de wetenschap. Daarom zijn we aangewezen op definities uit literatuur over algemeen crisismanagement. Een handzame, breed gedragen definitie van cybercrises bij gemeenten ontbreekt momenteel.

Verschillende rollen gemeente bij cybercrisis

Een gemeente kan op twee manieren betrokken raken bij een cybercrisis:

- Als **slachtoffer** wanneer door een cybercrisis de gemeentelijke (digitale) processen, systemen of diensten bedreigt of ernstig verstoort worden
- Als **betrokkene** wanneer een (publieke of private) organisatie binnen de gemeente geraakt wordt door een cybercrisis en er bijvoorbeeld (fysieke) gevolgen ontstaan waarop de gemeente (en hulpdiensten) moeten acteren.

Consensus over de twee manieren waarop gemeenten betrokken raken bij een cybercrisis is er niet. Ook is nog niet duidelijk of gemeenten zichzelf ook zien als 'betrokkene' bij een crisis die zich niet afspeelt binnen de gemeentelijke organisatie, maar wel op gemeentegrond.

Het is onduidelijk welke verantwoordelijkheid en rol gemeenten hebben of kunnen innemen bij crises waarbij zij betrokkene zijn. De samenwerking tussen gemeentelijke Openbare Orde en Veiligheid (OOV) en bijvoorbeeld de Veiligheidsregio is niet duidelijk gedefinieerd. Het is de vraag waar de verantwoordelijkheid van de gemeente eindigt en waar de verantwoordelijkheid van de veiligheidsregio begint bij een cybercrisis. Het is onduidelijk in hoeverre gemeenten bevoegd zijn te acteren bij cybercrises die zich voordoen bij organisaties gevestigd in de gemeente.

Cybercrisisvoorbereiding
De BIO schrijft voor welke minimale set aan informatiebeveiligingsmaatregelen gemeenten geïmplementeerd moeten hebben (Rijksoverheid, 2019). Het woord crisis wordt niet in de BIO genoemd. Wel bevat de BIO richtlijnen voor de inrichting van cyber-incidentmanagement. Gemeenten zijn verplicht om de BIO te implementeren, maar kunnen uiteraard aanvullend hierop maatregelen voor bijvoorbeeld cybercrisis nemen. We hebben hierover geen literatuur gevonden. Het is onduidelijk of de BIO goed aansluiting vindt bij crisisstructuren. Ook is op basis van de BIO onduidelijk of samenwerking wordt verondersteld tussen de IT-afdeling, de gemeentelijke CISO én traditionele gemeentelijke crisisafdelingen zoals OOV.

Cybercrisisrespons
Tijdens de crisisrespons werken twee 'lagen' samen; de operationele laag van *first responders*, die crises bestrijden vanuit hun specialisme, en de strategische laag van bestuurders die beslissingen moeten nemen en verantwoordelijkheid dragen. Hierin identificeert de literatuur verschillende uitdagingen: niet dezelfde taal spreken, te veel *micro managen* en teveel operationele informatie op strategisch niveau. Het is onduidelijk of gemeenten deze problemen ervaren in de cybercrisisrespons. Er zijn daarnaast weinig *good-practices* te vinden voor cybercrisisrespons in het algemeen, en cybercrisisrespons bij Nederlandse gemeenten in het bijzonder.

Literatuur wijst uit dat qua externe communicatie, een organisatie het best kan accepteren dat het getroffen is door een crisis en daarbij zelf naar buiten komt en daarmee het narratief van de crisis bepaalt (deze aanpak heet *stealing thunder*). Organisaties met een dergelijke aanpak worden na een crisis meer vertrouwd en ervaren minder reputatieschade dan organisaties die kiezen voor ontkennen of verzachten. De beperkte voorbeelden die we kunnen vinden voor gemeenten wijzen uit dat de meeste gemeenten de *stealing-thunder* strategie hanteren. Dit aantal is echter te klein om te kunnen generaliseren.

Nazorg
Organisaties lijken huiverig om ervaringen te delen uit angst voor reputatieschade. Gemeenten worden wel opgeroepen (in de BIO) om incidentenrapportages te delen (met de IBD), zodat andere gemeenten hiervan kunnen leren. Deze rapportages blijven echter vaak beperkt tot incident-evaluaties. Uit de literatuur komt niet naar voren hoe gemeenten omgaan met dergelijke incidentrapportages, op welke wijze zij die vormgeven, en op welke wijze die worden uitgedragen binnen de gemeente.

3. Methode

In dit hoofdstuk staat de onderzoeksmethode centraal. Om antwoord te geven op de onderzoeksvragen zijn semigestructureerde interviews afgenomen onder medewerkers van Nederlandse gemeenten. Deze methode stelt ons in staat om op kwalitatieve wijze een beeld te krijgen van cybercrisisproblematiek bij gemeenten en de uitdagingen die gemeenten daarbij ervaren. De functies die zij vertegenwoordigen zijn uitgewerkt in paragraaf 3.1. De procedure en uitvoering worden verderop in dit hoofdstuk besproken onder paragraaf 3.2. Het interviewprotocol is gebaseerd op de hoofd- en deelvragen en de uitkomsten uit de literatuurstudie. De opzet van de semigestructureerde interviews is te vinden in bijlage A.

3.1 Respondenten

Om een zo volledig en betrouwbaar mogelijk beeld te krijgen op het thema cybercrisis bij gemeenten is voor dit onderzoek gesproken met gemeentemedewerkers met verschillende expertisegebieden en rollen. In dit onderzoek waren dat (Chief) Information Security Officers (CISO/ISO), adviseurs Openbare Orde en Veiligheid (AOV), adviseurs Informatiebeveiliging (AIB), burgemeesters en in een enkel geval met een communicatieadviseur of coördinator van de Servicedesk (zie tabel 1).

We lichten hieronder kort toe wat de rollen inhouden en wat de (vermeende) relatie is met het thema cybercrisis:

- CISO/ISO: de CISO heeft een controlerende en adviserende rol op het gebied van informatiebeveiliging. Bij een cyberincident of cybercrisis kan de CISO optreden als adviseur van de bestuurders of van het crisisteam, of als onderdeel van een CERT. De ISO ondersteunt de CISO in zijn/haar werkzaamheden.
- AOV: de AOV adviseert gemeentelijke bestuurders op het gebied van veiligheid- en crisisvraagstukken met een openbare orde en veiligheidscomponent en zou dus ook een rol moeten hebben bij cybercrisis met een OOV-component.
- AIB: de AIB adviseert veelal over een specifiek informatiebeveiligingsthema (bijv. incidentmanagement of cloudsecurity), rapporteert hierbij aan de CISO en kan bij cybercrisis als adviseur optreden. Meestal is deze functie ingericht bij grotere gemeenten, of binnen samenwerkingsverbanden van meerdere gemeenten.
- Burgemeester: de burgemeester is belast met de handhaving van de openbare orde en veiligheid, waaronder cybercrisis met een openbare orde component.
- Communicatieadviseur: de communicatieadviseur heeft als taak om bestuurders te adviseren hoe de gemeente naar burgers en bedrijven moet communiceren over een (cyber)crisis.
- Coördinator Servicedesk: interne incidenten komen over het algemeen als eerste binnen bij een Servicedesk. De coördinator Servicedesk is, vaak samen met de CISO, betrokken bij opschalingsbeslissingen van cyberincident naar cybercrisis.

We hebben in de interviewuitnodiging verzocht in ieder geval de CISO en de adviseur OOV te betrekken. Beide rollen lijken de spin in het web lijken te zijn bij interne crisis (CISO), dan wel externe crisis (AOV). De uiteindelijk respons is te vinden in tabel 1.

Er is gesproken met vijftien CISOs, negen AOV-ers, zes AIB-ers, twee burgemeesters, één communicatieadviseur en één coördinator Servicedesk. De mogelijke implicatie van deze verdeling benoemen wij in de discussie (zie par. 5.3). Deze gemeentemedewerkers vertegenwoordigen samen achttien gemeenten.

Tabel 1. Overzicht respondenten

Functie / Gemeente	CISO /ISO	AOV	AIB	Burge-meester	Com. Adv.	Co. Service desk
1	I		I			
2	I					
3	I		I			
4	I	I	I			
5	I	I				
6	I					I
7	I	I				
8	I	I				
9		I				
10	I					
11	I	I			I	
12	I	I				
13	I					
14	II	I				
15			I			
16				I		
17	I	I	I	I		
18			I			
Totaal	**15**	**9**	**6**	**2**	**1**	**1**

3.2 Procedure en uitvoering

In de periode van 1 juli 2020 tot 1 december 2020 zijn 22 semigestructureerde interviews afgenomen met 34 personen, verdeeld over achttien gemeenten.
De deelnemende gemeenten lagen verspreid over heel Nederland en bestonden uit zowel kleine (< 100.000 inwoners) als grote (> 100.000 inwoners) gemeenten. Medewerkers van de aangeschreven gemeenten zijn persoonlijk uitgenodigd via telefoon of e-mail en komen in alle gevallen uit het netwerk van het onderzoeksteam. In de meeste gevallen is positief gereageerd op deze uitnodiging. Slechts in drie gevallen wilde men niet deelnemen. Hierbij werd als

reden opgegeven dat er geen ruimte was in de agenda's of dat de aangeschreven medewerker van mening was weinig te kunnen bijdragen aan het onderzoek omdat cybercrisis nog geen actief thema was binnen de desbetreffende gemeente.

De (groeps-)interviews duurden ongeveer een uur. Door toedoen van COVID-19 maatregelen (beperken contactmomenten en reisbewegingen) hebben we de interviews op digitale wijze afgenomen (via Microsoft Teams). Voorafgaand aan de interviews is toestemming gevraagd om deze op te nemen voor verwerkingsdoeleinden. De interviewkandidaten hadden daar geen bezwaar tegen. De interviews zijn verwerkt in een gespreksverslag en vervolgens ter validering voorgelegd aan de respondent. Na de verwerking van het interview zijn de opnames verwijderd.

Voor de uitwerking van de interviewresultaten zijn de deelnemende gemeenten gepseudonimiseerd. We hebben gekozen voor pseudonimisering zodat in het onderzoeksverslag de privacy van de respondenten in zekere mate geborgd is.

4. Resultaten interviews

In dit hoofdstuk staan de uitkomsten van de interviews centraal. Het resultatenhoofdstuk volgt de structuur van de deelvragen en hiermee ook grotendeels de structuur van het gehanteerde interviewprotocol. Allereerst hebben we de vraag gesteld wat gemeenten verstaan onder een cybercrisis (par. 4.1). Vervolgens hebben we gevraagd hoe gemeenten zich voorbereiden op een cybercrisis binnen de gemeentelijke organisatie (par. 4.2), welke ervaringen gemeenten hebben met dergelijke cybercrisis (par. 4.3) en welke uitdagingen gemeenten hierbij ervaren (par. 4.4). Daarna bespreken we de rol van de gemeente bij cybercrisis bij organisaties gevestigd binnen de gemeentegrenzen. Allereerst hebben we gevraagd in hoeverre gemeenten hierin een rol voor henzelf zien weggelegd en, zo ja, hoe deze rol er dan uit zou moeten zien (par. 4.5). Vervolgens hebben we gevraagd naar eventuele ervaringen (par. 4.6) en uitdagingen (par. 4.7) die gemeenten ervaren bij de omgang met cybercrisis bij organisaties gevestigd binnen de gemeentegrenzen.

We verwijzen in de resultaten naar rollen (en niet naar namen) van geïnterviewde gemeentemedewerkers en differentiëren waar mogelijk tussen uitkomsten van grote dan wel kleine gemeenten.

4.1 Wat verstaan gemeenten onder een cybercrisis?

Zoals aangegeven is er gesproken met experts die verschillende rollen spelen bij een cybercrisis in een gemeente. We hebben eenieder gevraagd om zijn of haar definitie te geven van ‘cybercrisis’. Uit de interviews blijkt dat gemeenten onderscheid maken tussen cybercrises waarbij de gemeente primair het slachtoffer is of ‘slechts’ een van de betrokkenen (en bijvoorbeeld moet acteren op de openbare ordeverstoringen die zijn ontstaan wanneer een organisatie in de gemeente wordt geraakt door een cybercrisis).

10 van de 18 geïnterviewde gemeenten geven aan dat zij het begrip cybercrisis niet gebruiken en dat het ook niet formeel gedefinieerd is in planvorming. Alle CISOs geven aan dat zij een cybercrisis intuïtief definiëren als een groot incident waarbij de beschikbaarheid, vertrouwelijkheid en/of integriteit van een of meerdere gedigitaliseerde gemeentelijke processen mogelijk bedreigt of verstoord wordt. Deze definitie lijkt daarmee vooral uit te gaan van de gemeente als slachtoffer.

Wat men verstaat onder ‘een groot incident’ is bij twaalf gemeenten niet vastgelegd en verschilt per CISO. Zes gemeenten geven aan gebruik te maken van een opschalingstabel.[21] In een dergelijke tabel wordt afhankelijk van het type en de omvang van een incident beschreven hoe het afgehandeld moet worden.

[21] Voor een voorbeeld zie bijlage 3 van het ‘voorbeeld incidentmanagement- en respon-sebeleid’ van de IBD. Verkregen via https://www.informatiebeveiligingsdienst.nl/pro-duct/voorbeeld-incidentmanagement-en-response-beleid-2/

Voor de geïnterviewde AOV-ers (en in navolging ook de burgemeesters) is een cybercrisis in feite hetzelfde als een 'traditionele crisis', zoals een overstroming of brand, maar dan met de oorsprong in het digitale domein. Daarbij geven zij aan dat de gemeente primair verantwoordelijk is voor de bestrijding van de (veelal fysieke) gevolgen van de cybercrisis wanneer die impact heeft op burgers.

> *'Een definitie van een (externe) crisis of incident is; een crisis of incident die potentieel ontwrichtend is voor de inwoners of samenleving en die potentieel vitale infrastructuren raakt, waarbij er meer dan een enkele partij nodig is om het probleem op te lossen' (AOV, G6).*

Of de gemeente slachtoffer is of betrokkene lijkt hierbij minder uit te maken. In beide gevallen gaat het erom dat de openbare orde en veiligheid wordt bedreigd. Wat vanuit AOV-perspectief een cybercrisis bijzonder maakt is dat de oorzaak lastig te achterhalen kan zijn; dit in tegenstelling tot de meeste traditionele crises. Hiermee zien zij een cybercrisis als een 'bijzonder' type crisis. De AOV-ers geven aan dat zij veel samenwerken met de veiligheidsregio's, maar daar is (ook) nog weinig kennis over cybercrisis. Veiligheidsregio's typeren cybercrisis volgens hen als een nieuw type crisis.

> *'De kennis van de veiligheidsregio op het gebied van cyber is minimaal en voegt tijdens een cybercrisis nu niks toe. De veiligheidsregio moet bij diens klassieke taak blijven; het bestrijden van een crisis die naar buiten slaat. Schoenmaker blijf bij je leest' (CISO, G6).*

4.2 In hoeverre en hoe bereiden gemeenten zich voor op cybercrises?

Cyberincident- en crisisorganisatie

Als we kijken naar de voorbereiding van gemeenten op cybercrises is een tweedeling zichtbaar tussen kleine (<100.000 inwoners) en grote (>100.000 inwoners) gemeenten. Kleinere gemeenten hebben nauwelijks planvorming op het gebied cybercrisismanagement. Hun voorbereiding bestaat uit de implementatie van de BIO waarin een aantal vereisten staan met betrekking tot incidentmanagement en informatiebeveiligingsaspecten binnen bedrijfscontinuïteit. Zoals beschreven in het theoretisch kader kent de BIO geen specifieke vereisten voor cybercrisis.

Kleine gemeenten (<100.000)

Bij de negen kleine gemeenten, die zijn betrokken bij dit onderzoek, is het in de regel als volgt georganiseerd: alle incidenten – van klein (zoals één besmette computer door een keylogger[22]) tot groot (zoals een ransomware aanval) – komen binnen bij een servicedesk. Na de melding maakt de servicedeskmedewerker een risico-inschatting en schaalt eventueel op naar de IT-manager of CISO. Deze gemeenten beschikken dus niet over vastgelegde

[22] Een keylogger is software die toetsaanslagen opslaat waarmee een crimineel aan inloggegevens van computergebruikers kan komen. Verkregen via https://www.politie.nl/themas/keylogger.html

criteria waarmee ze op gestandaardiseerde wijze de aard, impact en aanpak van incidenten kunnen bepalen. Hier ligt geen draaiboek, maar een professioneel oordeel van een IT-manager, proceseigenaar of CISO aan ten grondslag. CISOs van drie kleine gemeenten geven aan dat zij ook geen behoefte hebben aan draaiboeken.

> *'Belangrijk is dat de juiste mensen de juiste informatie hebben, en mandaat. Die mensen kennen de stappen die zij moeten nemen' (CISO, G5).*

Een enkele kleine gemeente maakt gebruik van een beslismodel in de vorm van een stroomschema bij incidentmeldingen.

Grote gemeenten (>100.000)
De negen grote gemeenten hebben een (semi) geformaliseerd incidentmanagementproces. Vijf grote gemeenten geven aan gebruik te maken van de handreikingen van de IBD als het gaat om cybercrisisvoorbereiding. Een CISO stelt te beschikken over een ICT-calamiteitenplan, maar stelt ook;

> *'Een echt cybercrisisplan ontbreekt' (CISO, G4).*

Vier grote gemeenten hebben een globaal incidentendraaiboek. In de incidentdraaiboeken wordt bijvoorbeeld beschreven hoe een incident kan escaleren tot een crisis, hoe de crisisorganisatiestructuur eruitziet en wat de taken en verantwoordelijkheden van de verschillende actoren zijn tijdens een crisis. Eén van deze gemeenten geeft aan dat dit incidentendraaiboek alleen is gemaakt voor incidenten omtrent datalekken. Slechts twee grote gemeenten geven aan een specifiek cybercrisisdraaiboek te hebben. Bij één van deze twee gemeenten is dit draaiboek vooral gericht op het herstellen van gegevens en de continuïteit van de kritieke processen.

Een enkele grote gemeente geeft aan bewust een draaiboek te hebben voor kleine incidenten, maar niet voor grote incidenten.

> *'Goed crisismanagement hangt af van goede mensen met mandaat, niet van een draaiboek' (CISO, G2 en G3).*

> *'Gemeenten zijn goede brandweermannen. Als het crisis is dan zijn de lijntjes kort en wordt het gefixt. Als het crisis is heb je geen tijd om een draaiboek van vijftig pagina's door te lezen. De gemeente zou wel meer mogen nadenken over voorbereiding' (CISO, G10).*

Ook bij grote gemeenten komen incidenten in de regel binnen via de servicedesk. De geïnterviewde gemeenten geven aan dat de servicedesk een eerste beoordeling maakt en vervolgens de eerste acties uitzet. Bij een 'groter' incident schakelen zij de CISO in. De CISO of Securitymanager kan vervolgens een CERT bijeenroepen, aldus verschillende geïnterviewden. Dit team bestaat veelal uit een IT-manager, de CISO en soms afgevaardigden van betrokken of getroffen gemeentelijke afdelingen. Zij houden zich in eerste instantie bezig met het inperken van de crisis, de zogenoemde *containment*. Als de impact groot genoeg is, kan ook een gemeentelijk crisisteam worden geformeerd. Op dat moment

wordt samenwerking gezocht met de algemene crisisorganisatie van een gemeente.[23] Die samenwerking is overigens niet vanzelfsprekend en wordt tijdens de koude fase (i.e. de fase vóór de crisis) nauwelijks opgezocht binnen gemeenten.

De CISO is de *linking pin* tussen het CERT en het gemeentelijk crisisteam, al is de CISO niet altijd lid van het CERT zelf. De rol van de CISO verschilt per gemeente. Soms is de CISO voorzitter van het CERT, soms wordt de CISO niet direct betrokken maar informeert die zijdelings. In de meeste gemeenten, waar we interviews hebben afgenomen, heeft de CISO mandaat om processen in de warme fase (i.e. de fase waarin de crisis gaande is) van een crisis stil te leggen. Dit gebeurde bij een aantal gemeenten tijdens bijvoorbeeld het Citrix-lek.

> *'Als puntje bij paaltje komt, heb ik mandaat om bepaalde dingen te doen, maar je probeert in gemeenschappelijkheid beslissingen te nemen' (CISO, G6).*

Een enkele gemeente ervaart wel dat dit mandaat later ter discussie kan komen te staan. Achteraf wilden bestuurders en afdelingsmanagers goed uitgelegd krijgen waarom zij soms gepasseerd zijn tijdens de warme fase.

> *'Ik merk dat ik nu knopen doorhak en beslissingen neem, met in mijn achterhoofd dat als die verkeerd blijken te zijn, dat ik dan altijd nog sorry kan zeggen. Dat wordt dan geaccepteerd' (CISO, G4).*

Oefeningen

Gemeenten gaan op dit moment zeer divers om met het oefenen van cybercrises. Negen van de achttien gemeenten geven aan op dit moment niet te oefenen met cybercrisisscenario's. De gemeenten die hebben geoefend of van plan zijn om te gaan oefenen doen dit (nog) niet op structurele basis.
Vanuit welke achtergrond geoefend wordt verschilt ook sterk:

- Een enkele gemeente geeft aan dat cybercrisisoefeningen vanuit de AOV worden georganiseerd, zonder een betrokken CISO.
- Twee gemeenten geven aan de ambitie te hebben om mee te doen aan een cybercrisisoefening zoals de VNG Cybergame.[24]
- Twee gemeenten oefenen op kleine schaal met eigen cybercrisisoefeningen binnen de gemeente, zonder dat hierbij alle bestuurslagen meedoen.

[23] De algemene crisisorganisatie bestaat minimaal uit de burgemeester, gemeentesecretaris, CISO, AOV, en Adviseur Communicatie. Zie ook: https://vng.nl/artikelen/interactieve-cyberoefening

[24] De VNG Cybergame is crisisgame voor gemeentebestuurders en ambtenaren. Gemeenten kunnen zich sinds 31 oktober 2019 hiervoor aanmelden. Zie ook https://vng.nl/nieuws/nieuwe-cybergame-officieel-gelanceerd

- Twee gemeenten hebben een grootschalige cybercrisisoefening ondernomen waarbij alle lagen van de gemeente mee oefenden. Deze oefening is uitgevoerd binnen een GRIP-3 structuur.[25] Bij één van deze gemeenten viel deze oefening gedeeltelijk in het water door COVID-19.

Enkele gemeenten hebben inmiddels meegedaan met een landelijk georganiseerde crisisoefening. De meningen over deze oefening verschillen. Sommige gemeenten waren er blij mee dat eindelijk gestructureerd geoefend is, terwijl andere gemeenten de oefening als 'te licht' ervoeren.

De interviews laten verder zien dat bij vrijwel alle gemeenten het bewustzijn er is dat meer oefening met cybercrisisscenario's zou moeten plaatsvinden.

> *'We zijn nu niet beoefend genoeg in het afhandelen van cybercrises. De veiligheidsregio beoefent crises bij de vleet, wij zouden dat voor cyber ook moeten doen' (AOV, G6).*

> *'Dit zeggen de boekjes natuurlijk al jaren; doe BCM (bedrijfscontinuïteitmanagement) en crisisoefeningen. Maar niemand doet dat. Dit komt omdat we het allemaal lastig vinden. Er zijn wel middelen beschikbaar maar niet altijd binnen gemeenteland. Dit heeft de afgelopen jaren te weinig aandacht gehad. Dan kun je als CISO roepen dat we moeten oefenen, maar de bestuurders hebben het druk' (CISO, G13).*

Ondanks dat de wens bij sommige gemeenten aanwezig is heeft herhaaldelijk oefenen nog niet plaatsgevonden. Het lijkt erop dat gemeenten nog zoekende zijn hoe zij invulling kunnen geven aan het oefenen ten tijde van COVID-19. In sommige interviews werd aangegeven dat een cybercrisisoefening wel gepland stond, maar dat maatregelen door toedoen van COVID-19 hiervoor een belemmering waren en voor uitstel zorgden.

Prioritering

Volgens het overgrote deel (11) van de CISOs staat cyberveiligheid voldoende hoog op de gemeentelijke agenda. De gemeenten die mee hebben gewerkt geven aan dat het thema cyberveiligheid binnen de meeste gemeenteraden en colleges van Burgemeester & Wethouders hoog op gemeentelijke agenda staat. Er wordt hier dan voornamelijk gesproken over informatiebeveiliging, niet over cybercrises. Zij ervaren dat vanuit de gemeente middelen en tijd worden vrijgemaakt. De CISOs van twee gemeenten geven aan dat met name prioriteit komt voor cyberveiligheid bij urgentie, dus wanneer elders in het land een

[25] GRIP staat voor Gecoördineerde Regionale Incidentbestrijdingsprocedure. Dit is de standaardaanpak bij crisisbeheersing met een openbare orde component. Er zijn diverse GRIP-niveaus. GRIP-3 betreffen situaties waarbij sprake is van (dreigende) maatschappelijke onrust.

cyberaanval aan het licht komt. Hierbij worden Maastricht University[26] en de cyberaanval op de gemeente Lochem (zie par. 1.1) veelal genoemd als casus.

> *'In de warme fase krijg ik iets makkelijk op de agenda bij het GMT[27] of de wethouder. In de koude fase moet ik echter flink aandikken wil ik iets op de agenda krijgen' (CISO, G4).*

De Citrix-kwetsbaarheid (zie par. 1.1) heeft bij veel CISOs ervoor gezorgd dat voorbereiden op cybercrises hoger op de agenda staat (zie ook par. 4.3). De grootschalige IT-uitval zorgde bij een gemeente voor dat cybersecurity bij veel afdelingsdirecteuren een belangrijk thema is geworden. De CISO geeft aan hier wel een knelpunt te ervaren. Deze directeuren hebben weinig IT-kennis en wensen zo min mogelijk uitvaltijd van systemen, maar hebben geen idee van de financiële implicaties van dergelijke wensen voor systemen.

Crisiscommunicatie

Acht van de negen gemeenten die wij gevraagd hebben of er een communicatiestrategie is met betrekking tot cybercrisis geven aan dat deze strategie er niet is.[28] Vijf gemeenten geven aan dat zij verwachten transparantie te zullen nastreven tijdens een incident. Dat wil zeggen dat zij zoveel mogelijk openheid willen geven over wat ten grondslag ligt aan de cybercrisis (bijv. een cyberaanval, of een fout). Een CISO van twee gemeenten geeft aan dat politieke sensitiviteit zal bepalen op welke wijze gecommuniceerd wordt. Vier gemeenten geven aan huiverig te zijn met het delen van (te veel) informatie, omdat hiermee potentiële kwetsbaarheden worden prijsgegeven.

> *'Onze rapporten naar de gemeenteraad en dergelijke worden openbaar gemaakt. Welke bijlage van zo'n rapport stuur je naar de raad en welke informatie stuur je onder embargo? We streven naar transparantie, maar niet ten koste van de veiligheid' (CISO, G13).*

> *'Als een incident alleen intern impact heeft en niet op straat ligt, waarom zou je er dan over gaan communiceren? Dat zorgt voor meer onrust (….) Je kunt mensen ook op ideeën brengen' (AOV, G6).*

Slechts één gemeente geeft aan een vooropgestelde communicatiestrategie te hebben. Een andere gemeente schetst de keerzijde van transparantie te hebben ervaren. De CISO geeft aan dat diens gepubliceerde jaarverslag voor de gemeenteraad werd opgepikt door een lokaal dagblad en gepubliceerd onder een sensationele kop.

---

[26] Op 15 oktober 2019 werd Maastricht University besmet met ransomware. De aanvallers eisten 197.000 euro losgeld. Zie ook: https://www.security.nl/posting/642452/Universiteit+Maastricht+werd+besmet+via+phishingmail+en+verouderde+software

[27] GMT staat voor Gemeentelijk Management Team. Dit team draagt gezamenlijk de verantwoordelijkheid voor het leiden van de gemeentelijke organisatie. Veelal bestaand uit de gemeentesecretaris en de afdelingshoofden. Verkregen via https://www.ifv.nl/kennisplein/Documents/043_vademecum_gmt.pdf

[28] We hebben in verband met de aanwezige rollen van de respondenten niet aan elke gemeente gevraagd of er een communicatiestrategie is.

'Dit wierp wel de vraag op (vanuit de burgemeester); zijn we nog steeds voor transparantie. Het antwoord vanuit het college en de raad; ja!' (CISO, G10).

Samenwerking CISO en AOV, en informele netwerken

Bij tien gemeenten komt naar voren dat in de voorbereiding op crisis weinig wordt samengewerkt tussen de traditionele crisisorganisatie (de AOV) en de CISO. Hier lijkt geen verschil te zijn tussen de deelnemende grote en kleine gemeenten, maar er ligt wel een andere oorzaak aan ten grondslag. Grote gemeenten geven meestal als reden dat weinig wordt samengewerkt, omdat de organisatie daarvoor 'te groot is', 'je kunt niet al je collega's kennen'. CISOs van kleinere gemeenten geven veelal aan dat samenwerking met de AOV nog niet is gezocht omdat ze al druk genoeg zijn met het implementeren van de BIO en andere dagelijkse werkzaamheden.

Vier AOV-ers geven aan dat een start gemaakt is om te oefenen met cybercrisis. Dat wil zeggen dat men voornemens is om te gaan oefenen of dat al een oefening gepland staat. De volgende AOV blikt vooruit op een eventuele samenwerking tijdens een crisis tussen de CISO en AOV:

'Ik denk dat ze dan heel veel moeite krijgen. Je krijgt dan een groep mensen die nog nooit heeft samengewerkt. De CISO aan de digitale kant, tegenover een crisisorganisatie. Daar moet informatie uitkomen waarmee de burgemeester beslissingen moet maken. Nee, ik denk niet dat dat goed zou gaan' (AOV, G2 en G3).

Een andere AOV stelt;

'Hier is nog een wereld te winnen' (AOV, G13).

De CISO van gemeente 13 vat samen;

'Je ziet dat zij vanuit een heel andere achtergrond komen dan wij. Je ziet dat zij onze kennis nodig hebben, en wij hebben hun kennis nodig, maar iedereen heeft ook nog zijn eigen werk te doen. Dit gaat niet heel erg snel. … Je hebt geen eindeloze uren om hierin te steken, en daarom ligt er nu geen overkoepelend beleidsstuk dat interne en externe cybercrises samenbrengt. '

Tot slot kwam in de interviews naar voren dat binnen regionale overleggen (veelal op veiligheidsregio-niveau) vier CISOs kennis en informatie uitwisselen waarmee de individuele gemeenten zich beter kunnen voorbereiden op cybercrisis.

4.3 Welke ervaringen hebben gemeenten met cybercrises binnen de gemeentelijk organisatie?

We hebben de geïnterviewden gevraagd in hoeverre zij ervaring hebben met een cybercrisis binnen de gemeentelijk organisatie. De respondenten geven aan dat zij niet of nauwelijks grote cyberincidenten – laat staan cybercrises – hebben meegemaakt. Een gemeente geeft aan dat een digitale aanval heeft plaatsgevonden op bepaalde publieke werken, waarbij een grote dreiging

ontstond voor maatschappelijke ontwrichting. De CISO geeft aan dit zelf te hebben afgehandeld, samen met servicemonteurs van het publieke werk. Er kwam toen vanuit de veiligheidsregio geen hulp. In een regionaal overleg waarbij de burgemeester de ernst van de zaak duidde, werd deze kwestie niet serieus genomen, aldus de AOV-er. Bij slechts één geïnterviewde gemeente heeft een crisis plaatsgevonden waarbij de CISO, de AOV én de burgemeester betrokken zijn geweest bij afhandeling.

De geïnterviewde CISOs zien het als een uitdaging om zich goed voor te bereiden op cybercrises. Zij stellen dat er weinig tijd en capaciteit is voor oefenen en dat in praktijk nog weinig 'lessons learned' bekend zijn omdat echt grote incidenten en cybercrisis weinig voorkomen. Bij geïnterviewde AOV-ers spelen deze zorgen minder, omdat daar bij de meeste afdelingen meer een oefencultuur aanwezig lijkt te zijn.

Het merendeel van de CISOs noemt het Citrix-lek begin 2020 als de eerste keer dat zij in aanraking zijn gekomen met, zoals de geïnterviewden aangeven, 'iets wat in de buurt komt van een cybercrisis'. Vijf gemeenten moesten de dienstverlening stopzetten om mitigerende maatregelen te nemen. De meeste CISOs geven aan dat de impact van het Citrix-lek (zie par. 1.1) overigens beperkt bleef. Dat wil zeggen dat de geïnterviewde gemeenten over het algemeen geen (grote) schade hebben ondervonden en ook het narratief naar de buitenwereld voor weinig reuring heeft gezorgd.

Meer dan de helft van de gemeenten geeft aan dat zij te maken hebben gehad met phishing, malware, ransomware en datalekken. Dit zijn veelal kleine incidenten gebleven. Eén gemeente geeft aan na een aantal kleinschalige malware-infecties een *gouden uur regel* te hebben ingesteld: het CERT mag binnen een uur na melding van de malware/ransomware de geïnfecteerde computer confisqueren. Dit bleek nodig omdat collega's hun computer niet wilden afstaan. Een andere gemeente geeft aan dat zij nog wel lang last hebben gehad van imagoschade naar aanleiding van een datalek een aantal jaren geleden waarmee zij in het nieuws zijn geweest. Zij worden hier nog regelmatig aan herinnerd door met name journalisten.

Vier gemeenten geven aan te zijn getroffen door incidenten op het vlak van beschikbaarheid waarbij dienstverlening meerdere uren deels of grotendeels is uitgevallen. Redenen waren onder andere een overbelaste server, doorgesneden stroomkabels door graafwerkzaamheden, en ontoereikende infrastructuur. Dit waren toevallige, niet-moedwillige incidenten. Het verschilt of de geïnterviewde gemeenten deze incidenten bestempelen als een crisis, of als (reguliere) IT-uitval. In het geval waarbij de stroomuitval uiteindelijk als crisis werd bestempeld kwam doordat de gemeente maar op 50% van de capaciteit haar burgerdienstverlening ten uitvoer kon brengen. Hierdoor moest de CISO opschalen richting de bestuurlijke portefeuillehouder, IT-directeur en communicatieadviseur. Deze multidisciplinariteit maakt dat de geïnterviewde CISO het een crisis is gaan noemen.

4.4 Welke uitdagingen ervaren gemeenten bij de omgang met cybercrises?

Rol van de CISO

CISOs worstelen met hun rol in de context van cybercrises. Dit komt door een discrepantie tussen de koude en warme fase. In de koude fase heeft de CISO geen leidinggevende rol, maar een adviserende rol richting bestuurders en managers. De geïnterviewde CISOs geven aan dat dit ook zo behoord te zijn in de warme fase, maar daarin blijkt regelmatig dat de CISO niet alleen advies geeft, maar dat ook verwacht wordt dat de CISO beslissingen neemt. Hier voelen de geïnterviewde CISOs zich niet prettig bij. De CISO van gemeente 2 en 3 verwoordde dit als volgt:

> *''Als ik geen mandaat heb bij goed weer, wil ik ook geen verantwoordelijkheid bij slecht weer'.*

Een geïnterviewde CISO (G5) geeft aan graag de samenwerking te willen zoeken met zijn collega's van OOV, maar dat het soms lastig is om cyberdreigingen met potentieel fysieke gevolgen bij hen aanhankelijk te maken.

Informatievoorziening

Meerdere CISOs worstelen soms met de informatievoorziening over dreigingen en/of incidenten vanuit de officiële kanalen (zoals die van het NCSC en de IBD). Die ervaren zij soms als traag. Informatie uit de informele netwerken is sneller en blijkt vaak accuraat te zijn, zodat CISOs soms besluiten nemen op basis van niet-geverifieerde informatie.

> *'Je moet dienstverlening offline halen, terwijl er veel burgers van afhankelijk zijn. Hier wil je goed over nadenken. Je zag dat de traagheid van informatie vanuit landelijke organisaties ervoor heeft gezorgd dat wij als gemeente op basis van onvoldoende informatie keuzes hebben gemaakt' (CISO, G13).*

Samenwerking CISO en AOV

Bij gemeenten waar CISOs en AOV-ers al wel samenwerken, is de samenwerking nog redelijk prematuur. De uitdaging voor CISOs is om de organisatie duidelijk te maken dat informatiebeveiliging niet alleen een 'IT-feestje' is, zie ook hieronder. Bij gemeente 11 werd na een cybercrisisoefening duidelijk dat CISOs en AOV-ers echt twee verschillende talen spreken en dat de taal van de CISO vaak 'te technisch' wordt bevonden. Wat de CISO van gemeente 12 opvalt is dat:

> *'Traditioneel gezien (vanuit OOV-perspectief) de crisisorganisatie overal protocollen en GRIP-structuren voor klaar heeft liggen. Zodra een crisis over cyber gaat weet men niet goed wie waarvoor verantwoordelijk is. Het is nog een betrekkelijk nieuwe wereld'.*

'IT-feestje'

Een terugkerend knelpunt bij meerdere gemeenten is het feit dat informatiebeveiliging vaak wordt gezien als een 'IT-feestje', terwijl het veelal de wens van de CISO is dat het de gehele organisatie aangaat. Veel geïnterviewde CISOs hebben in de basis een technische/IT-achtergrond en vinden het soms

lastig om IT-terminologie te vertalen naar bestuurlijke adviezen. Bij de enige gemeente waar een grootschalige cyberoefening heeft plaatsgevonden merkten zowel de CISO als AOV dit op.

Een burgemeester (G15) verwoordt het als volgt:

> *'De CISO moet beseffen dat zijn rol niet alleen is om IT-problemen op te lossen, maar ook om ervoor te zorgen dat de bestuurder verantwoordelijkheid kan nemen.'*

Communicatie
Wat betreft communicatie geeft het merendeel van de geïnterviewde gemeenten aan dat zij in de incidenten, crises en crisisoefeningen die zij hebben ervaren, vooral proactief wilden zijn in de communicatie. Dit leidt overigens wel tot dilemma's in de praktijk:

> *'Je wilt als gemeente vooral de geruchtenstroom voor zijn, en wanneer je iets naar buiten brengt, moet dit het eerlijke verhaal zijn. Het gaat er in dat geval om dat je de goede balans vindt tussen 'openheid' en 'de boeven niet slimmer maken' (AOV, G8).*

Oefenen
Bijna elke gemeente geeft aan de waarde van oefenen in te zien, maar dit gebeurt in de praktijk nog weinig. Hier worden verschillende redenen voor gegeven. Kleinere gemeenten hebben vaak hun handen vol aan het implementeren van de BIO en de dito auditlast die bij gemeenten ligt. Zij geven in de interviews dan ook aan dat het soms lastig is om het uitvoeren van een cybercrisisoefening te prioriteren en om tijd vrij te maken om deel te kunnen nemen.
Bij grotere gemeenten lijkt dat het thema cybercrisis pas recent (sinds de afgelopen twee jaar) echt op de bestuurlijke agenda staat. Dit is ook te zien in de aandacht die de IBD, het CCV en andere overheidsinstanties geven aan cybercrises. De focus lag ook hier in eerste instantie op de interne informatiebeveiliging en minder bij de samenwerking tussen de interne informatiebeveiliging en openbare orde en veiligheid.

4.5 In hoeverre en hoe ziet de gemeente haar rol bij cybercrises bij organisaties gevestigd in de gemeente?

Gemeenten vinden het over het algemeen óf lastig óf onnodig om een rol in te nemen bij cybercrises bij organisaties gevestigd in de gemeente. De gemeenten die aangeven wel een rol in te willen nemen geven hierbij aan dat dit voornamelijk een adviserende of *'linking pin'* rol moet zijn. De organisatie die zich in een cybercrisis bevindt zou dan gebruik kunnen maken van het netwerk van de gemeente. De meeste gemeenten hebben namelijk zelf weinig expertise in huis voor het adequaat duiden en afhandelen van cybercrisis (denk daarbij bijvoorbeeld aan digitaal forensisch onderzoek), maar hebben in hun netwerk wel partijen zitten die over deze expertise beschikken. Hiermee kan de gemeente dus helpen door de verbinding te leggen tussen de marktpartijen en de getroffen organisatie.

De meeste gemeenten willen niet de rol van 'digitale brandweer' innemen, al ligt hier ook regelmatig aan ten grondslag dat de gemeente dit niet 'kan' omdat de betreffende expertise niet aanwezig is. Sommige gemeenten merken op dat de organisaties gevestigd in de gemeente eerder aankloppen bij hun IT-dienstverlener of zelf op zoek gaan naar een commerciële cybersecurity partij die hen kan helpen bij incidenten en crises.

De burgemeester van gemeente 15 geeft aan dat het interessant kan zij om organisaties met een serieuze maatschappelijk impact in het geval van een cybercrisis in kaart te brengen:

> *'Als hackers in coronatijd belangrijke distributiecentra hadden platgelegd… Distributiecentra zijn geen onderdeel van de vitale infrastructuur[29], maar zijn wel maatschappelijk cruciaal.'*

Gemeenten erkennen met regelmaat dat in hun gemeente wel vanuit maatschappelijk oogpunt cruciale organisaties aanwezig zijn, maar vragen zich af wat zij kunnen betekenen voor deze organisaties in het kader van (het voorkomen van) cybercrises. Een enkele gemeente oppert het idee van een lokale ISAC (i.e. Information Sharing & Analysis Center) met een aantal van deze cruciale organisaties binnen de gemeentegrenzen.[30] Hiermee kan in feite een formele structuur worden ingericht om kennis en ervaring met elkaar uit te wisselen en elkaar ondersteuning kunnen bieden ten tijde van cybercrises.
Andere gemeenten geven aan voldoende te hebben aan informele contacten met de CISOs van organisaties binnen gemeentegrenzen. De CISO van gemeenten 2 en 3 geeft aan over een groot informeel netwerk van CISOs te beschikken waar met regelmatig vragen worden besproken die de gemeente kan beantwoorden. Dat de gemeente omziet naar organisaties binnen gemeentegrenzen is in dat geval een vorm van 'buren die naar elkaar omzien', die geen formele vorm behoeft. Zo heeft gemeente 11 ten tijde van het Citrix-lek haar hulp aangeboden aan de CISO van een lokaal ziekenhuis omdat zij de Citrix-kwetsbaarheid nog niet had opgelost.

Gemeente 14 geeft aan dat sinds kort op veiligheidsregioniveau een initiatief is gestart om de regionale samenwerking op het gebied van cyberweerbaarheid en cybercrisis te bevorderen. Hier is de gemeente wel bij betrokken, maar heeft het geen kartrekkersrol. Dit is een gezamenlijk initiatief vanuit CISO en AOV.

---

[29] Vitale infrastructuur: processen die zo essentieel zijn voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijk ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Verkregen via https://www.nctv.nl/onderwerpen/vitale-infrastructuur

[30] Een ISAC is een sectoraal samenwerkingsverband waarbinnen cyberkennis en -informatie wordt uitgewisseld. Verkregen via https://www.ncsc.nl/aan-de-slag/samenwerken/start-zelf-samenwerking/samenwerking-sector

4.6 Welke ervaringen hebben gemeenten met cybercrises bij organisaties gevestigd in de gemeente?

Tijdens de interviews heeft geen enkele gemeente aangegeven ervaring te hebben met cybercrisis bij organisaties gevestigd in de gemeente. Eén gemeente heeft aangegeven dat zij ten tijde van het Citrix-lek eind 2019/begin 2020 hun hulp hadden aangeboden aan de CISO van een lokaal ziekenhuis. Het ziekenhuis kwam in het nieuws omdat meerdere hackpogingen waren gedaan waarbij misbruik werd gemaakt van de Citrix-kwetsbaarheid. De burgemeester gaf opdracht aan de gemeentelijke CISO om contact te leggen met de CISO van het ziekenhuis om te onderzoeken of er behoefte was aan expertise (uit het netwerk) van de gemeente. Het ziekenhuis was blij met het aanbod, maar heeft daar geen gebruik van gemaakt.

4.7 Welke uitdagingen ervaren gemeenten bij de omgang met cybercrises bij organisaties gevestigd in de gemeente?

Zoals in de vorige paragraaf benoemt hebben gemeenten nog geen betekenisvolle rol gespeeld als betrokkene bij cybercrisis. Daarom is in de interviews gesproken over de *verwachte* uitdagingen en niet de *daadwerkelijke* uitdagingen bij cybercrisis binnen gemeentegrenzen.

Allereerst is gevraagd welke rol de gemeenten in moet willen of kan nemen. Een groot deel van de geïnterviewde gemeenten geeft aan graag een adviserende dan wel netwerkende rol te willen, maar, zoals ook al eerder genoemd, hebben zij naar eigen zeggen te weinig expertise om deze rol goed te kunnen vervullen. Veel gemeenten geven aan het eigen huis eerst op orde te willen brengen. Daarnaast zien gemeenten deze rol vooralsnog vooral vrijblijvend en informeel.
Een drietal gemeenten geeft aan dat het wellicht verstandig is om in kaart te brengen welke ‘high risk’ of cruciale organisaties binnen de gemeentegrenzen aanwezig zijn. Zij geven echter geen uitsluitende definitie van deze typen organisaties. Voor sommige gemeenten is het overduidelijk (bijv. gemeente Rotterdam t.o.v. Havenbedrijf Rotterdam, of Haarlemmermeer t.o.v. Schiphol), maar over het algemeen is nog geen profiel bepaald waaraan een dergelijke ‘high risk’ organisatie moet voldoen. Een burgemeester (G15) benoemt het idee dat in ieder geval rekening moet worden gehouden met in hoeverre een organisatie cruciaal is voor een specifieke sector of voor de werkgelegenheid in de regio.
Met name bij de kleinere gemeenten leeft het gevoel dat wanneer binnen de gemeentegrenzen een cybercrisis is men elkaar uiteindelijk wel weet te vinden. Zij geven daarbij aan daar geen formele structuren voor nodig te hebben, maar uit te gaan van zogeheten ‘nabuurschap’: ‘je helpt elkaar wanneer dat nodig is’.

5. Conclusie en discussie

In dit hoofdstuk worden allereerst de belangrijkste conclusies uiteengezet (par. 5.1). Vervolgens worden deze bediscussieerd (par. 5.2). Er is aandacht voor de beperkingen van het onderzoek in paragraaf 5.3. Het hoofdstuk eindigt met een slotbeschouwing in paragraaf 5.4.

5.1 Conclusie

In dit verkennende onderzoek zijn we nader ingegaan op de aard en omvang van cybercrises binnen gemeenten, hoe gemeenten zich voorbereiden op cybercrisis, en voor de uitdagingen waar gemeenten zich voor gesteld zien. De resultaten zijn gebaseerd op een beknopte literatuurstudie naar cybercrisis en 22 interviews met 31 personen, verdeeld over achttien gemeenten. De literatuurstudie had als doel om meer inzicht te verschaffen in de wetenschappelijke stand van zaken rondom de voorbereiding op, respons op, en lering van cybercrisis. De interviews zijn ingezet om de bevindingen te duiden in de gemeentelijke context.

In dit onderzoek stonden twee hoofdvragen centraal. Om beide hoofdvragen te beantwoorden, worden de deelvragen beantwoord en concluderend de uitdagingen per deelvraag benoemd. Hiermee wordt direct antwoord gegeven op de betreffende hoofdvraag.

Welke uitdagingen ervaren gemeenten bij cybercrisis binnen de gemeentelijke organisatie?

Om te duiden welke uitdagingen gemeenten ervaren bij cybercrisis binnen de gemeentelijke organisatie moet worden verduidelijkt wat gemeenten verstaan onder cybercrisis, in hoeverre gemeenten zich voorbereiden op cybercrisis en welke ervaringen gemeenten hebben met dit type cybercrisis.

Wat verstaan gemeenten onder cybercrisis?

Binnen gemeenten blijken verschillende visies te bestaan op het thema cybercrisis. De geïnterviewde CISOs zien een cybercrisis veelal als een groot intern incident, met implicaties voor de beschikbaarheid, integriteit en vertrouwelijkheid van systemen en informatie, waarbij opgeschaald dient te worden naar bestuurders. Deze opschaling maakt dat een incident in hun ogen een crisis mag worden genoemd. Overigens spreken CISOs vooral over (interne) incidenten, omdat opschaling naar crisis vrijwel niet heeft plaatsgevonden. De geïnterviewde AOV-ers spreken veelal van een cybercrisis zodra door toedoen van een digitale oorzaak een crisis ontstaat die de openbare orde en veiligheid raakt. Voorbeelden hiervan zijn digitale loketten die niet meer beschikbaar zijn, uitkeringen die niet meer uitgekeerd worden, een hack van publieke werken waardoor de fysieke veiligheid van burgers in gevaar komt, en een groot datalek met vertrouwelijke persoonsgegevens van burgers.

In hoeverre en hoe bereiden gemeenten zich voor op cybercrises binnen de gemeentelijk organisatie?

De gemeenten die mee hebben gewerkt geven aan dat het thema cyberveiligheid binnen de meeste gemeenteraden en colleges van Burgemeester

& Wethouders hoog op gemeentelijke agenda staat. Er wordt hier dan voornamelijk gesproken over informatiebeveiliging, niet over cybercrises.

De mate waarin gemeenten zich voorbereiden op cybercrisis lijkt echter sterk te verschillen. Bij de geïnterviewde gemeenten merken we hier een onderscheid in kleinere (<100.000 inwoners) en grotere (>100.000 inwoners) gemeenten. Bij kleinere gemeenten blijft de voorbereiding tot nu toe beperkt tot planvorming en, in sommige gevallen, verkennende gesprekken tussen CISO en AOV. Hier lijken drie redenen aan ten grondslag te liggen. Allereerst zijn de CISOs binnen deze gemeenten bezig met de implementatie van de BIO, vaak vanuit opdracht van afdelingsmanagers. Het voorbereiden op cybercrisis wordt daarbij niet als primaire taak of onderdeel gezien, mede vanwege de beperkte capaciteit hebben om met dit thema bezig te zijn. Daarnaast worstelen AOV-ers en, naar zeggen van geïnterviewden, ook veiligheidsregio's met het thema cybercrises als nieuw crisistype. Waar deze beide partijen op het gebied van traditionele crises, zoals een grote brand, de planvorming op orde hebben, blijkt dit voor cybercrises, zoals een grootschalige hack van bijvoorbeeld publieke werken die grote regionale impact kan hebben, niet het geval.

Grotere gemeenten zijn meestal een fase verder in de voorbereiding op cybercrisis dan kleinere. Er zijn bij deze gemeenten veelal basale draaiboeken voor incidenten en crises. In deze draaiboeken wordt bijvoorbeeld beschreven hoe een incident kan escaleren tot een crisis en wat dit betekent voor de organisatie van de respons. Een aantal grote en kleine gemeenten geven aan tijdens crises geen gebruik te willen maken van draaiboeken. Zij geloven dat de crisesrespons niet beperkt moet worden door planvorming, maar moet worden afgehandeld door ervaren mensen met mandaat.

Er zijn in dit onderzoek geen voorbeelden naar voren gekomen van structurele oefeningen van cybercrisisscenario's met de gehele gemeentelijke organisatie. Planvorming, wanneer aanwezig, is daarmee niet actief getoetst en gemeenten lopen daarmee het gevaar eventuele zwakke punten in de responsorganisatie niet te identificeren. Er zijn beperkte voorbeelden opgehaald van cybercrisisoefeningen die zijn georganiseerd door AOV-ers of de veiligheidsregio. De oefeningen die hebben plaatsgevonden sloten aan op de GRIP structuur van de veiligheidsregio.

Voor vervolgonderzoek raden we aan (grote en kleine) gemeenten meer handvatten te geven om structureel te oefenen en de *lessons learned* uit deze oefeningen te vertalen naar ontwikkeling en/of aanpassing in de planvorming. In het theoretisch kader benoemen we een aantal valkuilen die het leren van crisis kunnen belemmeren. Hiermee dient rekening te worden gehouden tijdens het evalueren – en dus leren – van de cybercrisisoefeningen.

We merken op dat het bij grotere gemeenten CISOs en AOV-ers elkaar moeilijk vinden, mede doordat de betrokken afdelingen traditioneel gezien niet veel met elkaar te maken hebben en ook anders zijn georganiseerd. De wens om samen te werken is wel aanwezig, maar het is lastig om dit ten uitvoer te brengen omdat ze aangeven 'een andere taal' te spreken. Daarnaast geven een aantal CISOs en AOV-ers aan dat beide afdelingen een ander doel nastreven. CISOs zijn vaak ge-

oriënteerd op de interne informatiebeveiliging, terwijl AOV-ers primair naar impact op de samenleving kijken. Vervolgonderzoek kan zich richten op het onderzoeken of bij andere gemeenten een sterke verbinding bestaat tussen de CISO en AOV, welke effecten deze verbinding heeft en of er handvatten zijn voor gemeenten om deze samenwerking te faciliteren en/of te versterken.

Incident- en crisisprotocollen en crisisrespons (CERT-structuur / GRIP) is bij weinig gemeenten geformaliseerd. Dit zorgt ervoor dat opschaling bij incidenten nu vaak informeel verloopt en daarbij ook veelal afhankelijk is van de (beperkte) kennis die de individuele gemeente heeft over dreigingen of de kennis en het inzicht van eerstelijnsmedewerkers (zoals servicebeheerders of IT-medewerkers). Samenwerking tussen de CISO en AOV is niet vanzelfsprekend op dit gebied. Vervolgonderzoek dient zich te richten op de vraag of formalisering van deze processen kan zorgen voor een meer adequate crisisvoorbereiding en afhandeling. Formalisering zou dan kunnen betekenen dat dreigingen vertaald worden naar handelingsperspectief voor de crisisorganisatie en/of de CISO.

Welke ervaringen hebben gemeenten met cybercrises binnen de gemeentelijk organisatie?
Op een enkele uitzondering na hebben de geïnterviewde gemeenten geen ervaring met een cybercrisis binnen de gemeentelijke organisatie of binnen de gemeentegrenzen. Dit zorgt ervoor dat gemeenten vooral spreken van hypothetische dreigingen (ondanks dat de ernst inmiddels wel wordt erkend) en dat het soms lastig is om het thema op de bestuurlijke agenda te houden. Op dit moment lijkt dat vaak af te hangen van een enthousiaste AOV of burgemeester. Dat zorgt tevens voor dat het een uitdaging kan zijn om beleidsvorming en oefencapaciteit van de grond te krijgen. We merken op dat elke crisis die in de publiciteit komt (bijv. Gemeente Lochem, Citrix, Maersk) wordt aangegrepen door de CISO om het thema op de gemeentelijke agenda te krijgen of te houden. Hoewel ‘cyber’, en daarmee dus ook cybercrisis, volgens de VNG op de gemeentelijke agenda zou moeten staan (vanuit de Agenda Digitale Veiligheid 2020-2024), maken gemeenten hier niet altijd genoeg tijd voor vrij of investeren alleen in informatiebeveiliging.

Welke uitdagingen ervaren gemeenten bij cybercrisis bij organisaties gevestigd in de gemeente?
Om te kunnen duiden welke uitdagingen gemeenten ervaren bij cybercrisis bij organisaties gevestigd in de gemeente moet worden verduidelijkt of en hoe gemeenten hun rol zien bij dergelijke crises en welke ervaringen gemeenten al hebben met dergelijke crises.

In hoeverre en hoe ziet de gemeente haar rol bij cybercrises bij organisaties gevestigd in de gemeente?
Gemeenten zijn nog zoekende in hoeverre en in welke vorm zij een rol zouden moeten hebben wanneer zich een cybercrisis voordoet bij een organisatie gevestigd in de gemeente. In geen enkel geval ziet de gemeente zichzelf als digitale brandweer. Mocht de overheid een dergelijke rol willen innemen dan is dat volgens de geïnterviewde gemeentemedewerkers allereerst een rol die de veiligheidsregio zou moeten vervullen. Dit is enerzijds begrijpelijk aangezien uit de literatuurstudie naar voren kwam dat veiligheidsregio’s al een aantal stappen verder lijken te zijn met de planvorming rondom de aanpak van cybercrisis in de

regio. Anderzijds uiten geïnterviewden ook hun twijfels over de deskundigheid van veiligheidsregio's en kwaliteit van deze plannen op het gebied van 'cyber'. Echter, de scope van dit onderzoek was beperkt tot gemeenten. Gefundeerde uitspraken in relatie tot veiligheidsregio's kunnen we derhalve niet doen.

De geïnterviewde gemeenten zien de afhandeling van een cybercrisis allereerst als een verantwoordelijkheid van de organisatie zelf. De gemeenten zijn bereid om hun netwerk aan te bieden aan organisaties die verzeild zijn geraakt in een cybercrisis. Het verschilt per gemeente of zij deze rol proactief willen communiceren of dat zij dit slechts reactief oppakken. In enkele gevallen is de gemeente actief organisaties aan het inventariseren die zij als cruciaal zien voor de gemeente of hebben de intentie om dat te gaan doen. Het is interessant om te onderzoeken welke rol voor gemeenten haalbaar, wenselijk en functioneel is, of dat een dergelijke rol beter is weggelegd voor een andere (overheids)organisatie, zoals een veiligheidsregio. Een onderdeel van dit onderzoek zou moeten zijn om de relatie tussen gemeenten en veiligheidsregio's te verduidelijken om zodoende inzichtelijk te maken waar de verantwoordelijkheid van gemeenten eindigt en waar die van veiligheidsregio's begint.

Welke ervaringen hebben gemeenten met cybercrises bij organisaties gevestigd in de gemeente?
Gemeenten hebben geen ervaringen met cybercrises bij organisaties gevestigd in de gemeente.

5.2 Discussie

Nu beschouwen we de belangrijkste conclusies die op basis van de resultaten zijn getrokken in voorgaande paragraaf. We bespreken hier de volgende zes thema's: (1) definitie en interpretatie van cybercrisis, (2) samenwerking tussen de CISO en AOV bij grotere gemeenten, (3) prioritering van cybercrisis, (4) formaliseren van cybercrisisaanpak, (5) leren van cybercrisis, en (6) gemeenten en veiligheidsregio's.

Definitie en interpretatie van cybercrisis
In het theoretisch kader operationaliseren wij cybercrisis op twee manieren: (1) cybercrisis waarbij de gemeente betrokkene is, en (2) cybercrisis waarbij de gemeente slachtoffer is. De eerste definitie focust op de maatschappelijke impact van cybercrisis en de tweede op de impact op de informatiebeveiliging van de gemeenteorganisatie. De geïnterviewde AOV-ers vinden meestal meer aansluiting bij de eerste definitie en de geïnterviewde CISOs meer bij de tweede. Dit lijkt een logisch gevolg te zijn van de context waarbinnen zij werken. Voor de AOV is een cybercrisis een 'andere smaak' crisis, dus ze bekijken het vanuit de crisisdefinitie. Een CISO ziet een cybercrisis als een 'opgeschaald informatiebeveiligingsincident', dus zij beschouwen cybercrisis vanuit een informatiebeveiligingsoogpunt. De vraag is of het verschil in interpretatie bevorderlijk is voor de ontwikkeling van een gezamenlijke visie op cybercrisis en de aanpak ervan. Zoals eerder benoemd spreken de CISO en AOV twee verschillende talen. Het is bevorderlijk dat zij elkaars taal – en wereld – beter leren begrijpen. Vervolgonderzoek kan bijdragen om dat gat te dichten.

CISOs gebruiken de crisiskennis van AOV-ers onvoldoende
CISOs en AOV-ers van grotere gemeenten geven aan elkaar moeilijk te vinden binnen de gemeentelijke organisatie. De betrokken afdelingen hebben traditioneel gezien weinig met elkaar van doen. We kunnen hier de parallel trekken met onderzoek van Boeke (2018) naar verschillen in de voorbereiding op cybercrisis tussen kleine en grote landen. Hij vond dat grotere landen veelal meer moeite hebben om de juiste expertise met elkaar in contact te brengen, ondanks dat meer capaciteit beschikbaar is in verhouding met de kleinere landen. In feite halen grotere gemeenten hiermee geen voordeel uit de extra capaciteit die beschikbaar is ten opzichte van kleinere gemeenten. De suggestie, die ook deels aansluit bij voorgaande paragraaf, is om ook bij grotere gemeenten te onderzoeken hoe de CISO en AOV dichter bij elkaar kunnen worden gebracht, zodat CISOs ook gebruik kunnen maken van de crisiskennis van AOV-ers.

Prioritering van cybercrisis
De geïnterviewde gemeenten geven op dit moment meer prioriteit aan informatiebeveiliging (eigen huis op orde) en digitale weerbaarheid (van burgers en ondernemers in de gemeente), en minder prioriteit aan cybercrisis. Dit sluit ook aan bij wat recent beleidsonderzoek van Stol en Bantema (2020) laat zien. Dit gebeurt vanuit de gedachte dat eerst de basis op orde moet zijn. De vraag is of het voorbereiden op (en specifiek oefenen met) cybercrisis ook onderdeel zou moeten zijn van 'de basis op orde krijgen'. Immers, in de BIO is een hoofdstuk opgenomen over bedrijfscontinuïteit, wat met het voorvallen van een cybercrisis ernstig in het geding kan komen. Ook de VNG hint hiernaar. In de Agenda Digitale Veiligheid 2020-2024 wordt gesteld: *'de noodzaak om te oefenen met digitale noodscenario's ter voorbereiding op daadwerkelijke incidenten zou integraal onderdeel moeten zijn van het bedrijfscontinuïteitsplan van iedere gemeente*' (VNG, 2019, p. 10). Hoewel gemeenten nog relatief weinig zijn geconfronteerd met cybercrisis, is het wel van belang om tot zekere hoogte erop voorbereid te zijn. Vervolgonderzoek kan helpen om inzichtelijk te maken hoe (op minimale wijze) dat te kunnen doen.

Formaliseren van cybercrisisaanpak
De triage rondom incident- en crisis-protocollen is bij weinig gemeenten geformaliseerd. Het is de vraag of formaliseren van protocollen en plannen daadwerkelijk zorgt voor een betere afhandeling bij een werkelijke cybercrisis. Ansell et al. (2010), evenals Boin et al. (2016, 2020), stellen dat bij een crisis vaak wordt afgeweken van protocollen en plannen, bijvoorbeeld omdat deze verouderd zijn of omdat er niet mee geoefend is. Ook de geïnterviewden zetten hier een groot vraagteken bij. Vanuit de crisisliteratuur (Ansell et al., 2010; Boin et al., 2016, 2020) lijkt formaliseren dus alleen relevant te zijn wanneer geoefend wordt met plannen en protocollen en wanneer deze up-to-date worden gehouden. Wij veronderstellen echter dat formaliseren niet de weg is, ook gezien de veelvoud aan hoedanigheden waarin cybercrises zich kunnen voordoen. In vervolgonderzoek kan ons inziens wel worden toegewerkt naar leidraden waarin aandachtspunten en mogelijke acties kort en bondig zijn geformuleerd. Deze leidraden kunnen ondersteunend zijn aan de (in)formele netwerken die al op hun plaats zijn.

Leren van cybercrisis
In het afgelopen jaar hebben bij gemeenten en organisaties een aantal cybercrises plaatsgevonden die de publiciteit hebben bereikt (zie par. 1.1). In een aantal gevallen zijn na deze cybercrises publieke rapportages opgeleverd met de *lessons learned* (De Winter, 2019; Maastricht University, 2020). CISOs grijpen deze *lessons learned* aan om intern de voorbereiding op cybercrisis te agenderen en maatregelen te nemen. De vraag is of deze manier van leren diepgaand genoeg is om te spreken van organisationeel leren, oftewel dat de lessen die verankerd worden in de organisatie leiden tot zowel een verandering in gedrag als in de opvattingen binnen de gemeentelijke organisatie (Smith & Elliott, 2007). Leren van fouten van andere gemeenten is in zekere mate goed, maar het is daarnaast ook belangrijk om cybercrises zelf te ervaren, bij voorkeur middels een oefening, zodat de geleerde lessen passend zijn op de eigen organisatie.

Rol veiligheidsregio en rol gemeente
De G4-gemeenten hebben recent een verkenning uitgevoerd om onder andere te onderzoeken hoe de gemeente zich bij een cybercrisis kan verhouden tot de veiligheidsregio en andersom (Berenschot, 2020). Zo zien de G4-gemeenten wel een rol weggelegd voor de gemeente bij een cybercrisis met maatschappelijke effecten (i.e. een dreiging) in een beleidsdomein van de gemeente, maar niet bij een cybercrisis met een maatschappelijke verstoring. Voor vervolgonderzoek is het relevant om te onderzoeken in hoeverre de afbakening van de G4-gemeenten aansluit bij andere gemeenten.

5.3 Beperkingen

In dit onderzoek hebben wij gesproken met 31 medewerkers van achttien gemeenten. Hoewel dit een mooi aantal is voor verkennend onderzoek zijn vanwege het lage aantal deelnemende gemeenten de conclusies die we trekken beperkt generaliseerbaar. Wel hebben we dit proberen te ondervangen door zowel kleine als grote gemeenten te betrekken en gemeenten te werven vanuit heel het land. Daarnaast is het mogelijk dat de geïnterviewde gemeenten met dit onderzoek hebben meegedaan ómdat zij zich al beter voorbereiden op een cybercrisis, dan wel op een hoger volwassenheidsniveau zitten.

Bij het werven van interviewkandidaten hebben de onderzoekers de nadruk gelegd op betrokkenheid van CISOs en AOV-ers (zie ook par. 3.1). De onderzoekers hebben uiteindelijk aanzienlijk meer CISOs (N = 18) dan AOV-ers (N = 9) geïnterviewd. Dit heeft mogelijk tot gevolg dat in de resultaten een (onevenredig) grote focus ligt op de visie op en aanpak van cybercrisis vanuit informatiebeveiligingsoogpunt en minder vanuit openbare orde en veiligheid. We identificeren twee oorzaken die hieraan ten grondslag kunnen liggen. De eerste oorzaak is dat de betrokken onderzoekers meer CISOs in hun professionele netwerk hebben en daarmee ook meer CISOs hebben benaderd. De tweede oorzaak is dat het thema, zo blijkt uit de interviews, ook daadwerkelijk meer opgepakt lijkt te worden door CISOs. Daarop aansluitend merkten de onderzoekers tijdens interviews met AOV-ers op dat zij relatief weinig betrokkenheid hebben bij (interne) cyberincidenten en -crisis.

Alle interviews zijn afgenomen ten tijde van de COVID-19-pandemie. Dit kan impact hebben gehad op zowel de functieverdeling van de respondenten (een mogelijk derde reden waarom minder AOV-ers hebben deelgenomen), maar ook

op de planvorming rondom cybercrisis en de uitvoering hiervan. Veel AOV-ers (bij met name kleinere gemeenten) zijn belast met het toezicht op de lokale maatregelen rondom COVID-19 en hebben in deze periode dus ook de prioriteit daar liggen. Als gevolg is er dus minder prioriteit voor cybercrisisoefeningen.

De interviews zijn semigestructureerd afgenomen en dit kan hebben gezorgd voor 'interviewer-bias'. Enerzijds heeft het semigestructureerde interviewprotocol gezorgd voor focus in de besproken onderwerpen, anderzijds kan het ook zo zijn dat de respondenten minder ruimte hebben ervaren om af te wijken van de thema's die werden benoemd door de interviewer.

Bepaalde onderwerpen die in de literatuurstudie naar voren zijn gekomen hebben we niet kunnen uitvragen bij gemeenten. Bijvoorbeeld het onderdeel communicatiestrategie; dat lijkt te komen doordat gemeenten nog aan het verkennen zijn hoe zij met cybercrises om willen gaan of gewoon simpelweg vanwege de beperkte ervaring die gemeenten hebben met cybercrisis.

5.4 Slotwoord

De samenleving digitaliseert in een hoog tempo en wordt steeds afhankelijker van ICT. De geldt zowel voor gemeenten als voor organisaties gevestigd binnen de gemeentegrenzen. De mogelijke impact van een cybercrisis neemt hiermee ook toe. De VNG erkent in de Agenda Digitale Veiligheid 2020-2024 (VNG, 2019) het voorbereiden op een cybercrisi*s* als één van de drie speerpunten in de komende jaren. Dit onderzoek laat zien dat gemeenten nog zoekende zijn hoe zij hier handen en voeten aan moeten geven. Er is wel erkenning van het probleem, maar nog geen *silver bullet* naar de aanpak. Elke cybercrisis die in het nieuws komt (bijv. Gemeente Lochem, Citrix, Maersk) wordt aangegrepen om ervan te leren, want geen enkele gemeente wil de volgende zijn die in een cybercrisis beland. Dit onderzoek heeft inzichtelijk gemaakt voor welke uitdagingen gemeenten staan op het voorbereiden van cybercrisis. In vervolgonderzoek dienen de uitdagingen die geïdentificeerd zijn in dit verkennende onderzoek getackeld te worden om de samenleving in het algemeen digitaal weerbaarder te maken, en gemeenten in het bijzonder.

Literatuurlijst

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management*, *35*(6), 717–723. https://doi.org/10.1016/j.ijinfomgt.2015.08.001

Ansell, C., Boin, A., & Keller, A. (2010). Managing transboundary crises: Identifying the building blocks of an effective response system. *Journal of Contingencies and Crisis Management*, *18*(4), 195–207. https://doi.org/10.1111/j.1468-5973.2010.00620.x

Arpan, L. M., & Pompper, D. (2003). Stormy weather: Testing "stealing thunder" as a crisis communication strategy to improve communication flow between organizations and journalists. *Public Relations Review*, *29*(3), 291–308. https://doi.org/10.1016/S0363-8111(03)00043-2

Autoriteit Persoonsgevens. (2020). *Jaarcijfers Meldplicht Datalekken 2019*. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/jaarcijfers_meldplicht_datalekken_2019.pdf

Beldad, A. D., van Laar, E., & Hegner, S. M. (2018). Should the shady steal thunder? The effects of crisis communication timing, pre-crisis reputation valence, and crisis type on post-crisis organizational trust and purchase intention. *Journal of Contingencies and Crisis Management*, *26*(1), 150–163. https://doi.org/10.1111/1468-5973.12172

Berenschot. (2020). *Handreiking cybergevolgbestrijding (CGB) G4-gemeenten*. https://assets.amsterdam.nl/publish/pages/946958/handreiking_cybergevolgbestrijding_g4_-_deel_2_koude_fase.pdf

Birkland, T. A. (1998). Focusing events, mobilization, and agenda setting. *Journal of Public Policy*, *18*(1), 53–74. https://doi.org/10.1017/S0143814X98000038

Birkland, T. A. (2009). Disasters, lessons learned, and fantasy documents. *Journal of Contingencies and Crisis Management*, *17*(3), 146–156. https://doi.org/10.1111/j.1468-5973.2009.00575.x

Boeke, S. (2018). National cyber crisis management: Different European approaches. *Governance*, *31*(3), 449–464. https://doi.org/10.1111/gove.12309

Boin, A., 't Hart, P., Stern, E., & Sundelius, B. (2017). The politics of crisis management. In *The Politics of Crisis Management: Public Leadership Under Pressure* (2de ed.). Cambridge University Press. https://doi.org/10.1017/9781316339756

Boin, A., Overdijk, W., van der Ham, S., & Sloof, D. (2020). *Handboek voor strategisch crisismanagement* (1ste ed.). The Crisis University Press.

Collier, J. (2017). Strategies of cyber crisis management: Lessons from the approaches of Estonia and the United Kingdom. In M. Taddeo & L. Glorioso (Red.), *Ethics and Policies for Cyber Operations* (pp. 187–212). Springer International Publishing. https://doi.org/10.1007/978-3-319-45300-2_11

Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review*, *10*(3), 163–176. https://doi.org/10.1057/palgrave.crr.1550049

Coombs, W. T. (2014). State of crisis communication: Evidence and the bleeding edge. *Research Journal of the Institute for Public Relations*, *1*(1), 1–12.
Coombs, W. T., & Holladay, S. J. (2012). *The handbook ofcrisis communication*. Wiley-Blackwell. https://doi.org/10.1002/9781444314885
Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010
De Winter, B. (2019). *Door het oog van de naald: Analyse van het beveiligingsincident in Lochem*. https://www.lochem.nl/fileadmin/internet-doc/Bestuur-Organisatie-Nieuws/Nieuws/2019/hack/Duidingsrapportage_Lochem-WHITE.pdf
Deverell, E., & Hansén, D. (2009). Learning from crises and major accidents: From post-crisis fantasy documents to actual learning in the heat of crisis. *Journal of Contingencies and Crisis Management*, *17*(3), 143–145. https://doi.org/10.1111/j.1468-5973.2009.00574.x
Domenie, M. M. L., Leukfeldt, E. R., van Wilsem, J. A., Jansen, J., & Stol, W. P. (2013). *Slachtofferschap in een gedigitaliseerde samenleving* (1ste ed.). Boom Lemma Uitgevers.
Elliott, D. (2009). The failure of organizational learning from crisis - A matter of life and death? *Journal of Contingencies and Crisis Management*, *17*(3), 157–168. https://doi.org/10.1111/j.1468-5973.2009.00576.x
Enocson, J., & Söderholm, L. (2018). *Prevention of cyber security incidents within the public sector* [Masterthese, Linköping University]. http://liu.diva-portal.org/smash/record.jsf?pid=diva2:1228271
Groenendaal, J., Helsloot, I., & Scholtens, A. (2013). A critical examination of the assumptions regarding centralized coordination in large-scale emergency situations. *Journal of Homeland Security and Emergency Management*, *10*(1), 113–135. https://doi.org/10.1515/jhsem-2012-0053
IFV. (2020). *Cyberrisico's en veiligheidsregio's*. https://www.ifv.nl/kennisplein/Documents/20200228-IFV-Cyberrisicos-en-veiligheidsregios.pdf
Jong, W. (2019). Wijzen op de schuld van een ander. *Tijdschrift voor communicatiewetenschap*, *47*(2), 116–132.
Kim, B., Johnson, K., Park, S.-Y., & Liu, S. (2017). Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. *Cogent Business & Management*, *4*(1), 1–15. https://doi.org/10.1080/23311975.2017.1354525
Kovoor-Misra, S. (2009). Understanding perceived organizational identity during crisis and change. *Journal of Organizational Change Management*, *22*(5), 494–510. https://doi.org/10.1108/09534810910983460
Maastricht University. (2020). *Reactie Universiteit Maastricht op rapport FOX-IT*. https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2020/02/05/reactie-universiteit-maastricht-op-rapport-fox-it/reactie-universiteit-maastricht-op-rapport-fox-it.pdf
Metropolitan Police Service. (2019). *The little book of CYBER scams 2.0*. https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/fraud/met/little-book-of-cyber-scams-2.0.pdf
NCTV. (2018). *Nederlandse cybersecurity agenda*.

https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig/CSAgenda_def_web.pdf
NCTV. (2019). *Cybersecuritybeeld Nederland: CSBN 2019*. https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/06/12/tk-bijlage-cybersecuritybeeld-nederland-csbn-2019/tk-bijlage-cybersecuritybeeld-nederland-csbn-2019.pdf
NCTV. (2020a). *Cybersecuritybeeld Nederland: CSBN 2020*. https://www.thehaguesecuritydelta.com/media/com_hsd/report/237/document/CSBN2019-online-tcm31-392768.pdf
NCTV. (2020b). *Nationaal crisisplan digitaal*. https://www.nctv.nl/documenten/publicaties/2020/02/21/nctv-nationaal-crisisplan-digitaal-_-webversie
Østby, G., & Katt, B. (2020). Cyber crisis management roles – A municipality responsibility case Study. In Y. Murayama, D. Velev, & P. Zlateva (Red.), *IFIP Advances in Information and Communication Technology* (Vol. 575, pp. 168–181). Springer International Publishing. https://doi.org/10.1007/978-3-030-48939-7_15
Otuoze, A. O., Mustafa, M. W., & Larik, R. M. (2018). Smart grids security challenges: Classification by sources of threats. *Journal of Electrical Systems and Information Technology*, *5*(3), 468–483. https://doi.org/10.1016/j.jesit.2018.01.001
Pauchant, T., & Mitroff, I. (1992). *Transforming the crisis-prone organization: Preventing individual, organizational, and environmental tragedies*. Proquest/Csa Journal Division.
Pearson, C. M., & Clair, J. A. (1998). Reframing crisis management. *Academy of Management Review*, *23*(1), 59–76. https://doi.org/10.5465/amr.1998.192960
Pearson, C. M., & Mitroff, I. I. (1993). From crisis prone to crisis prepared: A framework for crisis management. *Academy of Management Perspectives*, *7*(1), 48–59. https://doi.org/10.5465/ame.1993.9409142058
Rathenau Instituut. (2020). *Raad weten met digitalisering: Hoe de gemeenteraad kan sturen op de maatschappelijke impact van digitale technologie*. https://www.rathenau.nl/nl/kennisgedreven-democratie/raad-weten-met-digitalisering
Regtvoort, F., & Siepel, J. H. (2014). *Risico-en crisiscommunicatie: Succesfactor in crisissituaties* (4de ed.). Coutinho.
Rijksoverheid. (2019). *Baseline Informatiebeveiliging Overheid*. https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/
Rosenthal, U. (1984). *Rampen, rellen, gijzelingen: Crisisbesluitvorming in Nederland*. De Bataafsche Leeuw.
Smith, D., & Elliott, D. (2007). Exploring the barriers to learning from crisis. *Management Learning*, *38*(5), 519–538. https://doi.org/10.1177/1350507607083205
Stol, W., & Bantema, W. (2020). Stadsbestuur en digitale veiligheid: Een analyse van beleidsplannen. In M. Malsch & J. W. Sap (Red.), *De veilig stad 2: Orde en verwarring in de stad* (1ste ed., pp. 363–386). Boom Criminologie.
Van Houten, P., Spruit, M. E. M., & Wolters, K. (2019). *Informatiebeveiliging onder controle: Grondslagen, management, organisatie en techniek van*

cybersecurity. (4de ed.). Pearson.
Veiligheidsberaad. (2018). *De rol van de veiligheidsregio's bij digitale ontwrichting*. https://www.veiligheidsberaad.nl/?jet_download=1612
VNG. (2018). *Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2019/2020*. https://www.informatiebeveiligingsdienst.nl/nieuws/dreigingsbeeld-informatiebeveiliging-2019-2020/
VNG. (2019). *Agenda digitale veiligheid 2020 – 2024. Een veilige (digitale) gemeente.* https://vng.nl/publicaties/agenda-digitale-veiligheid-2020-2024
VNG. (2020). *Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 2021/2022*. https://www.informatiebeveiligingsdienst.nl/nieuws/dreigingsbeeld-informatiebeveiliging-2021-2022/
WRR. (2019). *Voorbereiden op digitale ontwrichting*. https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting

Bijlage A – Interviewprotocol

Introductie

- Het doel van dit interview is om de uitdagingen die uw gemeente ervaart rondom cybercrisis in beeld te brengen.
- Het gaat hierbij zowel om cybercrisis die spelen binnen de gemeentelijke organisatie, als bij organisaties gevestigd in de gemeente.
- Vindt u het wenselijk dat de data anoniem wordt behandeld? We nummeren de interviews en verwijzen in het onderzoeksrapport naar deze nummers en niet naar namen en gemeenten.
- We zouden graag het gesprek willen opnemen zodat we tijdens het interview de volledige aandacht hebben bij het gesprek en achteraf het interview goed kunnen uitwerken. Na de uitwerking van het interview verwijderen we de opname.
- Het interview zal ongeveer 1 uur in beslag nemen
- In het eerste deel van het interview willen we het graag hebben over cybercrisis bij de gemeentelijke organisatie en in het tweede deel over cybercrisis bij organisaties gevestigd in de gemeente. In beide gevallen starten we met de voorbereiding, vervolgens bespreken we jullie specifieke ervaringen (mocht dit het geval zijn) en daarna willen we het hebben over de uitdagingen die de gemeente ervaart.
- We starten met een korte voorstelronde en een aantal inleidende vragen.

Thema	Specifiek	Vraag	Verdieping
Introductie	Rol	Wat is uw rol en wat is uw link met het thema cybercrisis?	
Algemene vragen	Afbakening definitie	Wat is het verschil tussen een cyberincident en een cybercrisis?	Wat is uw definitie van een cyberincident?
			Wat is uw definitie van een cybercrisis?
	Agenda	In hoeverre staat het onderwerp ‘cybercrisis’ op dit moment op de gemeentelijke agenda?	Op welke manier?
			Wie is vanuit de gemeentelijk organisatie verantwoordelijk voor de agendering?
			Vanwaar is gekozen voor deze verantwoordelijke?

Crisis gemeentelijke organisatie	Voorbereiding	In hoeverre bereidt de gemeente zich voor op een cybercrisis?	Welke bronnen gebruikt de gemeente om zich voor te bereiden op cybercrisis?
		Hoe ziet de responsorganisatie eruit? M.a.w. welke rollen en verantwoordelijkheden zijn gedefinieerd/betrokken bij de afhandeling van een cybercrisis?	In hoeverre is hierin een link met OOV/de reguliere crisisbeheersingsorganisatie? Welke instellingen, teams of personen zijn betrokken bij de crisisvoorbereiding? Waarom is gekozen voor deze samenstelling? Is dit ook de gewenste samenstelling?
		Heeft de gemeente een specifiek plan voor het managen van cybercrises?	Hoe is dit plan tot stand gekomen? Welke protocollen/beleidsstukken maken hier onderdeel vanuit? Zouden wie na interview eventueel mogen inzien/toegestuurd mogen krijgen?
			Wie is binnen de gemeente verantwoordelijk voor dit plan?
			Traint/oefent de gemeente met dit plan en zo ja, hoe regulier en op welke wijze? Welke nood / rampscenario's rondom cyber worden op dit moment beoefend?
		Worden cybercrises geclassificeerd? Zo ja, hoe?	Wat is hierin de rol van de BIO?
	Ervaring	In hoeverre heeft de gemeente ervaring met cybercrisis binnen de eigen organisatie?	IF ervaring: Met wat voor crisis heeft gemeente te maken gehad? - Grootschalig IT-uitval

			- Datalek persoonsgegevens - Datalek bedrijfsgegevens - Onbetrouwbaarheid systemen - Anders?
			IF ervaring: Wat lag aan de basis van de cybercrisis?
			IF ervaring: Hoe is dit aan het licht gekomen?
			IF ervaring: Wie zijn betrokken geweest bij de afhandeling van de crisis? Is er een crisisteam geformeerd? Welke rollen en takken waren daarin gespecificeerd?
			IF ervaring: Hoe is de gemeente omgegaan met de communicatie omtrent de crisis binnen de organisatie? En waarom deze strategie?
			IF ervaring: Hoe is de gemeente omgegaan met de communicatie omtrent de crisis naar de buitenwereld? En waarom deze strategie? Is er nagedacht over het narratief van de crisis? - Stealing thunder: proactief, snel informeren, zelf narratief bepalen - Thunder: reactief, wachten, media bepaald narratief - Denial: Ontkennende boodschap - Diminish: Verzachtende boodschap - Deal: Accepterende boodschap - Anders:

			IF ervaring: Hoe verliep de samenwerking tussen operatie en strategie? Op welke manier is besluitvorming georganiseerd tijdens een cybercrises? Ligt die bij een strategische afdeling? Heeft de operatie autonomie?
			IF ervaring: In hoeverre wordt ervoor gezorgd dat de gemeente heeft geleerd van de crisis? IF strategie: Vanwaar is gekozen voor deze strategie? IF geen strategie: Hoe zou de gemeente dit willen aanpakken?
	Uitdagingen	IF ervaring: Welke uitdagingen heeft de gemeente ervaren bij de afhandeling van crisis?	Welke uitdagingen ervaart de gemeente bij de voorbereiding? (agendering, rollen, verantwoordelijkheden, samenwerking tussen organisatie)
			Welke uitdagingen ervaart de gemeente bij de respons? (communicatie intern/extern, rollen, verantwoordelijkheden)
			Welke uitdagingen ervaart de gemeente bij de nazorg? (leren van, kennis delen, terug naar normaal)
		IF geen ervaring: Welke uitdagingen verwacht de gemeente t.o.v. interne cybercrisis?	Vanwaar zijn er deze verwachtingen?
Crisis buiten de gemeentelijke organisatie	Voorbereiding	In hoeverre is de gemeente voorbereid op een cybercrisis binnen de gemeentelijke grenzen?	OP welke wijze identificeert de gemeenten risico's?

			Welke risico's identificeert de gemeente? Oefenen met dergelijke cybercrises?
		Welke rol wenst de gemeente in te nemen bij cybercrisis binnen gemeentegrenzen?	Hoe verhoudt deze rol zich tot de rol van de Veiligheidsregio?
			Bij welke afdeling/afdeling ligt de verantwoordelijkheid? (OOV?)
			Om welke reden wil de gemeente deze rol innemen?
			In hoeverre is hierover op regionaal niveau, landelijk niveau of binnen samenwerkingsverbanden consensus?
			Is de gemeente voldoende geëquipeerd om deze rol in te nemen? Waarom wel of waarom niet?
	Ervaring	In hoeverre heeft de gemeente ervaring met cybercrisis binnen haar gemeentegrenzen?	IF ervaring: Met wat voor crisis heeft gemeente te maken gehad? Hoe is deze aan het licht gekomen? Op basis waarvan heeft de gemeente besloten hierop te acteren?
			IF ervaring: Wat voor cyberaanval lag aan de basis van de crisis?
			IF ervaring: Wie zijn betrokken geweest bij de afhandeling van de crisis? Is er een crisisteam geformeerd? Welke rollen en takken waren daarin gespecificeerd?
			IF ervaring: Hoe is de gemeente omgegaan met de communicatie omtrent de crisis binnen de organisatie? En waarom deze strategie?

			IF ervaring: Hoe is de gemeente omgegaan met de communicatie omtrent de crisis naar de buitenwereld? En waarom deze strategie? (*Stealing thunder of thunder? Denial, diminish of deal?*)
	Uitdagingen	Welke uitdagingen ervaart de gemeente bij de omgang met cybercrisis binnen haar gemeentegrenzen?	Welke uitdagingen zijn er in de voorbereiding?
			Welke uitdagingen zijn er bij de respons?
			Welke uitdagingen zijn er bij de nazorg?
Overig	Nabranders	Zijn er nog onderwerpen of vragen die niet aan bod zijn gekomen in dit interview die jullie wel als relevant achten?	Licht toe….

Afronding

- Bedankt voor uw medewerking. In de komende weken werken wij de interviews uit en gaan we resultaten analyseren.
- Het interview zullen wij beknopt uitwerken. Zou u deze uitwerking willen tegenlezen en binnen twee weken van eventueel commentaar willen voorzien?
- Zoals eerder aangegeven zijn we benieuwd naar cybercrisisplannen, -beleidstukken, -kaders die ons een beter beeld geven bij de uitdagingen die gemeenten ervaren rondom cybercrisis. Mochten dit vertrouwelijke stukken dan kunnen we een geheimhoudingsverklaring laten ondertekenen door alle onderzoekers (al valt dit al onder de gedragscode wetenschappelijke integriteit).
- Mochten er nog nabranders zijn, schroom dan niet om contact met ons op te nemen. Nogmaals bedankt voor uw medewerking!

Thorbecke

Academie

THE HAGUE
UNIVERSITY OF
APPLIED SCIENCES

NHL
STENDEN
university of
applied sciences