Veiligheids beraad

Notitie

Aan
Veiligheidsberaad

Van
Dhr. Weerwind, portefeuillehouder Kansen en bedreigingen van de informatiegestuurde samenleving

Datum
1 november 2018

De rol van de veiligheidsregio's bij digitale ontwrichting

In deze notitie zijn de kaders en uitgangspunten beschreven voor de rol van de veiligheidsregio's bij digitale ontwrichting. Met dit programma wordt beoogd meer inzicht te creëren in de bestuurlijke verantwoordelijkheden en bevoegdheden, instrumenten, en handelingsperspectieven bij digitale ontwrichting. Op basis van dit inzicht kan worden toegewerkt naar een adequate positie van de besturen van de veiligheidsregio's bij digitale ontwrichting en een betere samenwerking met andere overheden en netwerkpartners.

In de ontwikkeling van het programma wordt samengewerkt met de commissie Bestuur en Veiligheid van de VNG en met de Regioburgemeesters.
Uitgangspunt daarbij is dat gemeenten, (regio)burgemeesters en veiligheidsregio's ieder een eigen rol hebben ten aanzien van digitale veiligheid. Deze rollen kunnen overlappend zijn.

In deze notitie wordt onderscheid gemaakt tussen de fysieke omgeving (de tastbare wereld om ons heen) en de digitale omgeving (internet, computers, applicaties, enz), waarbij de notitie zich met name richt op digitale veiligheid. De digitale omgeving ontwikkelt zich snel. De digitale afhankelijkheid van burgers, bedrijven en overheid neemt toe, is sterk verweven met vrijwel alle onderdelen van de maatschappij en kent vooralsnog geen grenzen.

1. Brede bestuurlijke verantwoordelijkheid bij digitale veiligheid

Digitale veiligheid is een breed onderwerp, waar veel burgers, bedrijven en (overheids)-instanties een rol en taken in hebben. Binnen de overheid wordt deze verantwoordelijkheid wel gevoeld, maar het ontbreekt veelal nog aan inzicht in de verantwoordelijkheidsverdeling. Een vraag die op de bestuurlijke tafel ligt, is welke rollen er bestaan en wie verantwoordelijk is in de digitale omgeving. Hoe zijn de verantwoordelijkheden en bevoegdheden verdeeld en wat is de rol van de besturen van de veiligheidsregio's hierin?

Inzicht in de verantwoordelijkheidsverdeling begint bij het onderscheiden van de verschillende aspecten van digitale veiligheid waarbij een burgemeester een verantwoordelijkheid kan hebben. Dit zijn:
> informatieveiligheid (eigen organisatie);

> risicoanalyse en -beheersing;
> openbare orde en veiligheid;
> bestrijding van digitale criminaliteit;
> cybergevolgbestrijding.

Een burgemeester kan daarbij vanuit meerdere rollen een verantwoordelijkheid hebben, te weten als burgemeester van zijn/haar gemeente, als voorzitter of bestuurslid van een veiligheidsregio en als regioburgemeester. Ook op andere bestuurlijke niveaus liggen verantwoordelijkheden voor de bovengenoemde aspecten van digitale veiligheid. Daarbij valt te denken aan ministeries en Rijksheren.

Over al deze bestuurlijke tafels heen is bovendien sprake van overlap: onderwerpen kunnen vanuit verschillende invalshoeken op verschillende bestuurlijke tafels terecht komen.

> Een overkoepelend beeld van de verschillende rollen van een burgemeester bij digitale veiligheid is beschreven in de notitie *Samenwerking landelijke overleggen veiligheid op cyber*, die is opgesteld door de ondersteunende bureaus van het Veiligheidsberaad, de commissie Bestuur en Veiligheid (VNG) en de Regioburgemeesters.
>
> Daarnaast maakt het IFV in opdracht van de Raad Directeuren Veiligheidsregio (RDVR) een bestuurlijke netwerkkaart digitale ontwrichting. Deze netwerkkaart moet inzicht geven in de bestuurlijke verantwoordelijkheden en verplichtingen binnen de huidige wet- en regelgeving en in relatie tot de functionele ketens. De ontwikkeling van deze netwerkkaarten vereist een dialoog over de verantwoordelijkheden en bevoegdheden in verschillende scenario's.

Conclusie: De verschillende aspecten van digitale veiligheid waarbij burgemeesters een verantwoordelijkheid kunnen hebben, en de verschillende bestuurlijke tafels waarop digitale veiligheid aan de orde kan komen, maken het noodzakelijk om tot een heldere afbakening te komen van verantwoordelijkheden en bevoegdheden, zodat de bestuurder effectief, vanuit de juiste rol kan acteren.

In hoofdstuk 3 wordt specifiek ingegaan op de verantwoordelijkheden en bevoegdheden van de besturen van de veiligheidsregio's bij digitale ontwrichting .

2. Digitale ontwrichting en cascade-effecten

De digitale ontwikkeling brengt de maatschappij veel kansen. Door de toenemende digitale vervlechting ontstaan echter ook kwetsbaarheden. Zo kunnen verstoringen ontstaan in de digitale omgeving, die gevolgen hebben voor de fysieke omgeving en voor de openbare orde en veiligheid. Deze verstoringen kunnen voortkomen uit een technische storing of ongeval, maar ook uit sabotage of een digitale aanval.

> Voorbeelden van digitale kwetsbaarheden die consequenties hebben voor de fysieke omgeving zijn bereikbaarheidsproblemen als gevolg van storing in een tunnel, bij een groot verkeersknooppunt, in een grote haven of op een vliegveld.
> Ook kan worden gedacht aan een stremming op de waterwegen door een niet-werkende sluis of aan problemen als gevolg van uitval in de elektriciteitsvoorziening.
> Een incident in bijvoorbeeld de chemische industrie kan ontstaan vanuit een kwetsbaarheid in de digitale systemen.

Een afzonderlijk effect van een digitale ontwrichting in de fysieke omgeving kan leiden tot afgeleide effecten en vervolgens tot een waaier van effecten (cascade-effect of sneeuwbaleffect genoemd).

> Voorbeeld van een cascade-effect is een digitale ontwrichting in de Rotterdamse haven, waardoor de afhandeling van goederen stilvalt, waardoor opstoppingen ontstaan op de aanvoerroutes in de regio of zelfs daarbuiten, waardoor de bereikbaarheid voor hulpdiensten afneemt. Ook in de scheepvaart en het railvervoer ontstaan stremmingen, waardoor een trein met chemische lading stil komt te staan in stedelijk gebied, etc.
> Een ander voorbeeld is een fysieke of digitale aanval op een groot internetknooppunt of een gelijktijdige aanval op enkele telefonieproviders, waardoor communicatieverbindingen uitvallen, waardoor chaos ontstaat in de openbare ruimte, mensen 112 slecht kunnen bereiken, communicatie tussen hulpdiensten wordt bemoeilijkt, etc.

Conclusie: De toenemende digitalisering en verwevenheid van de digitale en de fysieke omgeving maakt het noodzakelijk om te komen tot inzicht in de risico's en cascade-effecten van digitale ontwrichting voor de openbare orde in de fysieke omgeving.

3. Verantwoordelijkheden en bevoegdheden van veiligheidsregio's bij digitale ontwrichting

Bestuurlijke verantwoordelijkheden en bevoegdheden (inleiding)
Openbare orde en veiligheid is een bestuurlijke verantwoordelijkheid, waar diverse bevoegdheden bij horen. Deze verantwoordelijkheden en bevoegdheden zijn duidelijk, als zowel oorzaak als gevolg van de verstoring in de fysieke omgeving liggen. Minder duidelijk zijn de bestuurlijke bevoegdheden (zo die er al zijn) als de oorzaak van de verstoring in de digitale omgeving ligt.

De vraag die voorligt, is welke verantwoordelijkheden en bevoegdheden de besturen van de veiligheidsregio's hebben om digitale ontwrichting te voorkomen of ten minste het effect op voorhand te beperken ('koude fase' of risicobeheersing genoemd), in te grijpen als een concreet incident voorzienbaar is ('lauwe fase') en, de gevolgen van een digitale ontwrichting te bestrijden ('warme fase').

> Een voorbeeld is de onbekendheid van veiligheidsregio's met de digitale weerbaarheid van chemische bedrijven. Om de (toenemende) risico's op digitale ontwrichting te kunnen inschatten en waar mogelijk hierop te kunnen acteren, hebben de (besturen van de) veiligheidsregio's informatie nodig. Het is op dit moment niet helder of en onder welke condities het bestuur deze informatie kan verkrijgen bij een (private) partij zoals een chemisch bedrijf op het grondgebied van de veiligheidsregio.
> Ook is niet helder of het bestuur aanvullende eisen kan stellen, bijvoorbeeld bij de vergunningverlening, wanneer er sprake is van een digitaal risico met (mogelijke) gevolgen voor de fysieke veiligheid.

Een vervolgvraag is hoe het bestuurlijk samenspel is tussen de veiligheidsregio's, de gemeenten en het Rijk. Door gebrek aan (breed gedragen) inzicht hierover is er geen helder bestuurlijk handelingsperspectief voor de veiligheidsregio's. Tekenend is wellicht dat het geld dat het kabinet-Rutte III heeft gereserveerd in het regeerakkoord 'versnipperd' is verdeeld

over zes departementen[1], waarbij er geen duidelijk leidend departement is waar mee gesproken kan worden.

Het lijkt in ieder geval voor de hand te liggen dat de besturen van de veiligheidsregio's op de hoogte moeten zijn van de digitale omgeving en voorbereid moet zijn om (op voorhand of achteraf) te kunnen ingrijpen op openbare orde en veiligheidsproblemen die van daaruit in hun regio kunnen ontstaan.

Conclusie: Het beperkte inzicht in de verantwoordelijkheden en bevoegdheden van de (besturen van de) veiligheidsregio's ten aanzien van digitale ontwrichting vereist opbouw van kennis.

Bestuurlijke aspecten

1. De verantwoordelijkheden en bevoegdheden van de besturen van de veiligheidsregio's in de digitale omgeving zijn nog onvoldoende helder (juridisch en in relatie tot de functionele ketens). Hierdoor kunnen de besturen hun rol niet nemen.
2. Hierdoor is ook onvoldoende helder in hoeverre de ambtelijke organisatie is ingespeeld op het omgaan met digitale ontwrichting en de ondersteuning van het bestuur hierop. Dit verschilt echter per veiligheidsregio.

Onderstaand wordt specifiek ingegaan op de aspecten risicobeheersing en gevolgbestrijding bij de veiligheidsregio's.

Risicoanalyse en -beheersing

De veiligheidsregio's hebben een wettelijke taak in het voorkomen, beperken en bestrijden van branden, rampen en crises. Aangezien de oorzaak van branden, rampen en crises ook in de digitale omgeving kan liggen, zullen de veiligheidsregio's moeten anticiperen op het voorkomen van digitale ontwrichting dan wel het verkleinen van de kans erop. Dit kunnen zij zelf doen of in samenwerking met netwerkpartners.

Dit belang neemt toe, omdat er sprake is van een toenemende digitalisering binnen de maatschappij. Ook neemt de verbondenheid sterk toe, zowel binnen de digitale omgeving, als tussen de digitale en fysieke omgeving. Hierdoor worden ook de risico's op digitale ontwrichting die een effect hebben op fysieke omgeving en daarmee op de openbare orde en veiligheid steeds groter.

Als een veiligheidsregio inzicht heeft in de risico's op digitale ontwrichting , kan ook een analyse worden gemaakt van de mogelijke effecten in de fysieke omgeving en van de cascade-effecten die daarbij kunnen optreden. Dit inzicht is nodig voor de hele 'veiligheidsketen': risicobeheersing, (preparatie op) incidentbestrijding en crisisbeheersing, risico- en crisiscommunicatie richting burgers, en normalisering.

> Bovenstaand is het voorbeeld genoemd van digitale weerbaarheid van chemische bedrijven. Een ander voorbeeld is de bouwvergunning. Ook daarbij moet rekening worden gehouden met digitale aspecten. Bijvoorbeeld aanvullende eisen aan een gebouw waarin een groot data- of rekencentrum is gevestigd, vanwege de fysieke gevolgen (openbare orde en veiligheid) van digitale ontwrichting .

[1] De departementen Veiligheid en Justitie (NCTV), Defensie (MIVD), Binnenlandse Zaken en Koninkrijksrelaties (AIVD), Buitenlandse Zaken, Infrastructuur en Milieu, en Economische Zaken

Vervolgens is de uitdaging van de veiligheidsregio's om, op basis van de analyse van digitale risico's, op te treden waar dat nodig is. Dat kan door middel van (op een andere manier kijken naar) vergunningverlening en handhaving, incidentbestrijding en gevolgbestrijding en door het zoeken van relevante 'digitale' netwerkpartners.

Bestuurlijke aspecten
3. Er is onvoldoende helderheid over de verantwoordelijkheid van de besturen van de veiligheidsregio's voor digitale risico's die gevolgen (kunnen) hebben voor de openbare orde en veiligheid.
4. Ook is er onvoldoende helderheid over de bijbehorende bevoegdheden van de regiobesturen.

Gevolgbestrijding
Onder cybergevolgbestrijding worden alle activiteiten verstaan die worden ontplooid om de situatie te normaliseren nadat een digitale ontwrichting heeft plaatsgevonden. De focus voor de veiligheidsregio's ligt daarbij op de gevolgen van een digitale ontwrichting in het fysieke domein en op het beschermen en voorlichten van burgers. Daarbij zal vrijwel altijd behoefte zijn aan coördinatie om te komen tot een gedeeld situatiebeeld en tot prioritering van de (capaciteits)inzet. Hierbij kan ook een parallel gezocht worden met andere (relatief nieuwe) vormen van gevolgbestrijding, zoals terrorismegevolgbestrijding.

Conclusie: Gezien hun wettelijke taken hebben de veiligheidsregio's (samen met netwerkpartners) een rol in het voorkomen en beperken van digitale ontwrichting die effecten in de fysieke omgeving tot gevolg kunnen hebben, en in het bestrijden van de gevolgen van digitale ontwrichting in de fysieke omgeving. Beide rollen moeten echter nader worden verkend.

Bestuurlijke aspecten
5. Cybergevolgbestrijding is (net als bijvoorbeeld terrorismegevolgbestrijding) nog onontgonnen terrein, waarbij de rol van de veiligheidsregio's (ook in relatie tot netwerkpartners) nog niet helder is.

4. Informatieveiligheid van de eigen organisatie

Informatieveiligheid heeft betrekking op de eigen verantwoordelijkheid van de afzonderlijke veiligheidsregio's voor een betrouwbare en veilige informatievoorziening. Daarbij valt te denken aan maatregelen in het fysieke domein (bijv. toegangscontrole) en het digitale domein (bijv. firewalls) om de digitale weerbaarheid van de eigen organisatie te vergroten.

Bestuurlijk convenant veiligheidsregio's
De besturen van de veiligheidsregio's hebben in 2016 een convenant ondertekend, waarmee ze in gezamenlijkheid projectmatig toewerken naar informatieveiligheid bij de afzonderlijke regio's. De regio's maken daarbij gebruik van de Baseline Informatieveiligheid Gemeenten (BIG). Uitgangspunt is dat informatieveiligheid een regionale verantwoordelijkheid is, maar een gezamenlijk belang kent. Gedurende de looptijd van het project wordt vanwege het gezamenlijk belang drie maal aan het Veiligheidsberaad gerapporteerd over de informatieveiligheid van de regio's.

> Momenteel wordt toegewerkt naar een baseline informatieveiligheid voor alle overheden, de BIO. Ook de BIG wordt hierin opgenomen. De BIG-variant voor de veiligheidsregio's (BIVR) echter nog niet. Daar is ambtelijk aandacht voor.

Met de werkwijze van collegiale toetsing die nu door de 25 veiligheidsregio's is ontwikkeld, is het fundament gelegd voor een langduriger traject van het versterken van de informatie-veiligheid binnen de regio's.

Vitale partner
Een aandachtspunt is dat veiligheidsregio's door de Rijksoverheid niet als zogenaamde 'vitale partner' zijn aangemerkt en daardoor geen informatie krijgen van en kunnen brengen naar het Nationaal Cyber Security Centrum (NCSC). Vanuit het Programmaoverleg Informatievoorziening (POI) van de veiligheidsregio's wordt hierover ambtelijk overleg gevoerd met het NCSC. De (ambtelijke) ambitie van de veiligheidsregio's is om de landelijke vakgroep Informatieveiligheid, waarin de specialisten van de veiligheidsregio's zijn verenigd, te ontwikkelen tot een ISAC (Information Sharing and Analysis Center). Een ISAC is een sectoraal instrument dat is ontwikkeld door het NCSC (Nationaal Cyber Security Centrum), waarmee de sector zich professioneel organiseert rondom het thema cybersecurity.

Vitale processen
Vergelijkbaar hiermee zijn ook de landelijke crisissystemen van de gezamenlijke veiligheidsregio's niet aangewezen als 'vitale processen', waar 112 en C2000 (landelijke systemen van de Rijksoverheid) wel als zodanig zijn aangewezen.

> De veiligheidsregio's kennen op dit moment de volgende gezamenlijke crisissystemen: het crisismanagementsysteem LCMS, het slachtofferinformatiesysteem SIS en het geografische informatiesysteem Geo4OOV. Deze zijn in gezamenlijkheid ontwikkeld en worden beheerd door het Instituut Fysieke Veiligheid.

Meer in het algemeen geldt dat de inzet vanuit de veiligheidsregio's (brandweer, ambulance, crisiscoördinatie) niet aangewezen is vitaal proces, maar bijvoorbeeld inzet van de politie wel.

Een aanpalende ontwikkeling is dat door de veiligheidsregio's samen met Rijkswaterstaat en het ministerie van Defensie onderzoek wordt verricht naar de mogelijkheid van een overheidsbreed glasvezelnet. Hiermee wordt de afhankelijkheid van de het openbare internet verkleind, hetgeen met name voor de vitale processen van de regio's van belang is.

Bestuurlijke aspecten
6. Doordat de veiligheidsregio's geen partner zijn van het Nationaal Cyber Security Centrum (NCSC) worden zij niet geattendeerd op actuele risico's en dreigingen, waar zij vanuit hun wettelijke taak een rol in (kunnen) hebben. Ook worden zij nu niet ondersteund bij het op orde brengen en houden de eigen informatieveiligheid.
7. De landelijke crisissystemen van de gezamenlijke veiligheidsregio's zijn niet aangemerkt als vitale processen, waardoor deze geen extra bescherming genieten.