Nederlands Instituut Publieke Veiligheid

Bestuurlijke bevoegdheden cyber

Bevoegdheden en interventiemogelijkheden van burgemeesters en/of voorzitters veiligheidsregio bij (dreigende) digitale incidenten

Nederlandse Academie voor
Crisisbeheersing en Brandweerzorg
Postbus 7010
6801 HA Arnhem
Kemperbergerweg 783, Arnhem
www.nipv.nl
info@nipv.nl
026 355 24 00

Colofon

© Nederlands Instituut Publieke Veiligheid (NIPV), 2022

Auteur(s)	L. van der Varst, J. Groenendaal, W. Bantema, F. Cools
Contactpersoon	L. van der Varst
Opdrachtgever Contactpersoon	Veiligheidsberaad/ Portefeuillehouder Cyber en Digitale ontwrichting Fieke Ettes en Daphne Spreeuwenberg
Datum	30 september 2022

Wij hechten veel belang aan kennisdeling. Delen uit deze publicatie mogen dan ook worden overgenomen op voorwaarde van bronvermelding.

Het Nederlands Instituut Publieke Veiligheid is bij wet vastgelegd onder de naam Instituut Fysieke Veiligheid.

Inhoud

	Voorwoord	**4**
	Samenvatting	**5**
	Inleiding	**7**
1	**Verantwoordelijkheden**	**9**
1.1	Cyberkwadrant	9
1.2	Verantwoordelijkheden	10
1.3	Bevoegdheden	11
1.4	Rollen	12
1.5	Online aangejaagde verstoringen	14
2	**Cyber interventieladder**	**17**
2.1	Achtergrond	17
2.2	Interventiepiramide	17
2.3	Cyberinterventieladder	18
3	**Overkoepelende bevindingen**	**21**
3.1	Bevindingen	21
3.2	Interventiemogelijkheden	22
3.3	Aanknopingspunten voor een vervolg	22
	Bijlage 1: Deelnemers workshops	**25**
	Bijlage 2: Geraadpleegde bronnen	**26**

Voorwoord

De digitalisering van de samenleving blijft één van de grote ontwikkelingen van deze tijd. Technologische ontwikkelingen volgen elkaar in een onverminderd tempo op. Dit brengt vele kansen voor de samenleving met zich mee. Maar zorgt, vanwege onze toenemende afhankelijkheid van digitale systemen, ook voor kwetsbaarheden. De vervlechting van digitale systemen en maatschappelijke processen zorgt ervoor, dat we als samenleving rekening moeten houden met digitale ontwrichting als crisisscenario.

Liggen bij de 'klassieke' rampen en crises zowel oorzaak als gevolg in de fysieke omgeving, voor rampen en crises in de toekomst geldt dit steeds minder. Een van meest voorstelbare scenario's van deze toekomstige rampen is een digitale ontwrichting, waarbij de oorzaak in de digitale wereld ligt. Dit betekent ook iets voor de taken en bevoegdheden van voorzitters van veiligheidsregio's. Daarom heeft het Veiligheidsberaad het NIPV gevraagd om een verkenning uit te voeren naar de bestuurlijke bevoegdheden bij (dreigende) cyberincidenten.

Het thema digitale ontwrichting is onderdeel van de Strategische Agenda van het Veiligheidsberaad. Aan de hand van een bestuurlijk routeboek verkent het Veiligheidsberaad drie opgaven op dit thema. Deze opgaven gaan dieper in op 1) bestuurlijke bevoegdheden; 2) afstemming tussen crisispartners; en 3) de informatiepositie van bestuurders van de veiligheidsregio's. Met de verkenning die voor u ligt is de eerste stap gezet en is helderheid verkregen in de bestuurlijke bevoegdheden.

De verkenning biedt een overzicht van de huidige bevoegdheden en overige interventiemogelijkheden van burgemeesters en/of voorzitters veiligheidsregio's bij deze (dreigende) digitale incidenten. Het onderzoek biedt ons meerdere aanknopingspunten voor een vervolg, waaronder het vergroten van kennisoverdracht over bevoegdheden, rollen en taken bij digitale incidenten en het organiseren van cybersessies met burgemeesters en NCTV/NCSC.

Het rapport nodigt mijns inziens uit om samenwerking met crisispartners te blijven opzoeken. Wat kunnen en mogen we als crisispartners van elkaar verwachten bij digitale ontwrichtingen? Ik wens veiligheidsregio's en crisispartners dan ook toe dat we actief met elkaar in gesprek blijven over de aanpak van digitale crisisscenario's.

G.M. Van den Top
Portefeuillehouder Digitale Ontwrichting namens het Veiligheidsberaad

Samenvatting

Het Veiligheidsberaad heeft het NIPV verzocht een verkenning uit te voeren naar bestuurlijke bevoegdheden bij (dreigende) digitale incidenten. Daarbij gaat het om juridische bevoegdheden en mogelijke andere interventiemogelijkheden van burgemeesters en/of voorzitters van veiligheidsregio's.

Voor dit onderzoek is ervoor gekozen om op basis van vier verschillende scenario's de interventiemogelijkheden van burgemeesters en/of voorzitters van veiligheidsregio's te verkennen. Die verkenning heeft plaatsgevonden in workshops met een gevarieerde groep van cyberexperts en professionals uit het werkveld. Tevens is literatuur verzameld en geanalyseerd over cyberveiligheid en -gevolgbestrijding, alsmede studies naar bevoegdheden.

Burgemeesters en/of voorzitters veiligheidsregio's hebben géén bevoegdheden waarmee zijn specifiek bij cyberincidenten in kunnen grijpen. Burgemeesters en/of voorzitters veiligheidsregio's beschikken niet over wettelijke bevoegdheden op het gebied van cybersecurity.[1]

Indien een burgemeester en/of voorzitter veiligheidsregio op basis van zijn juridische bevoegdheden wil ingrijpen bij een (dreigend) cyberincident, is dat alleen mogelijk als ten gevolge van dat (dreigende) cyberincident de openbare orde en/of veiligheid in het geding is. De inzet van zo'n bevoegdheid is een noodgreep. Zij zal in praktijk niet (lichtzinnig) worden ingezet, ook omdat die bevoegdheid, zo kwam uit de workshops naar voren, niet bijdraagt aan het verhelpen van het cybersecurity- probleem.

Organisaties, bedrijven en instellingen zijn zelf verantwoordelijk voor hun bedrijfsvoering en cyberveiligheid. Bij digitale incidenten zijn de betreffende organisaties dan ook zelf verantwoordelijk voor het oplossen van het probleem. Hierbij kunnen zij een beroep doen op private cybersecurity experts, eigen (software)leveranciers of sectorale cybersecurity/ incidentrespons teams.

Veiligheidsregio's richten zich op cybergevolgbestrijding. Dat willen zeggen dat zij zich bij cyberincidenten richten op de maatschappelijke effecten voor de openbare orde en veiligheid (als gevolg van het cyberincident). Dat doen ze van oudsher, ongeacht de oorzaak van het incident. Bij het bestrijden van de effecten kunnen burgemeesters/ voorzitters van veiligheidsregio's een beroep doen op hun reguliere bevoegdheden.

Een burgemeester en/of voorzitters veiligheidsregio staan, zo blijkt uit deze verkenning, in de 'koude/ lauwe fase' wel andere interventies ter beschikking op het gebied van cyberwaakzaamheid en cyberweerbaarheid (zie paragraaf 3.2). Het betreft géén juridische bevoegdheden, maar 'zachte interventies' op het gebied van vergunningen, risicodialoog en stakeholdermobilisatie. Deze interventies bieden burgemeesters (vanuit hun rol als

[1] Naast het ontbreken van bevoegdheden, beschikken gemeenten en veiligheidsregio's bovendien niet over een eigen informatie- en expertisepositie op het gebied van cybersecurity.

bestuurder, aanjager en bemiddelaar) aangrijpingspunten voor het bevorderen van cyberwaakzaamheid en -weerbaarheid. Deze interventies worden in praktijk niet of nauwelijks gebruikt.

Net zoals in de ‘koude/lauwe fase’, beschikt een burgemeester en/of voorzitter veiligheidsregio’s in de ‘warme fase’ over reguliere bevoegdheden ten aanzien van openbare orde en veiligheid. Een burgemeester en/of voorzitter veiligheidsregio beschikt niet over specifieke bevoegdheden die hij/zij kan inzetten bij digitale incidenten. Net als bij andere bovenregionale crises spelen er bij digitale incidenten, waarbij meerdere regio’s betrokken zijn, wel een aantal terugkerende vragen en onduidelijkheden. Onder meer op het gebied van informatievoorziening, bestuurlijke afstemming en wederzijdse verwachtingen: wat kan (en mag) een burgemeester/voorzitter veiligheidsregio bij digitale incidenten van het Rijk (NCTV, NCSC) verwachten en andersom?

Inleiding

Achtergrond

Onder burgemeesters en voorzitters van veiligheidsregio's spelen vraagstukken op het gebied van cyberverstoringen, zo blijkt uit het *Bestuurlijke routeboek digitale ontwrichting* (Veiligheidsberaad, 2019). Het routeboek is op verzoek van het Veiligheidsberaad opgesteld in afstemming met onder meer de VNG, G4 en Regioburgemeesters, het Nationaal Cyber Security Centrum (NCSC) en het Ministerie van Justitie en Veiligheid. Doel van het routeboek is te komen tot een betere informatiepositie en handelingsperspectief voor besturen van veiligheidsregio's rond het thema digitale ontwrichting.

Daarbij gaat het om de vraag over welke juridische bevoegdheden van burgemeesters en voorzitters van veiligheidsregio's beschikken in het geval van maatschappelijke ontwrichting die haar oorzaak vindt in digitale verstoringen. Denk daarbij aan de digitale veiligheid van organisaties van evenementen of de digitale aansturing van productieprocessen van bedrijven die werken met gevaarlijke stoffen of organisaties in de volksgezondheidszorg zoals ziekenhuizen. Welke interventiemogelijkheden hebben burgemeesters en/of voorzitters van veiligheidsregio's in de digitale ruimte?

Opdracht

Het Veiligheidsberaad heeft het NIPV verzocht een verkenning uit te voeren naar de bevoegdheden van burgemeesters en voorzitters van veiligheidsregio's bij (dreigende) digitale incidenten. Daarbij gaat het om juridische bevoegdheden en mogelijke andere interventiemogelijkheden van burgemeesters en/of voorzitters van veiligheidsregio's.

De opdracht is uitgevoerd door Laurens van der Varst (projectleider / senior onderzoeker) en Frank Cools (senior onderzoeker) van de Vakgroep Crisisbeheersing (NIPV), Willem Bantema (lector Bestuur en Digitalisering, Thorbecke Academie/NHL Stenden Hogeschool) en Jelle Groenendaal (onderzoeker Risk Response).

Afbakening

Dit onderzoek is een verkenning naar de bestuurlijke interventiemogelijkheden van burgemeesters en/of voorzitters van veiligheidsregio's. Daaronder verstaan wij enerzijds de juridische bevoegdheden die voornoemde bestuurders hebben en anderzijds de – wat wij noemen – 'andere interventiemogelijkheden' die niet zijn te herleiden naar een wettelijke bevoegdheid. Dit onderzoek gaat zodoende niet in op zogenaamde cyberbevoegdheden die belegd zijn bij andere functionele ketens binnen het Nederlandse systeem van crisisbeheersing.[2]

[2] Voor een overzicht van de (functionele) ketens zie: Bestuurlijke Netwerkkaarten Crisisbeheersing, www.nipv.nl.

Aanpak

Voor dit onderzoek is ervoor gekozen om op basis van vier verschillende concrete scenario's de interventiemogelijkheden van burgemeesters en/of voorzitters van veiligheidsregio's in workshops met een gevarieerde groep van cyberexperts en professionals uit het werkveld te bespreken, onder wie vertegenwoordigers van gemeenten en veiligheidsregio's, VNG, NCTV en NCSC.[3] Voor dit project zijn meerdere workshops georganiseerd; deze vonden plaats in 2022 op 14 april, 12 mei, 2 juni en 14 juli. De insteek van de workshops was om op basis van realistische casussen de interventiemogelijkheden van burgemeesters en/of voorzitters van veiligheidsregio's vanuit diverse invalshoeken in kaart te brengen. Daarbij hebben we de *Cyberscenario's voor veiligheidsregio's* (Heijmen, Van der Varst en Groenendaal, 2021) als uitganspunt gehanteerd.[4] De bevindingen uit deze verkenning zijn gevalideerd tijdens een overleg van de landelijke werkgroep Cyber en digitale ontwrichting op 29 september 2022. Tevens is literatuur verzameld en geanalyseerd over cyberveiligheid en -gevolgbestrijding, alsmede studies naar bestuurlijke bevoegdheden (zie bijlage 2: Geraadpleegde bronnen).

Nevenvangst uit workshops
Tijdens de workshops zijn diverse onderwerpen ter sprake gekomen die waardevol zijn om vast te leggen. Vandaar dat we die aandachtspunten in dit kader toelichten.

Aandachtspunten:
> Informatie en alarmering (afstemmen 'crisisplannen overheden' met 'crisisplannen risico-bedrijven');
> Informatiepositie van veiligheidsregio's in relatie tot cyberdreigingen in het eigen verzorgingsgebied;
> Grootste uitdaging, ofwel het 'grijze gebied': dreiging, ofwel 'koude en lauwe fase'.
> In relatie tot in-huis-expertise: aandacht hebben voor verschillen tussen gemeenten (groot versus klein); zouden veiligheidsregio's voor kleinere gemeenten hierbij een ondersteunende rol kunnen hebben?
> Besef van bevoegdheden binnen andere (functionele) ketens en toezichthouders.
> Naast bevoegdheden kijken naar plichten (zorg- en informatieplicht van overheden en bedrijven) en communicatieve en zachtere interventies.
> Bevoegdheden hebben alleen meerwaarde als ze handhaafbaar en effectief zijn.
> Privacy-issues bij delen van informatie
> Cyber is deels een nieuw en onontgonnen terrein.
> Terugkerende vragen bij bovenregionale digitale incidenten op het gebied van informatievoorziening, bestuurlijke afstemming, capaciteit en expertise (schaarste) en verwachtingen tussen veiligheidsregio's en het Rijk.

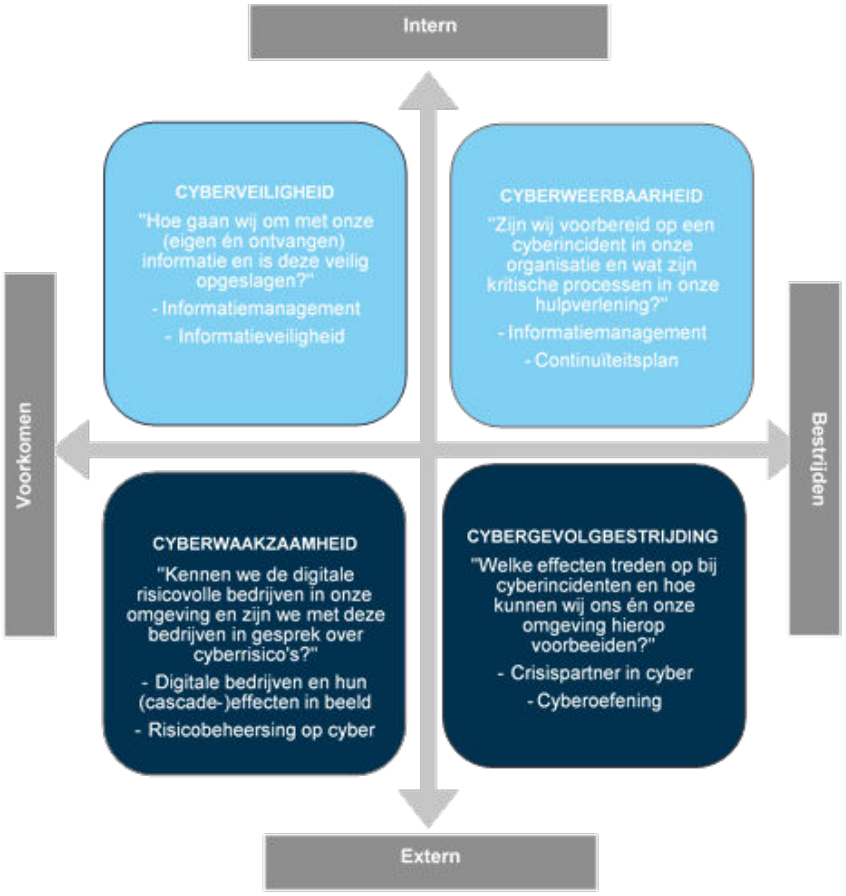
[3] Zie bijlage 1 voor een overzicht van de deelnemers aan de workshops.
[4] https://archief.nipv.nl/wp-content/uploads/sites/2/2022/03/20210616-IFV-Cyberscenarios-voor-veiligheidsregios.pdf.

1 Verantwoordelijkheden

Bij het verkennen van interventiemogelijkheden van burgemeesters en/of voorzitters van veiligheidsregio's is het goed om eerst in kaart te brengen hoe en bij welke organisaties de verantwoordelijkheid voor cyberveiligheid is belegd. Op basis daarvan onderzoeken we welke interventiemogelijkheden burgemeesters en/of voorzitters van veiligheidsregio's tot hun beschikking hebben. Daarbij gebruiken we het 'cyberkwadrant', dat we hieronder toelichten. Daarna zoomen we in op verantwoordelijkheden, bevoegdheden en rollen

1.1 Cyberkwadrant

Een bruikbaar ordeningskader is het zogeheten cyberkwadrant zoals opgesteld door Veiligheidsregio IJsselland, zie figuur 1.1. Dat kwadrant ordent de regulering van cyberveiligheid langs twee assen: van voorkomen naar bestrijden, en van intern naar extern.



Figuur 1.1 Cyberkwadrant van Veiligheidsregio IJsselland

Omdat deze verkenning primair gericht is op de cyberbevoegdheden van burgemeesters en/of voorzitters van veiligheidsregio's jegens 'externe partijen' richten we onze aandacht vooral op de onderste twee kwadranten: cyberwaakzaamheid en cybergevolgbestrijding.

Uiteraard hebben burgemeesters en/of voorzitters van veiligheidsregio's ook een verantwoordelijkheid voor de cyberveiligheid in hun eigen gemeente c.q. veiligheidsregio, maar deze intern gerichte verantwoordelijkheid zal hieronder slechts kort aan bod komen.

1.2 Verantwoordelijkheden

In de Nederlandse wetgeving is de verantwoordelijkheid voor cyberveiligheid op hoofdlijnen als volgt georganiseerd.

Uitgangspunt
Alle burgers, organisaties, bedrijven en instellingen, zowel privaat als publiek, zijn er zelf verantwoordelijk voor dat hun eigen bedrijfsvoering en dus ook de eigen cyberveiligheid op orde is (Bestuurlijke netwerkkaart cybersecurity, 2019).[5] Bedrijven kunnen diverse maatregelen nemen op het gebied van cybersecurity. Denk aan basismaatregelen zoals tweetraps authenticatie, het installeren van software-updates en segmentatie van netwerken (zie: https://www.ncsc.nl/onderwerpen/basismaatregelen). Bedrijven kunnen er ook voor kiezen om vrijwillig te voldoen aan normeringen zoals de ISO 27001. Voor overheden geldt de Baseline Informatievoorziening Overheid (BIO).

Gemeenten zijn zelf verantwoordelijk voor cybersecurity binnen de gemeentelijke organisatie, waarbij zij bij cyberdreigingen en -verstoringen een beroep kunnen doen op de deskundigheid van de Informatiebeveiligingsdienst (IBD). Ook veiligheidsregio's zijn zelf verantwoordelijk voor cybersecurity.[6] Zij kunnen bij cyberdreigingen en -verstoringen een hulpverzoek indienen bij het NCSC. Dergelijke hulpverzoeken kunnen altijd gedaan worden, maar wettelijke taak van het NCSC licht (vooralsnog) bij Rijk en Vitaal. Per verzoek zal dus bekeken worden of hierop gehandeld kan/moet worden.

Vitale processen en sectoren
Diverse ministeries (lees: 'functionele ketens') hebben in het kader van bescherming van vitale processen en sectoren een beleidsverantwoordelijkheid voor vitale organisaties en bedrijven die binnen hun beleidsdomein vallen. De Wet beveiliging netwerk- en informatie-systemen (Wbni) maakt het mogelijk om bij ministerieel besluit bedrijven aan te wijzen als 'aanbieder van essentiële diensten' (AED). Deze AED's kunnen dan onder de Wbni verplicht worden om beveiligingsmaatregelen te treffen met betrekking tot hun netwerk- en informatiesystemen. AED's krijgen op basis van de Wbni de plicht om digitale incidenten met aanzienlijke gevolgen voor hun vitale dienstverlening te melden. Voorbeeld van voornoemde ministers (als bevoegd gezag) zijn de minister van Economische Zaken en Klimaat (EZK) die verantwoordelijk is voor het vitale proces 'olievoorziening' en de minister van Infrastructuur en Waterstaat (IenW) die verantwoordelijk is voor het vitale proces grootschalige productie / verwerking en/of opslag van (petro)chemische stoffen (chemiesector).

Brzo-bedrijven
Vanwege de bestuurlijke verantwoordelijkheid van burgemeesters en/of voorzitters van veiligheidsregio's voor rampenbestrijding en crisisbeheersing noemen we hier nog specifiek de zogenaamde Brzo-bedrijven.[7] Art. 6.1.1. van het Besluit Veiligheidsregio's bepaalt dat het

[5] Voor gemeenten en veiligheidsregio's betekent dit dat zij dus ook zelf verantwoordelijk zijn voor het op orde hebben van de eigen cyberveiligheid. Zie in dit verband de bovenste twee 'interne' kwadranten van de cyberkwadrant in paragraaf 1.1.
[6] Zie verder: Handreiking Cybergevolgbestrijding G4 (Berenschot, 2020).
[7] Besluit rampen en zware ongevallen. Zie www.wetten.overheid.nl.

bestuur van een veiligheidsregio een rampbestrijdingsplan vaststelt voor – kort gezegd – Brzo-bedrijven. Vanuit omgevingsveiligheid zijn de provincies bevoegd gezag c.q. verlener van de omgevingsvergunning aan Brzo-bedrijven.[8]

1.3 Bevoegdheden

In het kader van de bevordering van cyberveiligheid bij organisaties en bedrijven in het eigen verzorgingsgebied hebben burgemeesters en/of voorzitters van veiligheidsregio's géén wettelijke bevoegdheden die specifiek betrekking hebben op cyberveiligheid. Het beleidsterrein van burgemeesters en/of voorzitters van veiligheidsregio's is openbare orde en veiligheid. Indien voornoemde bestuurders ten aanzien van cyberincidenten gebruik willen maken van hun wettelijke bevoegdheden dan is dat mogelijk wanneer de openbare orde en veiligheid in het geding zijn. Zij doen dat dan op basis van de wettelijke bevoegdheden die staan weergegeven in tabel 1.1 hieronder.

Tabel 1.1 Wettelijke bevoegdheden van burgemeesters en/of voorzitters van veiligheidsregio's

Bevoegdheden	Beschrijving
Vergunningen (Art. 174 Gemeentewet, als verlengde van de openbare orde-bevoegdheid, ex art. 172)	Artikel 174 Gemeentewet geeft de burgemeester een specifieke bevoegdheid met betrekking tot toezicht op evenementen. Dit artikel is een verlengde van de openbare orde-bevoegdheid, ex artikel 172 Gemeentewet. Artikel 174 Gemeentewet vormt de grondslag voor het verlenen van een evenementenvergunning door de burgemeester. Daarnaast kan de burgemeester op basis van het tweede lid met het oog op de bescherming van de veiligheid en de gezondheid bevelen geven. Zo'n bevel kan geen last onder bestuursdwang of een bestraffende bestuurlijke sanctie in de zin van de Awb inhouden. Door middel van een (evenementen)vergunning kan een burgemeester eisen stellen in relatie tot openbare orde en veiligheid. Er kunnen voorschriften aan een evenementenvergunning (art. 2:24 en 2:25 model-APV) worden verbonden. Een burgemeester kan als nadere regels stellen omtrent de veiligheid.
Informatieplicht (art. 7 Wvr)	Een burgemeester en/of voorzitter veiligheidsregio heeft de plicht de bevolking te informeren over (dreigende) gevaren en incidenten. Op basis daarvan kan hij/zij van (mogelijk) getroffen bedrijven verlangen (eisen) dat zij hem/haar informeren over de aard van het (dreigende) gevaar of incident.
Noodbevel (art 175 Gemeentewet)	Bij dreigende ontwrichting van de samenleving kan een burgemeester of voorzitter veiligheidsregio een noodbevel afgeven om deze dreiging weg te nemen dan wel de bevolking te beschermen. Daarbij dient hij/zij de regels van subsidiariteit en proportionaliteit in acht te nemen. Dit geldt voor situaties waarbij geen andere wettelijke bevoegdheden voorhanden zijn.
Noodverordening	Bij dreigende ontwrichting van de samenleving kan een burgemeester of voorzitter veiligheidsregio een noodverordening afgeven om deze

[8] Het Rijk, provincies en bedrijfsleven werken momenteel samen om aandacht voor cyberveiligheid bij Brzo-bedrijven te versterken. Daarbij ligt de focus op bewustwording en kennis opbouw bij de bedrijven en de betrokken overheidsdiensten.

(art 176 Gemeentewet)	bedreiging weg te nemen dan wel de bevolking te beschermen. Daarbij dient hij/zij de regels van subsidiariteit en proportionaliteit in acht te nemen. Dit geldt voor situaties waarbij geen andere wettelijke bevoegdheden voorhanden zijn.

1.4 Rollen

Hierboven is de verantwoordelijkheidsverdeling ten aanzien van cyberveiligheid in Nederland beschreven en zijn de wettelijke interventiemogelijkheden opgesomd. Naast deze wettelijke bevoegdheden zijn er nog andere – niet juridische – interventiemogelijkheden waar een burgemeester en/of voorzitter van een veiligheidsregio ten behoeve van de bevordering van de cyberveiligheid in zijn of haar verzorgingsgebied gebruik van kan maken. In deze verkenning verwijzen we daarnaar als 'rollen' waar een bestuurder invulling aan kan geven. Denk daarbij aan bevorderen, bemiddelen, stimuleren, bewust worden en aanjagen.

Tijdens de workshops die in het kader van deze verkenning zijn gehouden, zijn de onderstaande voorbeelden genoemd van rollen die een burgemeester en/of voorzitter van een veiligheidsregio (en zijn/haar) organisatie op zich kan nemen. We doen dat aan de hand van de in paragraaf 1.1 genoemde kwadranten cyberwaakzaamheid en cybergevolgbestrijding.

Cyberwaakzaamheid
Veiligheidsregio's kunnen bijdragen aan het bevorderen van cyberwaakzaamheid. Instrumenten die regio's hiervoor ter beschikking staan, zijn bijvoorbeeld:

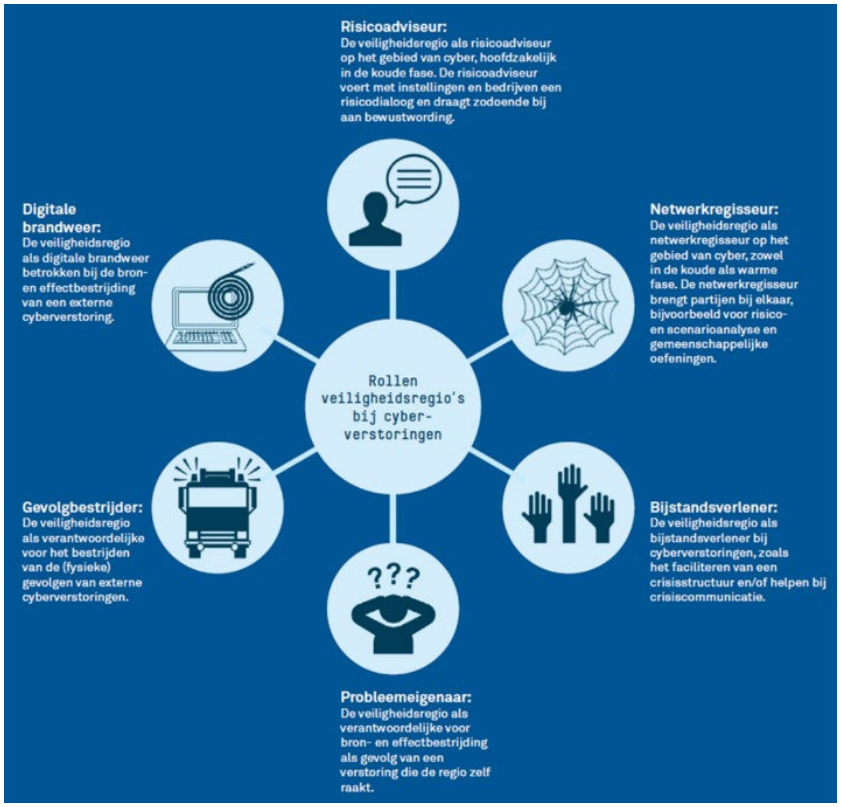
> het agenderen van cyberveiligheid in gesprekken met risicovolle organisaties en bedrijven in hun verzorgingsgebied (reguliere risicodialoog)
> het maken van gemeenschappelijke afspraken voor alarmering, opschaling en onderlinge coördinatie (planvorming)
> het bespreken van scenario's en gezamenlijk oefenen
> cyberwaakzaamheid en -gevolgbestrijding als thema in het regionaal risicoprofiel, planvorming en oefenbeleid.

Daarnaast zouden veiligheidsregio's samen met betrokkenen bijvoorbeeld cascade-effecten (zie het kwadrant) in kaart kunnen brengen. Bijvoorbeeld: hoe ziet de drinkwaterketen er uit en wat gebeurt er als een van de schakels in de keten wordt geraakt door een cyberverstoring? Op basis van die inzichten kunnen de verschillende partners in de keten zelf aan de slag om ketenkwetsbaarheden te beperken[9].

Cybergevolgbestrijding
Er zijn landelijk diverse organisaties die ook tijdens cybergevolgbestrijding overheden ten dienste kunnen staan. Zo kunnen gemeenten bij cyberincidenten een beroep doen op de Informatiebeveiligingsdienst (IBD) en staat het NCSC vitale aanbieders en andere aanbieders die onderdeel zijn van de Rijksoverheid bij in het nemen van maatregelen om de continuïteit van hun diensten te waarborgen of te herstellen.[10] Veiligheidsregio's kunnen bij cyberincidenten een hulpverzoek indienen bij het NCSC.

[9] In de workshops kwam enkele keren naar voren dat de expertise op dit gebied bij gemeenten en/of veiligheidsregio's een serieus aandachtspunt is.
[10] https://open.overheid.nl/repository/ronl-ec4dde7f-d0b3-46dc-83f7-174c42584100/1/pdf/tk-bijlage-overzicht-wet-en-regelgeving-cybersecurity.pdf.

Burgemeesters en/of voorzitters van veiligheidsregio's richten zich op de bestrijding van de maatschappelijke *gevolgen* van cyberverstoringen. Zij zijn niet verantwoordelijk voor het oplossen van cybersecuritykwetsbaarheden en -verstoringen bij andere (publieke en private) organisaties. Veiligheidsregio's kunnen organisaties en bedrijven die door een cyberincident zijn getroffen wél ondersteunen bij het crisismanagement. Let wel: het betreft hier een procesmatige en géén inhoudelijke ondersteuning op het gebied van cyberveiligheid. Een voorbeeld daarvan is de cyberaanval op de gemeente Hof van Twente waarbij de veiligheidsregio Twente onder meer een operationeel leider ter beschikking heeft gesteld aan de getroffen gemeentelijke organisatie om de crisisbestrijding procesmatig te begeleiden.



Figuur 1.2 Rollen van veiligheidsregio's bij cyberverstoringen

In figuur 1.2 hierboven zijn een aantal rollen van veiligheidsregio's bij cyberverstoringen opgenomen (Heijmen, Van der Varst en Groenendaal, 2021). Let wel: dit zijn mogelijke rollen die een veiligheidsregio *zou kunnen* vervullen. Een rol voor de veiligheidsregio als digitale brandweer ligt door het ontbreken van cybersecurityexpertise niet voor de hand. De rollen dienen vooral als hulpmiddel en als herinnering om per casus pragmatisch te kijken naar de toegevoegde waarde die een veiligheidsregio kan hebben, los van haar wettelijke taken.

Ten slotte kunnen Burgemeesters en/of voorzitters van veiligheidsregio's in de warme fase van cybergevolgbestrijding ook als *bestuurder, aanjager* of *bemiddelaar* een rol op zich nemen richting organisaties als IBD, NCSC en DTC (zie het kader op de volgende pagina).

Cyberveiligheid, BRZO en niet-vitale bedrijven
In het Bestuurlijk Omgevingsberaad maken het Ministerie van IenW en provincies bestuurlijke afspraken over een versterkingsactie cybersecurity bij (Brzo)-bedrijven. Hierbij gaat het onder andere om het opbouwen en delen van kennis op het gebied van cybersecurity met bedrijven en betrokken overheidsdiensten.[11]

Bedrijven die geen vitale aanbieder zijn, kunnen terecht bij het Digital Trust Center (DTC), onderdeel van het ministerie van EZK. Het DTC adviseert en informeert niet-vitale bedrijven in Nederland over verbetering van digitale weerbaarheid. In 2021 is het DTC gestart met het informeren van individuele bedrijven over cyberdreigingen, zoals een beveiligingslek in (bedrijfs)software of andere acute kwetsbaarheden. Daarnaast biedt het DTC bedrijven tools aan, zoals de cybersecurity-basisscan, gericht op het op orde zijn van de basisveiligheid.

1.5 Online aangejaagde verstoringen

Tot nu toe is er gesproken over cyberveiligheid in relatie tot incidenten zoals een virus, stroomuitval en gijzelsoftware. Dit zijn incidenten die in de IT- systemen en software van organisaties plaatvinden. Tijdens de workshops werd echter diverse keren het onderwerp ‘online aangejaagde verstoringen’ naar voren gebracht. Daarmee wordt gedoeld op verstoringen van de openbare orde die door (oproepen op) sociale media, in de online cyberwereld, zijn aangejaagd. Denk daarbij bijvoorbeeld aan de Facebookrellen in Haren (Project X, 2012), de avondklokrellen in verschillende gemeenten rond Covid-19 en de huidige recente boerenprotesten die online worden aangejaagd en georganiseerd. Omdat dergelijke verstoringen de bevoegdheden met betrekking tot openbare orde en veiligheid van burgemeesters en/of voorzitters van veiligheidsregio’s raken, vinden wij het zinvol om dit onderwerp ook in deze verkenning mee te nemen. Daarnaast maakt dit thema onderdeel uit van de *Cyberwegenkaart* van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) die later in deze paragraaf nog aan bod komt, en zijn er ook discussies en ontwikkelingen gaande op het gebied van bevoegdheden betreffende dit thema.

Met betrekking tot *online aangejaagde verstoringen* gelden op hoofdlijnen de volgende verantwoordelijkheden:

> De burgemeester is verantwoordelijk voor de openbare orde en veiligheid in zijn gemeente en beschikt over bestuurlijke instrumenten die ingezet kunnen worden ter voorkoming van openbare ordeverstoringen. Uit recent onderzoek blijkt dat een ruime meerderheid van burgemeesters zich verantwoordelijk voelt voor het voorkomen van dergelijke verstoringen (Bantema e.a. 2020). Bij de huidige bevoegdheden die ze daarvoor kunnen inzetten, kan gedacht worden aan een licht bevel, noodbevel of noodverordening of een (preventieve) last onder dwangsom. Daarnaast kan gedacht worden aan uiteenlopende interventies die geen bevoegdheden vereisen en vaak gericht zijn het in gesprek gaan met online ordeverstoorders of het inzetten van (online) communicatie om de situatie te beïnvloeden.[12]

> Recent zijn er situaties geweest waarbij burgemeesters een preventieve last onder dwangsom hebben opgelegd om een herhaling van opruiend online gedrag te voorkomen. Zo legde de burgemeester van Utrecht aan een inwoner van de gemeente Zeist een last onder dwangsom op, waarbij deze inwoner zich dient te onthouden van

[11] Antwoord op Kamervraag gesteld door lid Kathmann, Aanhangsel aan de Handelingen, 2021-2022, nr. 595.
[12] Er zijn ook strafrechtelijke en privaatrechtelijke mogelijkheden, maar we beperken ons hier tot het bestuursrecht.

online uitingen (op sociale media) die aanleiding (kunnen) geven tot wanordelijkheden. Als deze persoon zich niet aan de last onder dwangsom houdt, verbeurt hij een dwangsom van 2500,- euro. Volgens de gemeente bleef de maatregel in de bezwaarprocedure die volgde overeind. Inmiddels is de maatregel ingetrokken omdat de kans op herhaling als nihil wordt ingeschat.[13]

> Binnenkort verschijnt onderzoek van NHL Stenden Hogeschool naar de juridische haalbaarheid van de inzet van bevoegdheden op basis van de APV bij de aanpak van online aangejaagde ordeverstoringen. Uit dit onderzoek komt naar voren dat bestuursrechtelijk handhaven via de APV een complexe route is omdat grondrechten niet via de APV beperkt kunnen worden. Ook de Gemeentewet, een wet in formele zin, lijkt niet toegesneden op het online domein. Er zijn meerdere nuances hierop te maken en hier en daar zijn mogelijkheden om creatief gebruik te maken van de huidige wetgeving en de APV. Desalniettemin is de belangrijkste conclusie dat het, indien gewenst, bij wet in formele zin geregeld moet worden. De wetgever is dus aan zet (Bantema, Twickler en De Vries, 2022). Gemeentelijke bestuursrechtelijke experimenten hebben wel hun waarde en dragen wel bij aan inzicht in mogelijkheden en beperkingen en bij aan agendering in de landelijke politiek.

> De lokale driehoek kan het onderwerp online aangejaagde ordeverstoringen agenderen en nagaan welke stappen zij online en fysiek kunnen zetten ter voorkoming, monitoring en bestrijding van potentiële ordeverstoringen. Ook het OM speelt een belangrijke rol. Online content kan een strafbaar feit (bijvoorbeeld opruiing) opleveren, wat aanleiding kan zijn voor een huisbezoek, aanhouding en/of opsporingsonderzoek.[14]

Vanuit het Centrum voor Criminaliteitspreventie en Veiligheid is er voor gemeenten een cyberwegenkaart ontwikkeld die uit vier routes bestaat en laat zien op welke terreinen gemeenten aan de slag kunnen om cybercriminaliteit te voorkomen en te bestrijden.[15] Met name de tweede en vierde route raken aan bevoegdheden van burgemeesters, terwijl de derde route in dit kader relevant is met het oog op preventieve en communicatieve interventies om cyberveiligheid te vergroten. Hierin kan de gemeente ook bestuurlijk actief zijn. De eerste route is intern gericht en is géén onderdeel van deze verkenning.

1. Eigen huis op orde: verantwoordelijkheid nemen voor het goed functioneren van de eigen digitale systemen.
2. Cyberincidenten en cybercrisis: wees voorbereid en weet hoe te handelen in het geval van een crisis.
3. Cybercrime en gedigitaliseerde criminaliteit: weerbaar maken van bewoners en ondernemers.
4. Online aangejaagde ordeverstoring: zicht hebben op onrechtmatige activiteiten die zich online afspelen en daarmee fysieke ordeverstoringen kunnen veroorzaken.

Vanuit de VNG is een focusblad digitale veiligheid beschikbaar voor gemeenten.[16] In de handreiking staan voor verschillende risicoclusters, zoals kwetsbaarheid van systemen en online aangejaagde verstoringen, tools beschreven die gemeenten kunnen inzetten. Denk aan het uitwisselen van online signalen met partners, preventieve afstemming en het communiceren van een zogeheten ‘online tegengeluid’.

[13] https://www.rtvutrecht.nl/nieuws/3425026/burgemeester-van-utrecht-trekt-online-gebiedsverbod-in-voor-opruier
[14] https://hetccv.nl/fileadmin/Bestanden/Onderwerpen/Cybercrime/2022/Cyberwegenkaart_-_route_4__JH22.03.2022_.pdf.
[15] https://vng.nl/nieuws/lokale-cyberwegenkaart-geupdatet.
[16] https://vng.nl/sites/default/files/2022-03/VNG%20Focusblad%20Digitale%20Veiligheid.pdf

In een onderzoek van Stol en Bantema (2021) worden vier gemeentelijke taakgebieden vastgesteld die grotendeels overeenkomen met de cyberwegenkaart. De onderzoekers dragen een ‘nieuw’ taakgebied aan, waarin zij gemeenten adviseren eisen te stellen aan digitale veiligheid bij vergunningplichtige activiteiten. De gemeente is verlener van vergunningen. Bij elke vergunningverlening is er nu al aandacht voor veiligheid, en dat zou in de ogen van de onderzoekers ook zo moeten zijn voor digitale veiligheid. De gemeente kan bij vergunningverlening dan eisen stellen aan de digitale veiligheid en kan eventueel zorgdragen voor toezicht op de naleving daarvan. Te denken valt aan de digitale veiligheid van evenementen en de digitale veiligheid van andere bedrijfsmatige activiteiten binnen de gemeente.

Voorbeelden van cyberverstoringen uit het recente verleden
Gemeenten en veiligheidsregio’s kunnen op meerdere wijzen te maken krijgen met cyberincidenten:

1. Cyberverstoring binnen de eigen organisatie (voorbeeld: Hof van Twente, VNOG).
2. Cyberdreiging c.q. -verstoring bij bedrijven en organisaties in de eigen gemeente of het eigen verzorgingsgebied (voorbeeld: Universiteit Maastricht, Maersk).
3. Cyberverstoring met dreigende landelijke effecten voor de openbare orde en veiligheid (voorbeeld: KPN storing, Citrix, Log4j).
4. Online aangejaagde verstoringen met dreigende impact op de openbare orde en veiligheid (voorbeeld: Facebookrellen).

2 Cyber interventieladder

In het voorgaande hoofdstuk hebben we de verantwoordelijkheden, bevoegdheden en rollen van burgemeesters en/of voorzitters veiligheidsregio's geschetst. In dit hoofdstuk komen we tot een ordening van interventies, de *cyberinterventieladder* (paragraaf 2.3). Daarbij gaat het om het spectrum van de inzet van formele, juridische bevoegdheden tot de lichtere interventies zoals het aangaan van een dialoog of netwerk- en stakeholdermobilisatie. Hierbij gebruiken we de zogeheten handhavingspiramide als vertrekpunt (zie paragraaf 2.2.).

2.1 Achtergrond

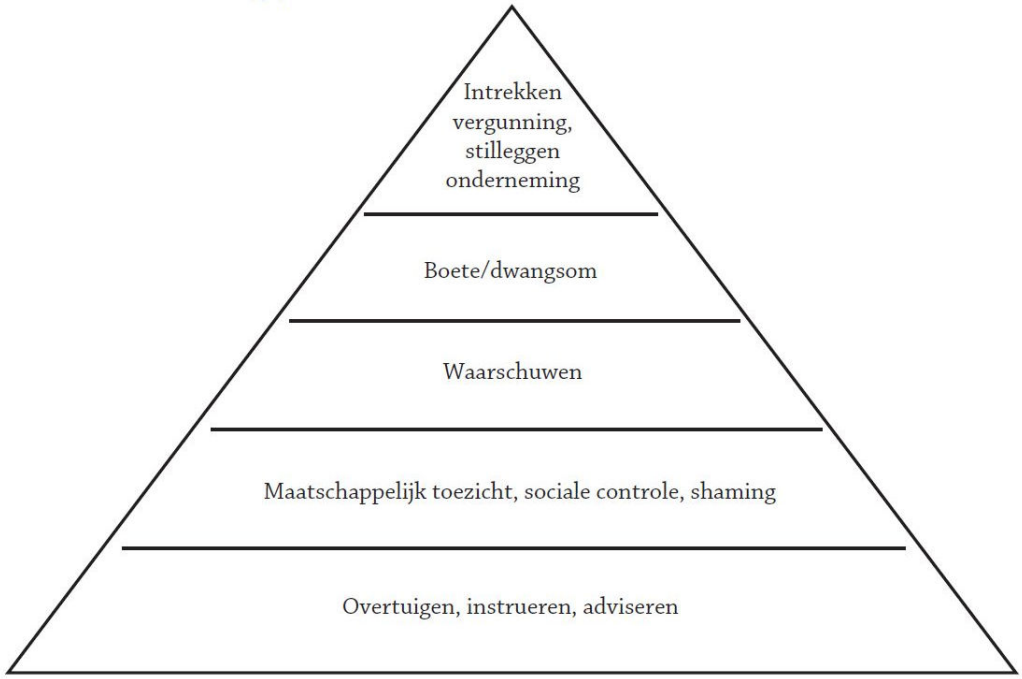
Zoals gezegd, hebben burgemeesters en voorzitters veiligheidsregio's bevoegdheden voor handhaving van de openbare orde en veiligheid. Uit onderzoek van NHL Stenden Hogeschool en de Rijksuniversiteit Groningen (Bantema et al., 2018; 2020) blijkt dat burgemeesters, hoewel ze geen formele bevoegdheden hebben die toezien op het digitale domein, zij veel openbare-ordevraagstukken oplossen zonder inzet van formele bevoegdheden. In recent onderzoek komen tal van interventies naar voren die recentelijk zijn ingezet (De Vries& Bantema, 2022), zoals online of offline in gesprek te gaan met mensen of samenwerking te zoeken met andere organisaties zoals het Openbaar Ministerie. Inzet van (nood)bevoegdheden zal in praktijk vooral een 'middel of last resort' zijn, een noodgreep. Stol en Bantema (2021) wijzen ook op mogelijkheden die vergunningverlening van onder andere evenementen biedt voor het aan de voorkant stellen van eisen aan digitale veiligheid en daar toezicht op houden. Bestuurlijke bevoegdheden specifiek gericht op de cyberveiligheid binnen bedrijven zijn ons niet bekend.

Belang van specifieke context
De inzet van interventies zal in praktijk vaak afhangen van de ernst en aard van de dreiging. Het vraagt derhalve situationeel bewustzijn wat in een concrete situatie effectief en gewenst optreden is. Daarbij moet echter niet vergeten worden dat de inzet van noodbevoegdheden weliswaar kan bijdragen aan het beëindigen van risicovolle (bedrijfs)activiteiten, maar niet per sé zorgt voor het verbeteren van cyberveiligheid.

2.2 Interventiepiramide

Een in de praktijk van toezicht en handhaving veel gebruikt instrument is de zogeheten interventie- (of handhavings)piramide (CCV, 2011). De interventiepiramide visualiseert de verschillende vormen van handhaving en toezicht – wat wil zeggen: de diverse niveaus waarop overheden kunnen reageren op regelovertredingen. De vorm van de piramide brengt tot uitdrukking dat er een opbouw of 'escalatieschaal' zit in deze interventies, van de wat 'zachtere instrumenten' zoals de dialoog aangaan, instrueren en adviseren tot 'hardere dwangmiddelen' als het intrekken van de vergunning of het stilleggen van de onderneming. Ook wordt duidelijk dat indien nodig trapsgewijs voor een strengere maatregel gekozen kan worden. De brede onderzijde van de piramide symboliseert dat de meeste bedrijven en

burgers welwillend zijn en een bijdrage willen leveren aan de naleving van regels. Wanneer (te) snel wordt opgeschaald of stappen worden overgeslagen, kan dat de intrinsieke motivatie aantasten van welwillende bedrijven en burgers die door verschillende omstandigheden de regels niet (kunnen) naleven. Bij elke stap omhoog in de piramide worden de groep aan wie zwaardere sancties wordt opgelegd kleiner. De top van de piramide wordt geacht afschrikwekkend te werken voor de lagere trappen van de piramide. *'Zacht waar het kan en hard waar het moet'* is het credo van deze benadering.



Figuur 2.1 De handhavingspiramide (bron: CCV, 2011: 10)

2.3 Cyberinterventieladder

Analoog aan de handhavingspiramide hebben we een 'cyberinterventieladder' ontwikkeld, die op de volgende pagina staat weergegeven – zij het dan niet in de vorm van een piramide, maar in die van een tabel/ladder (in tabel 2.1). Dit praktische model onderscheidt verschillende interventiemogelijkheden die net als bij de handhavingspiramide in zwaarte toenemen. Afhankelijk van de mate waarin een mogelijk of vastgesteld cyberprobleem de openbare veiligheid bedreigt of aantast, kan de burgemeester en/of voorzitter veiligheids-regio voor een van de vijf treden kiezen.

Tabel 2.1 De cyberinterventieladder

Interventietreden	Interventiemogelijkheden
Dialoog	De eerste trede van de cyberinterventieladder is het aangaan van een dialoog met de organisatie / persoon over de mogelijke of vastgestelde problemen ten aanzien van de cyberbeveiliging. Doel van deze informerende dialoog is om bewustwording te stimuleren en de organisatie / persoon te bewegen om verantwoordelijkheid te nemen.
Aanspreken	De tweede trede van de cyberinterventieladder is het formeel aanspreken van de organisatie / persoon op de vermeende of geconstateerde tekortkoming of regelovertreding. Dit kan bijvoorbeeld door het sturen van een brief waarin de organisatie wordt gewezen op het niet naleven van een eventuele verplichting en de mogelijke consequenties hiervan.
Stakeholdermobilisatie	De derde trede van de cyberinterventieladder is het mobiliseren van andere belanghebbenden. Het Bevoegd Gezag kan bijvoorbeeld in het geval van een databeschermingsprobleem de Autoriteit Persoonsgegevens op de hoogte stellen, of bijvoorbeeld door middel van risicocommunicatie burgers waarschuwen voor het gebruik van bepaalde systemen.
Waarschuwen	De volgende en vierde trede van de cyberinterventieladder is het waarschuwen van de organisatie / persoon. Deze stap gaat verder dan aanspreken, omdat hier expliciet wordt aangegeven dat bij niet tijdig nakomen van verplichtingen zal worden ingegrepen. De waarschuwing kan middels een brief of formeel gesprek worden gecommuniceerd.
Ingrijpen	De vijfde en zwaarste trede van de cyberinterventieladder behelst het daadwerkelijk ingrijpen door het bevoegd gezag. Afhankelijk van de specifieke casus kan het bijvoorbeeld gaan om een boete of dwangsom, verscherpte toezichtstelling of een Noodbevel of Noodverordening. Ingrijpen kan nodig zijn wanneer een cyberprobleem leidt of kan leiden tot een dreiging of aantasting van de openbare veiligheid.

Het is voorstelbaar dat een burgemeester en/of voorzitter veiligheidsregio vanwege dreigende aantasting van de openbare orde of veiligheid ten gevolge van een cyberincident bevoegdheden wil inzetten. Dit met als doel de negatieve gevolgen voor openbare orde en/of veiligheid van het cyberincident weg te nemen. Hierbij kan gedacht worden aan inzet van een noodbevel/ noodverordening. Toepassing van noodbevoegdheden is gelegen in een zich plotseling aandienende en concrete noodsituatie. Er dient dan sprake te zijn van ‘ernstige wanordelijkheden’ (oproerige beweging of andere ernstige wanordelijkheden) of een ‘ramp’, dan wel de ernstige vrees voor het ontstaan daarvan.[17] De inzet van zo’n bevoegdheid is een noodgreep. Zij zal in praktijk niet lichtzinnig worden ingezet, ook omdat die bevoegdheid, zo kwam uit de workshops naar voren, niet bijdraagt aan het verhelpen van het cybersecurity- probleem.

Tot slot moet ook nagedacht worden welke plek vergunningverlening kan krijgen in deze cyberinterventieladder. In de APV van gemeenten is gespecificeerd wanneer een vergunning vereist is, afhankelijk van bijvoorbeeld de plaats, het aantal mensen en het tijdstip. De

[17] https://www.burgemeesters.nl/themas/bevoegdheden/noodbevoegdheden/

burgemeester kan voorschriften en beperkingen stellen aan de evenementenvergunning. Voor zover bekend, wordt er niet expliciet verwezen naar een risico-taxatie van digitale risico's, maar er lijkt ruimte te zijn om daar aandacht aan te besteden als ze raken aan de openbare orde en veiligheid of de gezondheid van inwoners. Dat kan al aan de voorkant en allicht ook breder gelden voor bedrijven die zich vestigen in de gemeente. Deze interventie is echter lastig in de piramide te plaatsen, omdat aan de ene kant uit wordt gegaan van het maken van afspraken en er tegelijkertijd harde formele eisen gesteld worden aan de digitale veiligheid, waarmee door hun preventieve werking hogere treden in de cyberinterventieladder niet ingezet hoeven worden.

3 Overkoepelende bevindingen

3.1 Bevindingen

Burgemeesters en/of voorzitters veiligheidsregio's hebben géén specifieke bevoegdheden waarmee zij bij cyberincidenten in kunnen grijpen. Burgemeesters en/of voorzitters veiligheidsregio's beschikken niet over wettelijke bevoegdheden op het gebied van cybersecurity.[18]

Indien een burgemeester en/of voorzitter veiligheidsregio op basis van zijn juridische bevoegdheden wil ingrijpen bij een (dreigend) cyberincident, is dat alleen mogelijk als ten gevolge van dat (dreigende) cyberincident de openbare orde en/of veiligheid in het geding is. De inzet van zo'n bevoegdheid is een noodgreep. Zij zal in praktijk niet (lichtzinnig) worden ingezet, ook omdat die bevoegdheid, zo kwam uit de workshops naar voren, niet bijdraagt aan het verhelpen van het cybersecurity- probleem.

Organisaties, bedrijven en instellingen, zowel privaat als publiek, zijn zelf verantwoordelijk voor hun eigen bedrijfsvoering en eigen cyberveiligheid. Bij digitale incidenten zijn de getroffen organisaties dan ook zelf verantwoordelijk voor het oplossen van het probleem. Hierbij kunnen zij een beroep doen op private cybersecurity experts, eigen (software)leveranciers of sectorale cybersecurity/ incidentrespons teams. Zo kunnen gemeenten bij cyberincidenten binnen de eigen organisatie, een beroep doen op de Informatiebeveiligingsdienst (IBD) en Rijk en vitale partijen op het Nationaal Cyber Security Centrum (NCSC).

Een burgemeester en/of voorzitters veiligheidsregio staan in de 'koude/ lauwe fase' wel andere interventies ter beschikking op het gebied van cyberwaakzaamheid en cyberweerbaarheid (zie paragraaf 3.2). Het betreft géén juridische bevoegdheden, maar 'zachte interventies' op het gebied van vergunningen, risicodialoog en stakeholdermobilisatie. Deze interventies bieden burgemeesters (vanuit hun rol als bestuurder, aanjager en bemiddelaar) aangrijpingspunten voor het bevorderen van cyberwaakzaamheid en -weerbaarheid. Deze interventies worden in praktijk niet of nauwelijks gebruikt.

Net zoals in de 'koude/lauwe fase', beschikt een burgemeester en/of voorzitter veiligheidsregio's in de 'warme fase' over reguliere bevoegdheden ten aanzien van openbare orde en veiligheid. Een burgemeester en/of voorzitter veiligheidsregio beschikt niet over specifieke bevoegdheden die hij/zij kan inzetten bij digitale incidenten. Net als bij andere bovenregionale crises spelen er bij digitale incidenten, waarbij meerdere regio's betrokken zijn, wel een aantal terugkerende vragen en onduidelijkheden. Onder meer op het gebied van informatievoorziening, beschikbare capaciteit en expertise, bestuurlijke afstemming en

[18] Naast het ontbreken van bevoegdheden, beschikken gemeenten en veiligheidsregio's bovendien niet over een eigen informatie- en expertisepositie op het gebied van cybersecurity.

wederzijdse verwachtingen: wat kunnen (en mogen) veiligheidsregio's bij digitale incidenten van het Rijk (NCTV, NCSC) verwachten?

3.2 Interventiemogelijkheden

Op basis van deze verkenning zien we binnen de genoemde interventiemogelijkheden in paragraaf 2.3 vier onderwerpen waarbinnen burgemeesters en voorzitters veiligheidsregio's een actieve rol kunnen pakken om cyberveiligheid binnen hun verzorgingsgebied te bevorderen.

1. **Cyberveiligheid en vergunningen.** In de workshops kwam het beeld naar voren dat cyberveiligheid momenteel voor veel gemeenten en veiligheidsregio's geen onderdeel is van het vergunningsproces. Gemeenten kunnen organisaties en bedrijven bij een vergunningverlening (bijvoorbeeld bij evenementen) vragen aantoonbaar aandacht te hebben voor Algemene Verordening Gegevensbescherming (AVG) en voor cyberveiligheid.
2. **Cyberveiligheid in contacten met organisaties en bedrijven.** Veiligheidsregio's en gemeenten kunnen het onderwerp cyberveiligheid agenderen in de gesprekken en contacten met bedrijven en organisaties in het verzorgingsgebied. Burgemeesters en/of voorzitters veiligheidsregio's kunnen het onderwerp bespreekbaar maken in hun eigen bestuurdersconferentie. Dergelijke agendering en uitwisseling kunnen bijdragen aan het vergroten van risico-awareness en aanzetten tot nadere afspraken over alarmering en afstemming tijdens cyberverstoringen.
3. **Stakeholder mobilisatie.** Burgemeesters en/of voorzitters veiligheidsregio's kunnen sectorale toezichthouders attenderen op concrete aanwijzingen van cyberkwetsbaarheden bij organisaties in het verzorgingsgebied.
4. **Ketenrisico's in beeld.** Gemeenten en veiligheidsregio's kunnen bewustzijn over cyberveiligheid bij organisaties in hun verzorgingsgebied vergroten door het in kaart brengen van ketens (bijvoorbeeld die van afval, voeding of drinkwater) en met ketenpartners te beoordelen wat de gevolgen voor de gehele keten zijn als systemen van een organisatie in de keten niet meer beschikbaar of betrouwbaar zijn door een cyberaanval. Dit als onderdeel van de generieke voorbereiding op rampen en crises.
5. **Regierol.** Mogelijk kunnen gemeenten en veiligheidsregio's een bijdrage leveren aan het motiveren van bedrijven tot het vergroten van hun cyberveiligheid. Er zijn en worden diverse projecten uitgevoerd in het kader van de City Deal 'Lokale weerbaarheid en cybercrime' die hier als voorbeelden kunnen dienen en waar meer gemeenten hun voordeel mee kunnen doen bij het (preventief) vergroten van de cyberveiligheid.

3.3 Aanknopingspunten voor een vervolg

Hieronder staan enkele mogelijke aanknopingspunten voor burgemeesters en voorzitters veiligheidsregio genoemd die wij op basis van het voorliggende rapport hebben afgeleid.

1. Cybersessies: werken met de interventieladder

Organiseer cyberbijeenkomsten voor burgemeesters. Zorg voor basis kennisoverdracht (over bevoegdheden en verantwoordelijkheden, Landelijk Crisisplan Digitaal, rol van

gemeenten, veiligheidsregio's en NCSC bij cyberincidenten), spreek met elkaar meerdere cyberscenario's door en oefen met de toepassing van de cyberinterventiepiramide.

2. Cyber in relatie tot vergunningen verder verkennen

Een van de aspecten die lastig te plaatsen is in de cyberinterventiepiramide betreft de cyberveiligheid in vergunningverlening. Desalniettemin zijn er concrete mogelijkheden om de cyberveiligheid al aan de voorkant beter te kunnen regelen. Hiertoe onderscheiden we enkele stappen die aanvullend onderzoek vereisen.

> Onderzoek als veiligheidsregio/ gemeente de mate waarin het thema cybersecurity op de agenda staat van (grote) organisatoren van evenementen en bedrijven in de regio. Deze eerste stap sluit aan bij de geest van 'responsive regulation' en de onderste treden van de cyberinterventiepiramide.
> Als er geen aandacht is voor digitale veiligheid, dan is de vraag in hoeverre dat gevaren kan opleveren en wat de risico's zijn. Daarom is het van belang om de digitale veiligheidsrisico's voor verschillende soorten bedrijven /evenementen te onderzoeken. In het bijzonder gaat het hier om bedrijven die weliswaar niet direct onder de vitale infrastructuur vallen, maar die wanneer zij hun cybersecurity niet op orde hebben wel degelijk digitaal ontwrichtende en orde verstorende incidenten kunnen veroorzaken. Specifiek voor evenementen is het nodig om tot een overzicht te komen van soorten evenementen en oog te krijgen voor specifieke risico's voor de cybersecurity, openbare orde en maatschappelijke impact die daarbij en rol spelen. Mogelijk dat een classificatie, vergelijkbaar aan de risico-classificatie bij evenementen (A, B en C- evenementen), daarbij kan helpen.
> In overleg met de branche of met specifieke bedrijven kunnen veiligheidsregio's samen met gemeenten afspraken maken over welke eisen opgenomen kunnen worden in vergunningen met betrekking tot de AVG en/of cybersecurity, om verschillen in vergunningvereisten te voorkomen. De BIO of een internationale standaard zoals de ISO 27001 zouden hiervoor als uitgangspunt gebruikt kunnen worden. Bekijk of en waar expertise is om hier toezicht op te kunnen houden binnen gemeente en veiligheidsregio, en of dit in te passen is in de huidige organisaties of dat er op een andere manier invulling aan gegeven moet worden.

3. Eigen informatie en kennispositie opbouwen

Een actievere rol van veiligheidsregio's en gemeenten op het gebied van cyberveiligheid vraagt een goede informatie en -expertisepositie. Verken hoe deze informatie en -expertisepositie in regionaal verband opgebouwd en versterkt kunnen worden.

Naast die kennispositie kan handelingsperspectief nodig blijken, bijvoorbeeld in relatie tot vergunningen. Het is zeer wel denkbaar dat vergunningverleners weinig kennis hebben over digitale veiligheid bij bedrijven, zeker in kleinere gemeenten. Mogelijk dat een checklist/handreiking gemeenten en veiligheidsregio's kan ondersteunen in de dialoog met risicovolle bedrijven en evenementenorganisatoren.

4. Ketenrisico's in beeld

Investeer als veiligheidsregio samen met gemeenten en ketenpartners in cyberbewustzijn. Breng ketenrisico's (bijvoorbeeld van de afval, voeding of drinkwaterketen) in beeld en beoordeel wat de gevolgen voor de gehele keten zijn als systemen van een organisatie in de keten niet meer beschikbaar of betrouwbaar zijn door een cyberaanval.

5. Terugkerende vragen en onduidelijkheden

Verken als Veiligheidsberaad samen met de RCDV en de NCTV hoe terugkerende onduidelijkheden bij bovenregionale digitale incidenten op het gebied van informatievoorziening, beschikbare capaciteit en expertise, bestuurlijke afstemming en wederzijdse verwachtingen weggenomen kunnen worden. Gezamenlijke planvorming, maar juist ook bestuurlijke scenariosessies en landelijke oefeningen als ISIDOOR-4 kunnen hieraan bijdragen. Belangrijke vraag betreft de wederzijdse verwachtingen die betrokkenen daarbij van elkaar hebben: wat kunnen burgemeesters/ voorzitters veiligheidsregio's bij digitale incidenten van de NCTV en het NCSC verwachten en andersom.

6. Planvorming, trainen en oefenen

Zorg in regionaal verband voor cyberrespons plannen (als uitwerking van en in aansluiting op het Landelijk Crisisplan Digitaal) en maak cyber onderdeel van de reguliere oefencyclus, ook op bestuurlijk niveau.

Bijlage 1: Deelnemers workshops

Aan de workshops hebben deelgenomen:

Daniel Rios Loogman (Veiligheidsregio Kennemerland), Dennis Overgaauw (Veiligheidsregio Amsterdam-Amstelland), Renee Linck (Renee Linck Advies), Shanna Fontaine (VNG), Natassia Siutkina (Veiligheidsregio Limburg-Zuid), Mariëtta Buitenhuis (AKD Advocaten), Catherina Donkersloot (Gemeente Amsterdam), Kato Vierbergen (VNG), Kees Verkade (NCSC), Merijn ten Dam (Provincie Noord Holland), Puck de Ruijter (Ministerie van JenV), Christian Buhler (Ministerie van JenV), Mirthe Frens (Veiligheidsregio Limburg-Zuid), Geert Wismans (Ministerie van JenV), Rianne Rodenburg (gemeente Leeuwarden).

Bijlage 2: Geraadpleegde bronnen

Bantema, W., Twickler, S. M. A. & De Vries, S. (2022). Juridische grenzen en kansen bij openbare-ordehandhaving. Een onderzoek naar mogelijkheden van de APV voor de aanpak van online aangejaagde ordeverstoringen. Leeuwarden: Onderzoeksgroep Cybersafety.

Bantema, W., Twickler, S.M.A., Munneke, S.A.J., Duchateau, M. & Stol, W.P. (2018). *Burgemeesters in cyberspace: Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld.* Sdu.

Bantema, W., Westers, S. & Munneke, S.A.J. (2020). *Niet bevoegd, wel verantwoordelijk? Handhavingsmogelijkheden bij online aangejaagde ordeverstoringen*. Boom Bestuurskunde.

Berenschot (2020), Handreiking Cybergevolgbestrijding G4-gemeenten: https://www.berenschot.nl/media/soylretv/handreiking_cybergevolgbestrijding_g4_-_deel_1_warme_fase.pdf

Bestuurlijke netwerkkaarten Crisisbeheersing. Netwerkkaart 21b Cybersecurity (2019).

Buitenhuis, M. (2022). De burgemeester: burgervader, handhaver van de openbare orde en sheriff van het internet? (deel 1). *Gemeentestem, 44*(7540), 230-238.

De Vries, S. & Bantema, W. (2022). *Aanpak in kaart. Inzicht in een regionale aanpak van online aangejaagde ordeverstoringen*. Onderzoeksgroep Cybersafety.

Centrum voor Criminaliteitspreventie en Veiligheid (2011), Effecten van toezicht en handhaving meten: https://hetccv.nl/fileadmin/Bestanden/Onderwerpen/Programmatisch_handhaven/Documenten/Effecten_van_toezicht_en_handhaving_meten_een_handreiking/handreiking_effecten_toezicht_2012_def.pdf

Gemeentewet: https://wetten.overheid.nl/BWBR0005416/2022-07-01.

Heijmen, D., Varst, van der, L., & Groenendaal, J. (2021). *Cyberscenario's voor veiligheidsregio's*. Instituut Fysieke Veiligheid en De Haagse Hogeschool.

Overzicht van wet- en regelgeving betreffende cybersecurity: https://open.overheid.nl/repository/ronl-ec4dde7f-d0b3-46dc-83f7-174c42584100/1/pdf/tk-bijlage-overzicht-wet-en-regelgeving-cybersecurity.pdf.

Stol, W. & Bantema, W. (2021). *Lokaal bestuur in een digitaliserende samenleving. Essay over een stap in de ontwikkeling: een handelingskader*. Onderzoeksgroep Cyberveiligheid.

Veiligheidsberaad (2019). *Bestuurlijk routeboek digitale ontwrichting*.

VNG (2022), Focusblad Digitale Veiligheid: https://vng.nl/sites/default/files/2022-03/VNG%20Focusblad%20Digitale%20Veiligheid.pdf

Wet veiligheidsregio's: https://wetten.overheid.nl/BWBR0027466/2022-05-01.

Wierenga, A.J., Roorda, B. (2021). *Zakboek Openbare orde en veiligheid*. Nederlands Genootschap van Burgemeesters.