

Op weg naar een toekomstbestendige informatievoorziening

Inleiding

De evaluatiecommissie van de Wet veiligheidsregio's geeft aanbevelingen aan veiligheidsregio's op het gebied van crisisbeheersing en brandweezorg. De commissie benoemt daarbij de informatievoorziening als een belangrijke randvoorwaarde. Zij adviseert een wettelijke basis te creëren voor gemeenschappelijke informatievoorziening, zodat alle crisispartners in alle fasen van een crisis en de voorbereiding daarop beschikken over dezelfde informatie. De RCDV wil dit advies versterken: informatievoorziening is essentieel om de aanbevelingen van de commissie voor de veiligheidsregio's te realiseren. Flexibele en effectieve samenwerking staat of valt met goede informatievoorziening.

De Raad Commandanten en Directeuren Veiligheidsregio's (RCDV) heeft onlangs haar ambities geformuleerd en doelen gesteld voor de komende jaren op het gebied van brandweezorg en crisisbeheersing. Dit paper sluit aan op de leidende principes en de ambities die door de RCDV zijn geformuleerd.

Informatievoorziening is een samenspel van informatieprocessen, informatiesystemen, afspraken, techniek en data. Informatievoorziening moet functioneel zijn voor lokaal en regionaal niveau. Landelijke standaarden en afspraken zijn cruciaal om bovenregionaal te kunnen samenwerken, om aan te sluiten op de crisispartners én om te voldoen aan eisen op gebied van informatieveiligheid. Informatie-uitwisseling tussen rijk en veiligheidsregio's (zoals in KCR2 vorm wordt gegeven) en tussen regio's onderling kan beter plaatsvinden op basis van landelijke standaarden en afspraken. Aan Informatievoorziening wordt daarnaast steeds hogere eisen gesteld en kan daarom niet zonder vernieuwing en innovatie.

Informatievoorziening is dus niet alleen techniek. Het is ook een samenwerkingsvraagstuk, waarbij techniek het middel is om antwoord te geven op informatievraagstukken. In deze position paper staan de organisatorische uitgangspunten én de ambities om het gebied van informatievoorziening met betrekking tot standaardisatie, beheer, en innovatie centraal. De uitdaging is om de regionale én de gezamenlijke informatievoorziening zo in te richten dat het ook in de toekomst hoogwaardige brandweezorg en crisisbeheersing mogelijk blijft maken.

Leidende principes

1 Naast brandbestrijding, hulpverlening, rampen en crises is informatiemanagement een primair proces

Veiligheidsregio's hebben een wettelijke taak om zorg te dragen voor informatiemanagement tijdens rampen en crisis. Informatie heeft strategische waarde en is minstens zo essentieel als mensen en middelen voor de uitvoering van rampenbestrijding, crisisbeheersing en brandweezorg. De veiligheidsregio's zijn informatiegebruikers én informatieverstrekkers voor de partners in rampenbestrijding en crisisbeheersing. Informatiemanagement is daarmee een primair proces naast brandweezorg, rampenbestrijding en crisisbeheersing. Deze taak en rol noodzaken de veiligheidsregio's om zowel hun eigen regionale informatievoorziening en -beveiliging, als de gezamenlijke informatievoorziening, op orde te hebben. Dat is een cruciale randvoorwaarde om een betrouwbare informatiepositie in rampenbestrijding en crisisbeheersing blijvend in te vullen. Om hieraan te voldoen is continue ontwikkeling essentieel. Dat vraagt om prioriteitsstelling en beleid op strategisch niveau.

Ondanks deze prominente positie van informatievoorziening staat het altijd ten dienste van de taken van de veiligheidsregio's, zowel op gebied van crisisbeheersing als brandweezorg en is daarmee tevens ondersteunend. Ontwikkelingen in de informatievoorziening zijn dus altijd bedoeld om de uitvoering van taken in die domeinen te verbeteren. Een sterke verbinding tussen de operationele of bestuurlijke vraagstukken en de ontwikkeling van nieuwe toepassingen in de informatievoorziening is daarvoor noodzakelijk. Dat kan door altijd een opdrachtgever uit de managementraden te verbinden aan de adviseurs vanuit de informatievoorziening. Ook in de uitvoering van projecten komt deze verbinding tot uiting door experts op het gebied van informatievoorziening samen met de vak- en proces-specialisten het project uit te laten voeren. De komende jaren zal deze verbinding worden geïntensiveerd, door op alle organisatieniveaus in het veiligheidsdomein te zorgen voor goed opdrachtgeverschap en goed opdrachtnemerschap.

2 Veiligheidsregio's zijn een landelijke betrouwbare informatieverstrekker

Gebrek aan informatie en duiding is het kenmerk van een ramp en crises. Als de veiligheidsregio's aan zet zijn, verwachten partners dat zij een landelijke betrouwbare informatieverstrekker zijn. Betrouwbaar kent hier verschillende betekenissen, die hierna uitgewerkt zijn.

Veiligheidsregio's zijn van vitaal belang voor de veiligheid en continuïteit van Nederland en zijn daarmee vitale actoren. De veiligheidsregio's dienen daarom de informatieveiligheid en continuïteit van de eigen informatievoorziening op orde te hebben. Dit vraagt om landelijk afdwingbare afspraken; de ketting is immers net zo sterk als de zwakste schakel. De 'vrijblijvendheid is voorbij'. De betrouwbaarheid van de infrastructuur voor informatiedeling tussen veiligheidsregio's, Rijksoverheid en crisispartners is namelijk afhankelijk van de bedrijfscontinuïteit van de individuele veiligheidsregio's. Om een betrouwbare en veilige, maar ook flexibele, infrastructuur op basis van de hoogst mogelijke beveiligingseisen te kunnen onderhouden, zijn gestandaardiseerde, moderne voorzieningen van hoge kwaliteit en regionale en landelijke expertise op het gebied van informatieveiligheid en cyberweerbaarheid nodig.

In de hoofdstructuur Rampen- en Crisisbeheersing (opgeschaalde situatie) hebben veiligheidsregio's de taak om 24/7 een situatiebeeld te kunnen genereren, onderhouden en delen. Naast continuïteit vraagt dat om kwaliteit van de informatievoorziening om een betrouwbare partner te zijn en te blijven. Veiligheidsregio's onderhouden een betrouwbaar en actueel informatiebeeld over maatschappelijke kwetsbaarheden, dreigingen en incidenten. Dit beeld ondersteunt de brandweezorg en crisisbeheersing in alle fasen van de veiligheidsketen. Veiligheidsregio's maken een lokaal en regionaal beeld. Kennis- en informatiedeling tussen de onderdelen van de veiligheidsketen zorgen vervolgens voor betere afstemming op de verwachte hulpvraag en hogere voorspelbaarheid van dienstverlening. Daarmee is de behoefte ontstaan om in het informatiebeeld achteruit maar met name korte en lange termijn vooruit te kunnen kijken. De hedendaagse "ongekende crises" vragen daarnaast om een bovenregionaal informatiebeeld ofwel uitzoomen naar een hoger niveau in het informatiebeeld.

Als laatste is een snelle en adequate informatiedeling tussen veiligheidsregio's, (landelijke) crisispartners en de Rijksoverheid een belangrijke randvoorwaarde. Om in alle fasen en op zowel regionaal als landelijk niveau te kunnen samenwerken is een gezamenlijke digitale infrastructuur noodzakelijk. Deze infrastructuur vraagt om continue afstemming, gezamenlijk ontwikkelen volgens gestandaardiseerde koppelvlakken, eenduidige definities en heldere afspraken. Landelijk georganiseerde crisispartners verwachten ook dat veiligheidsregio's één aanspreekpunt hebben en zich landelijk organiseren. Dat geldt ook voor de aansluiting op de tien gestandaardiseerde meldkamers.

3 Informatievoorziening is niet meer vrijblijvend

De veiligheidsregio's verschillen in ontwikkeling, inrichtingsvormen en informatiesystemen. Daarmee kunnen regio's leren van elkaars ervaringen en gebruik maken van elkaar informatiesystemen en informatieproducten. Het is belangrijk iedere regio in- en aan te sluiten. Het samen ontwikkelen vraagt dus ook om een houding van hulp vragen, bieden én aannemen. De afweging om de regionale ambities in lijn te krijgen met deze landelijke samenwerking is een dilemma.

Terwijl het gezamenlijk aanpakken van informatievoorziening noodzakelijk is om voldoende betrouwbaarheid en veiligheid te creëren, mede vanwege de vele beveiligingsissues, de landelijke aansluitingen, benodigde fall-back opties en de schaarste van mensen en middelen. Bieden van betrouwbaarheid en veiligheid betekent een hoge mate van samenwerking en gebruikmaking van dezelfde standaarden, datakoppelingen, digitale infrastructuur en beveiligingssystematiek.

Een echte slag in informatievoorziening tijdens rampen en crisis is te maken als er een verplichtend karakter voor deelname aan de informatievoorziening ten behoeve van de crisisbeheersing mede op basis van voorgeschreven standaarden bestaat. Dat maakt het mogelijk tijdens rampen en crisis eenvoudiger informatie uit te wisselen met de bij de ramp of crisis betrokken partijen. Informatievoorziening is een domein dat zich voortdurend ontwikkelt. Daarmee is innovatie ook niet vrijblijvend. Om aansluiting te houden bij de maatschappelijke en technologische ontwikkelingen zijn verbeteringen en innovaties nodig die kort cyclisch en flexibel zijn en in samenwerking met marktpartijen en partners worden aangepakt. Relevante innovaties richten zich op het inzichtelijk maken van kwetsbaarheden en risico's, het monitoren van dreigingen en het ondersteunen van beeldvorming, coördinatie en besluitvorming tijdens crises. Uiteraard zijn hierbij een creatief ontwikkelklimaat, regie en centrale financiering onmisbaar.

Ambities

1 Ontwikkeling bovenregionale en landelijke informatiepositie (KCR2)- landelijke afspraken

Eind 2024 zijn alle regio's via een (inter)regionaal informatieknoppunt aangesloten op het landelijke informatieknoppunt (werktitel KCR2).

Rampen en recente crises hebben het belang aangetoond van een goede informatiepositie van veiligheidsregio's, en een goede bovenregionale en landelijke informatiepositie. Dat heeft geleid tot het initiatief van het Knooppunt Coördinatie Regio's en Rijk (KCR2). De veiligheidsregio's en het Rijk werken in dit project samen aan de ontwikkeling van een informatievoorzieningsorganisatie, die te allen tijde een goed regionaal, bovenregionaal en landelijk beeld kan realiseren. Binnen deze samenwerking organiseren de veilig-

heidsregio's informatieknoppunten waardoor de informatie van crisispartners en van de eigen organisatie gedeeld kan worden, en uitwisseling mogelijk is met andere regio's en met landelijke partners. Deze knoppunten zijn vanzelfsprekend volgens afgesproken standaarden, normen en architectuur ingericht. Naast een technische inrichting een 24/7 actieve organisatie nodig die snel opgeschaald kan worden. De veiligheidsregio's moeten daarvoor bekwame menskracht beschikbaar en getraind hebben.

2 Inrichting informatievoorziening volgens eenduidige architectuur en standaarden

Elke regio houdt zich aan de uitgangspunten van de gezamenlijk architectuur, afspraken over standaarden, uitwisselformaten, koppelvlakken en kwaliteitsnormen. Daarmee neemt elke regio afscheid van eigen conflicterende systemen en standaarden en neemt ook verantwoordelijkheid voor de daaruit voortkomende financiële en personele consequenties.

Om bovenregionale en landelijke betrouwbare beelden te genereren over allerlei aspecten, zoals bijvoorbeeld informatie over opvang van vluchtelingen, personeelsbezetting en incidentstatistiek, zijn afspraken over de uitwisseling nodig over definities, actualiteit, kwaliteit en beveiliging, zowel op proces en inhoud, als technisch. Veiligheidsregio's hebben dezelfde wettelijke taak, maar verschillende governance-vormen en daarmee ICT-infrastructuren. Deze diversiteit is een gegeven. Om toch betrouwbare en eenduidige beeldvorming mogelijk te maken, gaan de veiligheidsregio's binnen elk onderdeel van de veiligheidsketen, actief op zoek naar overeenkomsten in de informatievoorziening. Daar waar overeenkomsten zijn, is ook voordeel te halen qua landelijk gedeelde informatievoorziening, gezamenlijke aanschaf van informatievoorzieningen of gedeelde eisen aan informatievoorziening. De overeenkomsten worden onderdeel gemaakt van de generieke basisarchitectuur, zodat alle regio's deze voordelen kunnen hergebruiken. Onderdeel van die basisarchitectuur is een gemeenschappelijk begrippenkader zodat gestandaardiseerde rapportages en informatie-uitwisseling onderling en met landelijk partners zoals de politie, Defensie of KNMI mogelijk zijn. De veiligheidsregio's zullen ondersteund door landelijke gremia en projecten, samen optrekken in de uitwerking van de gezamenlijke afspraken en de architectuur.

3 Informatieveiligheid en cyberweerbaarheid; aansluiten op vitale structuur

Eind 2024 zijn de veiligheidsregio's digitaal weerbaar en is hun eigen continuïteit gegarandeerd, volgens de Baseline informatiebeveiliging Overheid (BIO) en alle aanverwante geldende normen binnen de sector. Zij zijn in staat volwassen te acteren in de responsefase als onderdeel van de vitale sector.

Doordat informatievoorziening zo'n wezenlijke rol in de werkomgeving heeft gekregen, neemt het risico van digitale incidenten toe. De veiligheidsregio's worden inmiddels (h)erkend als vitale sector. Aansluiting op de nationale informatieveiligheidsstructuur ligt daardoor voor de hand. Naast preventieve maatregelen nemen veiligheidsregio's ook repressieve maatregelen voor digitale incidenten. De regio's organiseren naast hun eigen continuïteit en beveiliging op basis van de BIO, een team van specialisten die landelijk ondersteunt in die response. Monitoring (SOC) en response (CERT) zijn kernfuncties op het terrein van informatiebeveiliging. Bovendien bieden ze een basis voor andere functies; zowel intern (cyberweerbaarheid, bedrijfscontinuïteit) als extern (digitale ontwrichting in de maatschappij, verbinding met meldkamerfunctie, verbinding met crisispartners). De invulling voor deze functies wordt de komende jaren bepaald en ingericht. Veiligheidsregio's vervullen met VR-ISAC/SOC/CERT een volwaardige rol in het Landelijk Dekkend Stelsel (LDS) voor de cyberweerbaarheid van Nederland. Zij ontvangen beschikbare dreigingsinformatie en delen die met relevante partners binnen het LDS. Daarnaast worden in alle IV-projecten vanaf de start risico's en maatregelen op gebied van informatieveiligheid meegenomen (security by design).

Veiligheidsregio's moeten vanwege het vitale belang, 24/7 in staat zijn om hun werk te doen. Wanneer er sprake is van een verstoring in de informatievoorziening, zal een veiligheidsregio terug moeten kunnen vallen op een alternatief. In de komende tijd zal iedere regio afspraken maken over opvang van de informatievoorziening wanneer er sprake is van uitval.

4 Innoveren is noodzakelijk en doen we samen

Eind 2024 is de toepasbaarheid en de ethische aspecten van Artificiële Intelligentie onderzocht en vertaald naar standaarden die de regio's moeten implementeren.

Het blijven vernieuwen en ontwikkelen door innovaties uit de markt toe te passen en samen, maar ook met partners, te experimenteren, garandeert dat de informatievoorziening ook op orde blijft en maximaal wordt benut. Het doel van innovatie is versnelling te creëren in de ontwikkeling van de informatievoorziening en adaptief te worden op bruikbare nieuwe technologie. Relevante ontwikkelingen zijn momenteel: Artificiële Intelligentie (AI), Digital Twins (digitale kopieën van de werkelijkheid ten behoeve van onder andere planvorming en oefeningen) en robotisering. Om maximaal profijt te halen uit (inter-)regionale investeringen is het van belang om succesvolle innovaties ook breder toepasbaar te maken. Die innovaties worden gezamenlijk doorontwikkeld, zodat het eindproduct door het hele domein in gebruik kan worden genomen.

Wat betreft AI: het analytisch vermogen van de menselijke geest is beperkt. Informatiesystemen en algoritmen kunnen ons in de nabije toekomst ondersteunen in de analyse van grote hoeveelheden informatie. Het zetten van goede stappen vergt de nodige verkenning en een structurele ethische beschouwing door de regio's. Een aantal veiligheidsregio's is al gestart met deze verkenning door het experimenteren met deze techniek, daarbij gebruikmakend van kennis van experts. Onafhankelijk onderzoek geeft daarnaast een beeld over de toepasbaarheid en ethische aspecten. De ambitie is dit eind 2024 af te ronden.

5 Duidelijke wettelijke regelgeving voor datadeling

De nieuwe Wet veiligheidsregio's maakt het mogelijk dat alle noodzakelijke informatie voor rampenbestrijding, crisisbeheersing en brandweezorg te delen zijn.

Om informatie tussen partners te kunnen uitwisselen, zijn afspraken over het delen van data noodzakelijk. Daarbij gelden uitgangspunten als 'need to know', doel- en tijdbinding. De wetgever beschermt terecht het delen van privacygevoelige informatie. Bij rampen en crisis kan het echter noodzakelijk zijn datasets zonder belemmeringen

te delen. Hierin dient deze wet te gaan voorzien. Nu is er ruimte in de interpretatie van de wet, variërend van rekkelijk naar precies. Zo zou de voorzitter van de veiligheidsregio een bevoegdheid kunnen krijgen databronnen tijdelijk en voor een beperkte bewaartijd veilig te ontsluiten en zich daarover achteraf te verantwoorden.

De wetgever dient ook te voorzien in het vaststellen van een set standaarden wat het uitwisselen van datasets door betrokken partijen tijdens een ramp en/of crisis snel en eenvoudig mogelijk maakt (Open Source voor rampen en crises).

Bij datadeling in de koude en lauwe fase maken de regio's en hun partners gebruik van een netwerk van knooppunten en gaan uit van de basisprincipes: "Eénmalige opslag, meervoudig gebruik" en "Data blijft bij de bron". Daardoor is de kwaliteit van de data geborgd door de bronhouders. Gebruikers van de informatie koppelen bevindingen altijd terug en werken zo actief mee aan het actueel en correct houden van de brondata. Voor het delen van data is toegangscontrole volgens de wettelijke kaders ingericht, zodat de informatie niet in verkeerde handen kan vallen en onbruikbaar kan worden gemaakt of overgedragen aan de archiefhouder als de beschikbaarheid voor de operatie niet meer relevant of rechtmatig is.

de meldkamersystemen. Dat is te realiseren door op architectuurniveau, systeemniveau (koppelvlakken) en informatieniveau (datamodellen) afspraken te maken en door het verder inrichten van één gezamenlijk koppelpunt met de Landelijke meldkamersamenwerking (LMS). Bij opschaling en crisis zijn landelijke gestandaardiseerde afspraken noodzakelijk over de taken en rol van de calamiteitencoördinator als brug tussen regio's en meldkamer.

6 Versterken van de verbinding met de meldkamerfuncties

Eind 2024 zijn duidelijke afspraken over de informatiedeling tussen de veiligheidsregio's en de meldkamers gemaakt en geïmplementeerd.

Veiligheidsregio's fungeren in toenemende mate als knooppunten van informatie en leveranciers van een handelingsperspectief aan burgers. Via de meldkamer ontvangen veiligheidsregio's informatie over incidenten en de afhandeling ervan. De veiligheidsregio, politie en ambulancediensten kunnen de meldkamer op hun beurt voorzien van informatie die voortkomt uit processen van risicobeheersing en operationele voorbereiding. Met name wanneer sprake is van opschaling moet de informatievoorziening tussen meldkamer en hulpverleningsdiensten goed geregeld zijn. Daarom is het van belang informatievoorziening van de veiligheidsregio's goed af te stemmen op

juni 2022

versie 0.9



Raad van Commandanten
en Directeuren
Veiligheidsregio