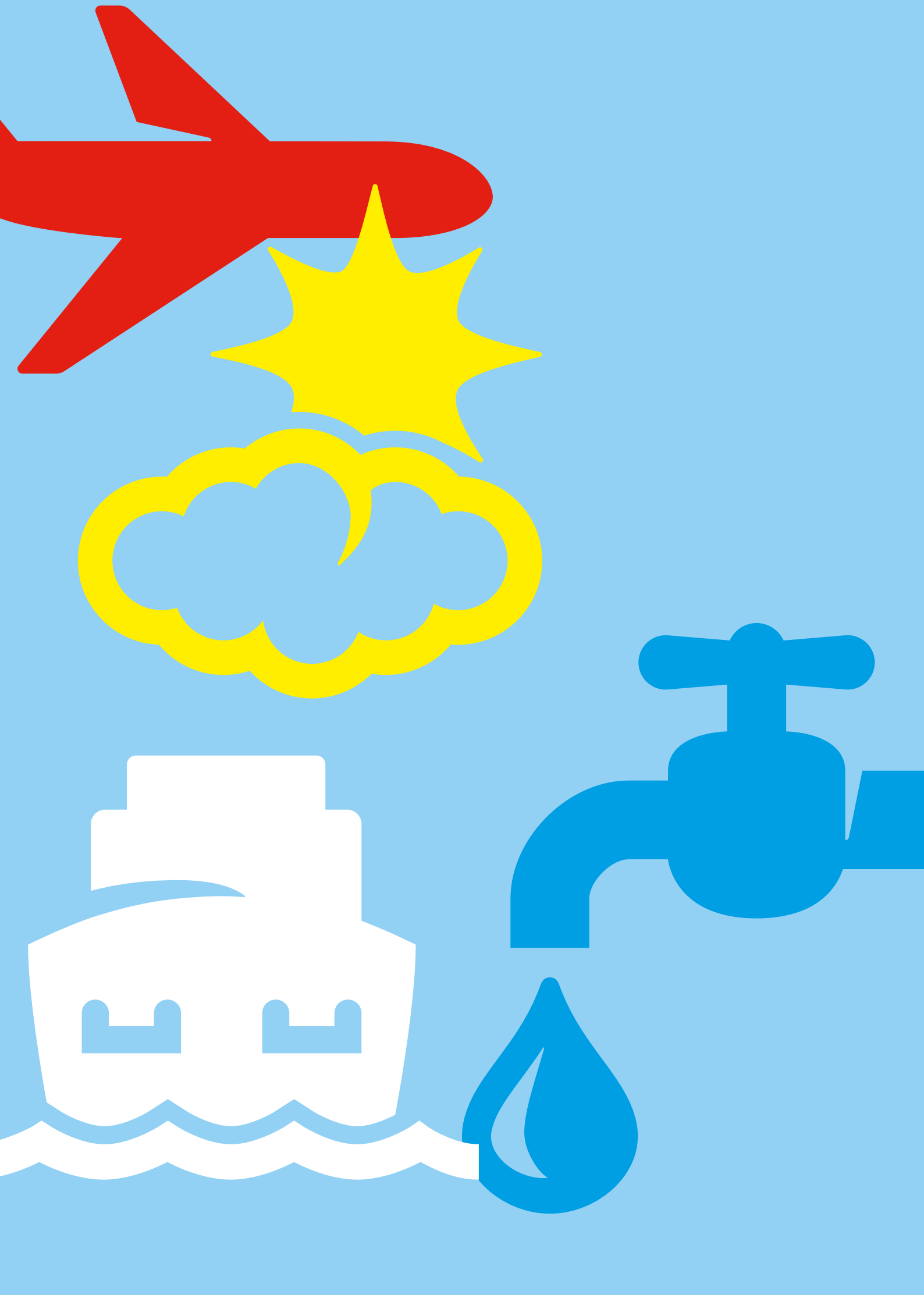
Ministerie van Infrastructuur
en Waterstaat

DCC-IenW

Beleidsplan Crisisbeheersing

2018-2022

Departementaal Coördinatiecentrum Crisisbeheersing



Beleidsplan Crisisbeheersing 2018-2022

Inhoud

Inleiding

Voor u ligt het Beleidsplan Crisisbeheersing 2018-2022. Dit beleidsplan is opgesteld vanuit de verantwoordelijkheid van het Departementaal Coördinatiecentrum Crisisbeheersing van het ministerie van Infrastructuur en Waterstaat (DCC-IenW) voor het opstellen en onderhouden van een coherent crisisbeheersingsbeleid, teneinde het ministerie voor te bereiden op het professioneel managen (voorkomen, beheersen en afhandelen) van crises. Dit beleidsplan bevat een meerjarig en richtinggevend kader waarin de verantwoordelijkheden en prioritaire risico-aandachtsgebieden op het gebied van crisisbeheersing staan opgenomen. Daarnaast wordt in dit plan aandacht besteed aan de organisatorische doorontwikkeling van crisismanagement binnen het departement. Een ***reflectie op het beleidsplan 2014-2017*** vindt u in ***hoofdstuk 1.***

Meer dan ooit staat Nederland bloot aan de gevolgen van mondiale veiligheidsontwikkelingen, of het nu gaat om het klimaat, geopolitieke ontwikkelingen, cybersabotage of internationale criminaliteit. Veel van deze ontwikkelingen hebben in steeds grotere mate impact op het werkveld van het ministerie van Infrastructuur en Waterstaat (IenW). Zo kan een cyberaanval op de digitale infrastructuur van de Rotterdamse haven grote gevolgen hebben voor het afhandelen van de zeescheepvaart en kan bijvoorbeeld een vliegtuigkaping het verkeer in de wijde omtrek van Schiphol ernstig verstoren. In deze gevallen en vele andere is nadrukkelijk een rol weggelegd voor het ministerie van IenW.

Om een beter beeld te krijgen van alle relevante ontwikkelingen voor IenW is het beleidsplan in 3 stappen opgebouwd:

1. Om een goed beeld te krijgen van alle (inter)nationale ***veiligheidsontwikkelingen*** en de relevantie voor de beleidsvelden van IenW is gebruik gemaakt van:
   - het Nationaal Veiligheidsprofiel
   - de door TNO en HCSS uitgevoerde inventariserende studie en de bilaterale interviews met betrokkenen van IenW en van ketenpartners. In Bijlage A vindt u het volledige rapport van HCSS/TNO.

   In de ***hoofdstukken 2 en 3*** wordt ingegaan op het Nationaal Veiligheidsprofiel én de relevante issues voor IenW en haar ketenpartners;
2. Om duidelijk te krijgen wat de kansen/bedreigingen én sterktes/zwaktes van de huidige crisisbeheersing zijn bij IenW en haar ketenpartners is een interactieve SWOT analyse uitgevoerd waaraan ongeveer 50 betrokkenen hebben deelgenomen. De uitkomsten van deze ***SWOT analyse*** zijn opgenomen in ***hoofdstuk 4;***
3. De ***synthese*** van ***de Veiligheidsontwikkelingen en van de SWOT analyse*** heeft plaatsgevonden in een afsluitende sessie in het LEF Future Center met een 25-tal betrokkenen én is opgenomen in ***hoofdstuk 5.***

In ***hoofdstuk 6*** is een ***beleidsagenda 2018-2022*** opgenomen waarin concrete activiteiten, actiehouders en planjaren zijn opgenomen.

Tenslotte wordt in ***hoofdstuk 7*** voorgesteld om het 'Beleidsplan Crisisbeheersing IenW' niet met een cyclus van 4 jaar te actualiseren, maar het meer een ***'levend' en actueel richtinggevend*** document te laten zijn voor de crisisbeheersing van IenW en haar crisispartners.

1 Reflectie op het Crisisbeheersingsplan 2014-2017

Onder verantwoordelijkheid van DCC-IenW is het Beleidsplan Crisisbeheersing 2014-2017 opgesteld. Het plan diende richtinggevend te zijn op zowel inhoudelijke thema's als op de organisatie van crisisbeheersing bij IenW. Daarnaast stond het beleidsplan onder meer in het teken van het incorporeren van de crisistypen en crisisorganisatie van het voormalige ministerie van VROM bij het DCC-IenW.

Een aspect waaraan minder aandacht was besteed betrof een meer uitgebreide beschouwing en beschrijving van (inter)nationale veiligheidsvraagstukken. Teneinde een meer robuuste kennisbasis te hebben ten aanzien van (inter)nationale veiligheidsissues is in dit nieuwe Beleidsplan Crisisbeheersing 2018-2022 veel aandacht gegeven aan mondiale ontwikkelingen in het veiligheidsdomein en de potentiële impact daarvan op risico- en crisisbeheersing. Zie bijlage A.

1.1 Behaalde doelen en voortgang inhoudelijke en organisatorische thema's

Inhoudelijke thema's

De inhoudelijk belangrijkste thema's en resultaten zijn:

- **Cyber.** Op het gebied van cybercrises is een groot aantal activiteiten uitgevoerd. Zo is de Expertgroep Cyber IenW opgezet en beoefend om cybercrises bij IenW inhoudelijk te bestrijden. De Expertgroep staat onder voorzitterschap van de *Chief Information Officer* (CIO) IenW; hoofd FMC. Een handboek met daarin het responsproces voor cybercrises en alle verantwoordelijkheden en bevoegdheden van de deelnemende IenW experts wijst de Expertgroep de weg. Ook het Nationaal Cyber Security Centrum (NCSC) is lid van de Expertgroep. Om de expertise bij IenW nog beter te bundelen is het Security Operation Centre (SOC) van Rijkswaterstaat (RWS) haar takenpakket aan het uitbreiden zodat het ook niet-RWS onderdelen van IenW kan bedienen. Onder regie van de CIO IenW wordt er een IenW-breed Meldloket ingericht voor cyber-incidenten voor nationale en Europese wetgeving: NL Meldplicht datalekken, NL Cybersecuritywet en EU NIB richtlijn (Netwerk en Informatie Beveiliging).
- **Satellietuitval.** Onder verantwoordelijkheid van Directoraat-Generaal Milieu en Internationaal (DGMI) is het project Inventarisatie Kwetsbaarheden Uitval Satellietnavigatie (IKUS) uitgevoerd. Het project is nationaal opgepakt omdat het ook allerlei sectoren buiten IenW raakt. Het is aan de sectoren binnen en buiten IenW om de resultaten uit het project te gebruiken en eventueel preventieve maatregelen te implementeren. In de luchtvaart en scheepvaart staat het thema GNSS (Global Navigation Satellite System) op de internationale agenda. Met het beschikbaar komen van het Europese satellietsysteem Galileo is er ook weer een nieuwe loot aan de GNSS stam bijgekomen. IenW richt samen met alle nationale partners de Public Regulated Service van het Europese Galileo-programma voor satellietnavigatie in. Dit regelt het beveiligd gebruik door geautoriseerde partijen van deze satellietnavigatie. IenW richt daartoe zelf als verantwoordelijk ministerie de Competent PRS Authority in.
- **Caribisch Nederland.** Voor Caribisch Nederland zijn de risico's in kaart gebracht en is de samenwerking vanuit het departement/DCC-IenW tot stand gebracht. Ook zijn er gezamenlijke crisisbeheersingsoefeningen gehouden.
- **Waterveiligheid.** Om het risicobewustzijn en de zelfredzaamheid van burgers ten aanzien van overstromingen te versterken is het project Module Evacuatie Grote Overstromingen uitgevoerd. Naast de website 'Overstroom ik' heeft het project o.a. geresulteerd in een aantal effectieve maatregelen om te 'Evacueren, als het tóch gebeurt'. Voor de noodpompen van IenW (in beheer bij RWS) is nu ook een zogenaamde EU module ingericht en afgesproken dat deze noodcapaciteit voor de gehele EU beschikbaar is indien noodzakelijk.

Organisatorische thema's

Organisatorisch is de afgelopen beleidsperiode veel inspanning gegaan naar het integreren van alle crises-typen en crisesorganen van het voormalige ministerie van VROM en van de nucleaire veiligheid zoals door ministerie van Economische Zaken (EZ) overgedragen is aan IenW. Hiervoor is de Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS) opgezet. Om het een en ander ook regionaal goed te effectueren hebben de Hoofdingenieur-directeuren (HID-en) van de regionale diensten van RWS de rol gekregen van Bestuurlijke Verbindingsschakel. Met de overdracht van het Bureau Crisis Expert Team – milieu en drinkwater (CET-md) en het Landelijk Laboratoriumnetwerk terreuraanslagen (LLN-ta) van de ILT naar het DCC-IenW per 1 januari 2017 heeft de ILT nu al haar crisiswerk overgedragen naar het DCC-IenW. Ook de harmonisatie van de kennis- en adviesstructuur zoals vastgesteld door de Stuurgroep Nationale Veiligheid naar aanleiding van de brand bij Chemie-Pack in Moerdijk is nu geïmplementeerd zoals voorgesteld in het rapport 'Eenheid in Verscheidenheid'.

In het crisisinformatiesysteem Integrale Crisis Advies Website (ICAweb) van IenW zijn alle organisatorische en functionele aanpassingen doorgevoerd. Tegelijkertijd is het ICAweb vernieuwd zodat het ook op laptops en tablets gebruikt kan worden. Met het Instituut Fysieke Veiligheid (IFV) is door RWS een contract getekend om het Landelijke Crisis Managementsysteem (LCMS) zowel bij RWS als bij het DCC-IenW te kunnen gebruiken. Hierdoor worden RWS en het DCC-IenW meer deelgenoot van de regionale en nationale crisisbeheersing bij het maken en gebruiken van een éénduidig beeld van de crisis.

2 Veiligheidsontwikkelingen

Nationale en internationale veiligheidsontwikkelingen hebben Nederland al van oudsher geraakt. In die zin is er niet veel nieuws onder de zon. Het verschil vandaag de dag ligt hem in het feit dat de veelheid van relevante ontwikkelingen aan het toenemen is, dat de voorspelbaarheid van het manifesteren ervan kleiner wordt, en dat deze ontwikkelingen meer in elkaar grijpen en zo tot een complexe crisis kunnen leiden. Een cyberaanval kan bijvoorbeeld door een niet-statelijke actor worden georkestreerd en leiden tot het ontregelen van chemische installaties. Dit kan weer tot vervuiling van oppervlaktewater leiden, waardoor buurten moeten worden ontruimd, met alle sociale en economische schade van dien. De precieze ontwikkeling van zulke crises is vaak moeilijk te voorzien. Het is wel mogelijk om te zorgen dat er voldoende bewustzijn is over de mogelijke risico's waaraan Nederland kan worden blootgesteld, ook in domeinen die voor IenW wellicht minder voor de hand liggen, maar wel impact op haar beleidsterrein kunnen hebben. Alleen op basis van een dergelijk bewustzijn kunnen de beste analyses worden gemaakt, kan de organisatie worden geprepareerd en kunnen benodigde middelen worden gealloceerd.

Om zicht te krijgen op alle (inter)nationale ontwikkelingen is een groot aantal nationale en internationale bronnen geraadpleegd. Het Nederlandse Nationaal Veiligheidsprofiel (NVP) heeft als leidraad gediend om zicht te krijgen op hetgeen er in Nederland speelt en in welke mate het van invloed is op de beleidsvelden van IenW.

Het NVP geeft een overzicht van de risico's van verschillende rampen, crises en dreigingen met een mogelijk ontwrichtend effect op onze samenleving. Er is sprake van een mogelijk ontwrichtend effect op de samenleving als één of meer van de vijf vitale nationale veiligheidsbelangen ernstig worden aangetast:

De vijf nationale veiligheidsbelangen

***Territoriale veiligheid**: "Het ongestoord functioneren van Nederland als onafhankelijke staat in brede zin, dan wel de territoriale integriteit in enge zin."*

***Fysieke veiligheid**: "Het ongestoord functioneren van de mens in Nederland en zijn omgeving."*

***Economische veiligheid**: "Het ongestoord functioneren van Nederland als een effectieve en efficiënte economie."*

***Ecologische veiligheid**: "Het ongestoord blijven voortbestaan van de natuurlijke leefomgeving in en nabij Nederland."*

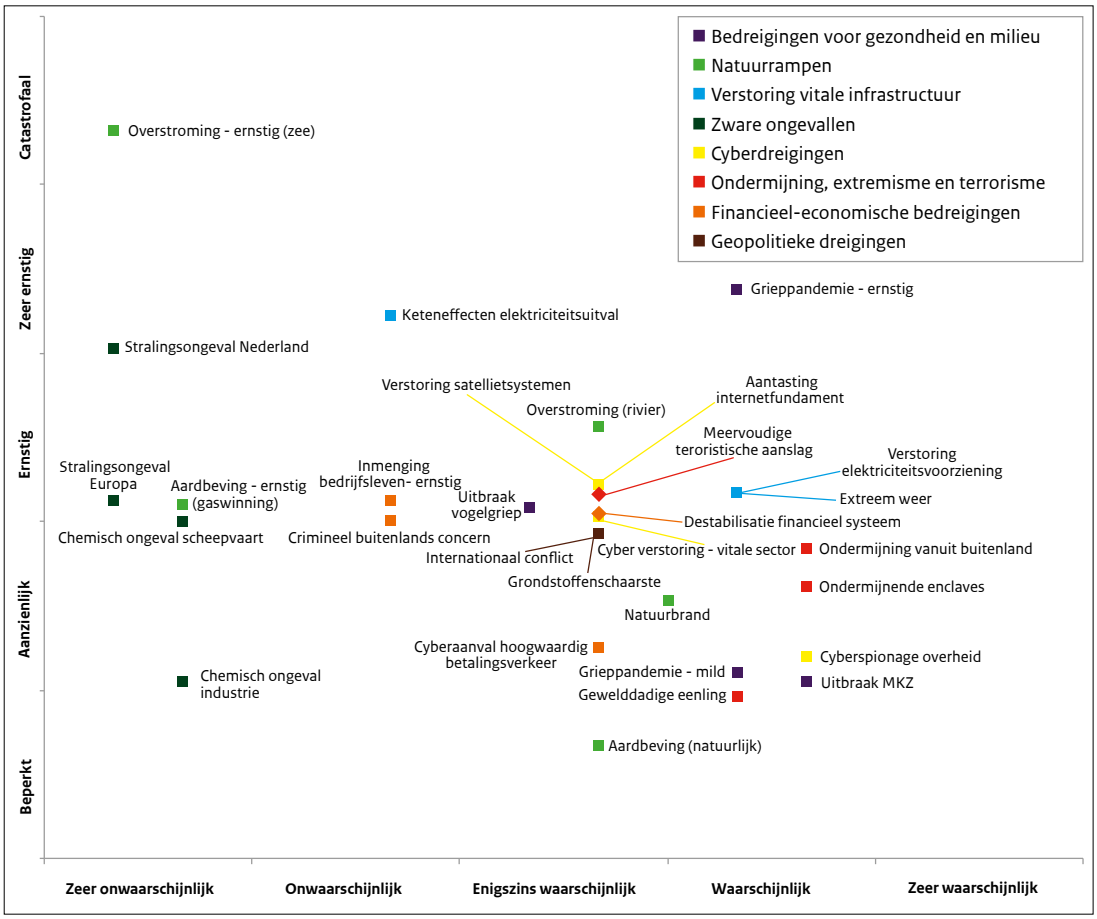
***Sociale en politieke stabiliteit**: "Het ongestoorde voortbestaan van een maatschappelijk klimaat waarin individuen ongestoord kunnen functioneren en groepen mensen goed met elkaar kunnen samenleven binnen de verworvenheden van de Nederlandse democratische rechtstaat en daarin gedeelde waarden."*

Om de ernst (impact) van een potentiële ramp of crisis te bepalen zijn deze nationale veiligheidsbelangen uitgewerkt in een aantal criteria. Zo wordt bijvoorbeeld bij 'fysieke veiligheid' gekeken naar het aantal doden, ernstig gewonden, chronisch zieken en het gebrek aan primaire levensbehoeften zoals voedsel, drinkwater en energie. Van elk type ramp is bepaald hoe waarschijnlijk het is dat deze zich voordoet.

In het NVP zijn acht verschillende thema's geanalyseerd: Natuurrampen, Bedreigingen voor gezondheid en milieu, Zware ongevallen, Verstoring vitale infrastructuur, Cyberdreigingen, Ondermijning/extremisme/terrorisme, Geopolitieke dreigingen Financieel-economische bedreigingen.

Risicodiagram
Om een beeld te krijgen van de relatieve ernst en waarschijnlijkheid van alle risico's zijn ter illustratie scenario's uitgewerkt die een mogelijke ramp, dreiging of crisis beschrijven. Deze zijn gebruikt voor de beoordeling van de impact en waarschijnlijkheid, zodat deze risico's onderling kunnen worden vergeleken. Daarnaast zijn per thema de belangrijkste ontwikkelingen en capaciteiten beschreven, zodat de uitgewerkte scenario's in de juiste context kunnen worden geplaatst.

*De uitkomsten van de beoordeling worden gepresenteerd in het **risicodiagram**. In dit diagram staat op de verticale as de totale impact. Die is berekend op basis van de individuele impactscores (optelsom van impact op territoriale veiligheid, fysieke veiligheid, economische veiligheid, etc). De schaal loopt op van beperkt tot catastrofaal. Op de horizontale as staat de waarschijnlijkheid. Beide assenzijn logaritmisch: zeer waarschijnlijk is tien keer zo hoog als waarschijnlijk, et cetera.*



Figuur 1. Risicodiagram

Naast het NVP zijn er op basis van (inter)nationale trendontwikkelingen en de gehouden interviews (zie Bijlage B, betrokkenen fase 1) een aantal thema's te benoemen die door alle sectoren en IenW beleidsterreinen heen van belang zullen zijn of worden. Wij onderscheiden hier de volgende thema's en ontwikkelingen:

- afhankelijkheid van cyber
- demografische ontwikkelingen
- toename in terroristische/criminele activiteiten
- klimaatverandering
- leren van incidenten/oefeningen en *serious gaming*
- digitalisering
- mediatisering

3 Prioritering veiligheidstrends

Om tot een vernieuwde inhoudelijke prioritering te komen zijn de verschillende soorten dreigingen uit figuur 1 hieronder doorvertaald naar de diverse beleidsterreinen van IenW (zie figuur 2). Om tot een goede prioritering te komen van de belangrijkste bedreigingen voor IenW is gekeken naar:

- *Relevantie*
  - De mate van bekendheid en georganiseerdheid van IenW met het type crisis. Onbekende en/of nog niet goed georganiseerde crises hebben een hogere prioriteit.
  - De mate van waarschijnlijkheid en potentiële impact van de betreffende crisis (de gebruikelijke risico-matrix, zie figuur 1)
- *Het organisatievermogen van DCC-IenW, in samenhang met crisisbeheersing binnen IenW als geheel:*
  - De ambities en organisatorische mogelijkheden in de komende periode (2017-2021) vormen de belangrijkste maatstaf voor de omvang en reikwijdte van het beleidsplan. Vooralsnog wordt uitgegaan van het voorbereiden en oefenen van minimaal twee grootschalige (interdepartementale, omvangrijke) crises per jaar, waarbij met name geoefend kan worden op het verbeteren van de interdepartementale samenwerking, netcentrisch werken en crisiscommunicatie (bestuurlijk en operationeel). De duur van de oefening, inclusiviteit (betrekken van burgers) en interactie (gericht op optimaliseren ketensamenwerking en leren) vormen hierbij de nader in te vullen bestanddelen. Daarnaast wordt een palet aan bedreigingen voorgesteld waarbij of vernieuwing (onbekendheid met een crisistype) of intra-departementale samenwerking en onderhoud van geoefendheid voorop staat. De aanbevelingen uit de LEF-sessie zijn hierbij integraal meegenomen.

Uit het onderzoek zijn de volgende prioritaire bedreigingen en organisatorische vraagstukken naar voren gekomen[1]:

	Werkt organisatorisch goed	Ruimte voor organisatorische verbetering
Belangrijke dreiging	**Onderhouden/versterken:** stijging waterpeil, extreem weer, vervuiling oppervlaktewater, cybercriminaliteit.	**Investeren:** ketenafhankelijkheden, cybersecurity (aantasting internetcapaciteit), stralingsongevallen (nucleair), terrorisme (plus aanslagen/kapingen).
Minder belangrijke dreiging	**Ruimte voor efficiëntere inzet:** aardbevingen/ bodemdalingen(gaswinning), infectieziekten humaan, dierziekten, voedselveiligheid, voedselzekerheid, antibioticaresistentie, verlies biodiversiteit, luchtvervuiling, geluidsoverlast, gebrekkige waterafvoer, verzilting, afname visstand, genetische manipulatie, chemische ongevallen, gebrek koelwater energiecentrales, cyberspionage, criminaliteit met geweld, disruptie handelsverkeer, drugsafvalvervuiling, corruptiegevaar.	**Beperkte aandacht:** crisisbeheersing BES eilanden, droogte en hitte, natuurbranden, zonnestormen, milieurampen, omgevings-besmetting, plagen (BES eilanden), drinkwater-tekorten, drinkwatervoorziening, transport-ongevallen, explosies/stadsbranden, common causes, verstoring automatisering IACS, piraterij (BES eilanden), migratie/vluchtelingenstromen, criminele inmenging.

Figuur 2: Koppeling veiligheidsdreigingen en organisatorische inzet

[1] *De mogelijke dreigingen die in het NVP staan waarvan is vastgesteld dat deze niet of slechts zeer zijdelings van relevantie zijn voor IenW zij hierin niet meegenomen.*

De belangrijkste dreigingen waar meer aandacht naar uit moet gaan, hetzij om inhoudelijke dan wel organisatorische redenen, zijn daarmee de volgende:

3.1 Ketenafhankelijkheden/effecten

Keteneffecten ontstaan wanneer de uitval van één vitaal proces, direct of op termijn, leidt tot uitval van andere vitale processen. In het algemeen is de maatschappelijke afhankelijkheid van energievoorzieningen, ICT en telecom, drinkwater en betaalverkeer groot. Uitval van bijvoorbeeld het betaalverkeer heeft grote gevolgen voor het functioneren van infrastructuur zoals mainports en openbaar vervoer. Bij telecommunicatie geldt feitelijk hetzelfde: alle vormen van vervoer en infrastructuur worden hierdoor geraakt. Voor IenW zijn keteneffecten relevant voor bijna alle beleidsterreinen.

Het NVP stelt dat er veel maatregelen zijn getroffen waardoor grootschalige, langdurige uitval van vitale processen onwaarschijnlijk is. Het NVP noemt naast de globale trends van toenemende digitalisering en afhankelijkheid van elektriciteit, ICT en telecommunicatie *geen* specifieke ontwikkelingen waardoor de waarschijnlijkheid van – negatieve – keteneffecten op korte termijn toeneemt.

Binnen IenW wordt het idee geuit dat vooral bij de risicobeheersing er meer kennis moet worden opgedaan op dit thema, en dat leereffecten beter moeten worden benut. In de huidige crisisorganisatie wordt veelal rekening gehouden en voorbereid op 'afgebakende' crisissituaties binnen bepaalde sectoren. Zoals opgemerkt tijdens in de SWOT analyse: "We zijn in de warme fase echt nog ver verwijderd van een integrale aanpak, ongeacht wat voor soort crisis zich voor doet." Met de toenemende complexiteit van crisissituaties groeit ook bij IenW het besef dat zij steeds afhankelijker is van haar ketenpartners en omgekeerd. Deze ketenafhankelijkheden blijven grotendeels onbekend en moeten beter in kaart moeten worden gebracht, uiteraard in lijn met de aandacht voor ketenafhankelijkheden vanuit de NCTV en de IenW werkgroep Vitaal. Ook het (verder) invoeren van netcentrisch werken is noodzakelijk om de samenwerking met ketenpartners te versterken.

3.2 Cybersecurity: aantasting internetcapaciteit

Bij aantasting van internetcapaciteit is het op voorhand niet duidelijk welke verbindingen wel en welke geen doorgang meer vinden. Het effect van verstoring van internetcapaciteit is min of meer gelijk aan verstoring van telecommunicatie. Deze risicocategorie heeft mogelijk gevolgen voor bijna alle beleidsterreinen van IenW, in ieder geval voor wegvervoer, spoor- en openbaar vervoer, zeescheepvaart, havens en Noordzee, luchtvaart, waterkwantiteit en kwaliteit, buisleidingen, drinkwater en binnenvaart, omdat belangrijke processen in deze sectoren gebruik maken van internetverbindingen. Wanneer deze risicocategorie zich veelvuldig manifesteert raakt dat de ambitie om van Nederland een knooppunt van excellente verbindingen en een land van slimme steden te maken.

Het internet is zo opgebouwd dat grootschalige uitval zeer onwaarschijnlijk is, maar individuele providers kunnen wel worden getroffen. De aanwezigheid in Nederland van mondiale knooppunten als de Amsterdam Internet Exchange vormen wel extra kwetsbare punten. In het NVP wordt aangegeven dat de kern van het Internet (de zogenaamde backbone zoals de IP en BGP protocollen) ook aangetast kan worden in termen van integriteit en vertrouwelijkheid. Hierdoor zouden dataverbindingen kunnen worden gemanipuleerd of afgeluisterd.

Thematisch gezien moet er interdepartementaal meer aandacht voor dit thema komen, en moet de kennisbasis worden opgebouwd, zelfs als de primaire verantwoordelijkheid bij het NCSC ligt. Ook samenwerking tussen ketenpartners, bijvoorbeeld in de private sector, is nog nauwelijks ontwikkeld. Kennis van de private sector is essentieel om complexe problemen aan te pakken.

3.3 Stralingsongevallen

Met de oprichting/overgang van de ANVS van het ministerie van Economische Zaken naar IenW is ook het beleidsterrein nucleaire veiligheid bij het laatstgenoemde departement komen te liggen. De risicocategorie stralingsongevallen is daarmee naast de ANVS en de ILT ook zeer relevant geworden voor het departement zelf. Grote stralingsongevallen zouden zich kunnen voordoen in Borssele en in nabijgelegen centrales (Doel, Tihange en Lingen).

Voor de impact van stralingsongevallen zijn omstandigheden zoals het weer en het seizoen van grote invloed. Daardoor kan een ongeval verder weg in Europa een even grote of grotere impact hebben dan een ongeval in Nederland of vlak over de grens. De impact van een groot stralingsongeval wordt als zeer groot geschat. Het NVP schetst ook hoe de kernenergiemix in beweging is binnen Europa. Verder wordt in het NVP rekening gehouden met de mogelijkheid van transportongevallen. Deze laatsten worden als meer waarschijnlijk maar beperkt van impact geschat.

Op dit dossier moet IenW als nieuwe portefeuillehouder nog meer duidelijkheid ontwikkelen over wat precies de rol van het ministerie is.

3.4 Extremisme en terrorisme

De risicocategorie extremisme en terrorisme is met name relevant voor IenW omdat verschillende potentiële doelwitten onder de beleidsterreinen van het departement vallen. Daarbij liggen met name weg-, spoor- en openbaar vervoer, zeescheepvaart, havens en Noordzee en luchtvaart voor de hand, maar kan ook worden gedacht aan waterkwantiteit en kwaliteit, buisleidingen, drinkwater en binnenvaart. De risicocategorie is daarmee relevant voor het hele departement.

Uitval van voorzieningen als gevolg van een aanslag wordt behandeld binnen het thema vitale infrastructuur. Uiteraard is bij terroristische aanslagen, kapingen en dergelijke de sociaal maatschappelijke impact groter dan bij natuurlijke oorzaken of ongevallen. Het NVP noemt verschillende ontwikkelingen waar met zorg naar wordt gekeken, zoals mogelijke toename van extremisme, immigratie en geopolitieke conflicten. De deelname van Nederland aan de coalitie tegen IS maakt dat de terroristische dreiging in ieder geval op korte en middellange termijn substantieel is.

Op dit onderwerp stellen betrokkenen dat er meer kan worden geleerd van incidenten, en dat er meer aandacht nodig is voor preventieve maatregelen, met name bij de beveiliging van vitale infrastructuur. Ook het functioneren van het Alerteringssysteem Terrorismebestrijding dient tegen het licht te worden gehouden[2].

[2] *Er loopt op dit moment een activiteit van de NCTV, met betrokkenheid van IenW, om het ATb meer te integreren met de nationale besluitvormingsstructuur van de crisisbeheersing.*

4 SWOT analyse Crisisbeheersing IenW

Om de kansen/bedreigingen en sterkten/zwaktes duidelijk te krijgen is met het ICT systeem Synmind een interactieve SWOT analyse uitgevoerd waaraan ongeveer 50 mensen hebben deelgenomen uit de crisis-organisatie van IenW en haar ketenpartners. Tijdens de interactieve sessie konden deelnemers met elkaar in discussie gaan en waren moderatoren actief om toelichtingen van deelnemers te vragen. In de tabel[3] hieronder is aangegeven hoe de deelnemers de kansen/bedreigingen/sterkten/zwaktes zien.

Vraag	Aspect crisis- of risicobeleid	Zeer zwak	Vrij zwak/ onvoldoende	Matig	Vrij sterk/ voldoende	Zeer sterk
1.5	Bijdrage crisisbeheersing			18%	65%	18%
1.6	Kwaliteit van oefeningen en trainingen			15%	69%	15%
1.4	Omschrijving rol crisisbeheersing			27%	59%	14%
1.1	Omschrijving rol risicobeheersing		4%	16%	76%	4%
1.3	Risicoanalyses			27%	73%	
1.2	Bijdrage risicobeheersing			47%	53%	
1.8	Samenwerking en communicatie IenM		9%	27%	64%	
1.10	Samenwerking en communicatie ketenpartners		7%	33%	60%	
1.9	Samenwerking en communicatie interdepartementaal		16%	47%	37%	
1.11	Samenwerking en communicatie burgers, private en publieke organisaties	7%	33%	27%	33%	
1.7	Gebruik ICT		19%	75%	6%	
1.12	Risico en crisisbeleid t.a.v. BES-eilanden		33%	33%	33%	

Figuur 3: uitkomsten Synmind sessie over crisis- en risicobeleid

Uit dit overzicht blijkt dat vooral op de punten van interdepartementale samenwerking, crisiscommunicatie, het gebruik van ICT bij crises en risico- en crisisbeleid ten aanzien van de BES-eilanden meer aandacht of nieuwe investeringen nodig blijven.

[3] *De bijdrage crisisbeheersing betreft de bijdrage van IenW aan het bepalen en uitvoeren van wet- en regelgeving, crisisplannen en procedures én over de effectiviteit van beleid en de inzet van middelen voor crisisbeheersing. De bijdrage risicobeheersing gaat over de transparantie en eenduidigheid van de rol en verantwoordelijkheden van IenW bij het bepalen en uitvoeren van risico-reducerende maatregelen, wet- en regelgeving, het verlenen van vergunningen en handhaving.*

4.1 Taken en verantwoordelijkheden van IenW en haar ketenpartners

IenW is verantwoordelijk voor een aantal complexe beleidsterreinen. Dit heeft invloed op de crisisbeheersingsorganisatie. Uit gesprekken met beleidsmedewerkers en ketenpartners is gebleken dat de rollen, taken en verantwoordelijkheden van IenW en haar ketenpartners ten aanzien van de crisisbeheersing niet altijd duidelijk zijn. Wat juridisch gezien onder de verantwoordelijkheid van IenW valt en wat onder andere departementen en veiligheidsregio's, is voor veel betrokkenen niet altijd duidelijk. Zo is gesteld dat "de onduidelijkheid zowel de interdepartementale rollen als de rolverdeling tussen departement en regio betreft."

Deze onduidelijkheid raakt tevens aan verwachtingen over de rol van IenW. Tijdens een crisis wordt het DCC-IenW gezien als spin in het web, maar met de kanttekening dat de verhouding tussen het DCC-IenW en de beleidsdirecties in de warme fase niet altijd helder is. De samenhang met de rollen van ketenpartners is ook niet altijd duidelijk: "In de praktijk blijkt nog regelmatig dat de uitvoering van de rol van IenW niet aansluit bij de verwachtingen bij onze partners".

4.2 Aandacht voor crisiscommunicatie

Communicatie tijdens crisis moet zo helder, open en transparant mogelijk zijn. Situaties zoals in Japan waarbij veel onduidelijk bleef na de ontploffing van een nucleaire reactor kunnen leiden tot wantrouwen ten opzichte van de overheid. Crisismanagement is ook een kwestie van verwachtingsmanagement. Burgers zijn steeds mondiger en willen eerlijk en het liefst zo snel mogelijk geïnformeerd worden. De behoefte aan informatie tijdens een crisis is groot en hier moet adequaat op worden ingespeeld.

Sociale media spelen een belangrijke rol in de groeiende informatiebehoefte. De rol die sociale media kunnen spelen tijdens een crisis is vooralsnog een onderbelichte kwestie binnen IenW. Een goed voorbeeld van het proactief benutten van sociale media is het 24-uurs social media team van de NS. Te allen tijde kunnen mensen vragen stellen, wordt er zo snel mogelijk gereageerd en daarnaast speelt de NS zelf in op actuele zaken. 24/7 is er bezetting en wordt informatie gemonitord. Het monitoren van 'live' informatie kan ook voor IenW tijdens een crisis zeer relevant zijn. Het monitoren van sociale media geeft inzicht in waar wat zich afspeelt, waar burgers actief zijn en waar een dringende behoefte aan hulp bestaat. Ook kan IenW zelf actief communiceren via sociale mediakanalen. Daarbij is naast de grote sociale mediaplatforms ook aandacht voor regionale netwerken gewenst. Zoals verwoord door een ketenpartner: "Als we goed duidelijk kunnen maken wat de eigen verantwoordelijkheid is en wat we als overheid te bieden hebben (en wat ook niet), dan kan de samenleving ook uitstekend helpen bij het bestrijden van crises." Hiervoor is veelal een andere mind-set gewenst in de huidige crisisbeheersing en moeten risico- en crisiscommunicatie een meer interactief dan directief karakter krijgen.

4.3 Gebruik ICT en digitale middelen bij crisis[4]

Technologische ontwikkelingen bieden zowel kansen als bedreigingen voor de crisisorganisatie van IenW. Ontwikkelingen in ICT leiden in het algemeen tot een steeds grotere afhankelijkheid van ICT systemen, zo ook in de beleidsterreinen van IenW en IenW zelf. Deze afhankelijkheid maakt de continuïteit van informatiesystemen binnen IenW belangrijk, zeker tijdens crisissituaties. Meerdere gesprekspartners hebben aangegeven dat de robuustheid van de bestaande ICT systemen beperkt is, waardoor er tijdens een crisis niet op vertrouwd kan worden. Het huidige crisisinformatiesysteem ICAweb wordt verder omschreven als gebruiksonvriendelijk, gecompliceerd, en niet goed aansluitend bij de huidige behoefte aan informatiedeling. Daarnaast heeft het systeem beperkte interactie met andere systemen, zoals systemen die door ketenpartners en crisisteams worden gebruikt.

ICT-ontwikkelingen bieden ook kansen, bijvoorbeeld voor verdere ontwikkeling van netcentrisch werken of het gecentraliseerd uitwisselen van informatie met veel verschillende ketenpartners. Om een goede regie over informatiesystemen en data-uitwisseling te houden zijn kennis en kunde van de systemen noodzakelijk.

[4] *Er loopt een traject om zowel het DCC-IenW als RWS (als de uitvoeringsorganisatie van IenW) aan te sluiten op LCMS, het crisisinformatiesysteem van VenJ en de Veiligheidsregio's.*

Deze is nu beperkt in de organisatie aanwezig. Informatiedeling en het inzetten en delen van kennis met ketenpartners is hiervoor een mogelijke oplossing. In de gesprekken over het gebruik van ICT is meermaals benadrukt dat ICT en digitale communicatiemiddelen ten behoeve van risico- en crisisbeheersing niet als doel op zich moeten worden gezien maar slechts als middel.

4.4 Rollen en verantwoordelijkheden ten aanzien van de BES-eilanden

Bonaire, Sint Eustatius en Saba vormen samen de BES-eilanden of Caribisch Nederland. Sint Eustatius heeft een haven met een grote petrochemische opslag en de capaciteit om grote olietankers aan te laten meren.[5] Deze grote petrochemische inrichtingen vallen onder de verantwoordelijkheid van IenW, samen met de luchtvaart op de eilanden en de drinkwatervoorziening.

Sinds 2010 hebben de BES-eilanden de status van 'bijzondere gemeente' binnen het Koninkrijk der Nederlanden. Met deze bestuurlijke wijziging zijn ook de taken en verantwoordelijkheden van het ministerie van IenW veranderd. Zo is IenW de bevoegde vergunningverlener voor grote industriële inrichtingen, bouwwerken op zee en scheepsactiviteiten, en verantwoordelijk voor de luchthavens en de voorbereiding en uitvoering van rampenbestrijding bij maritieme incidenten. De uitvoering van deze verantwoordelijkheid is grotendeels bij RWS belegd en toezicht en handhaving bij de ILT. De stelselverantwoordelijkheid voor de brandweerzorg, rampenbestrijding en crisisbeheersing[6] – waaronder de wet- en regelgeving – ligt bij de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) van het ministerie van Justitie en Veiligheid.

De bijzondere bestuurlijke positie van de BES-eilanden maakt dat de verdeling van verantwoordelijkheden voor rampenbestrijding en crisisbeheersing afwijkt van de verdeling in Nederland. De verdeling van verantwoordelijkheden, rollen en taken tussen de Openbare Lichamen (bestuurscolleges van de eilanden), IenW, RWS, de ILT en het ministerie van Justitie en Veiligheid kan daardoor moeilijk te vatten zijn. De rolverdeling ten aanzien van risico- en crisisbeheersing op de BES-landen is nog niet volledig uitgewerkt en bekend bij de verschillende beleidsdirecties en ketenpartners. Hierdoor bestaan er ook zorgen over de veiligheid van grote inrichtingen en de mate van voorbereidheid op grote incidenten die geadresseerd dienen te worden.

Door de beperkte hulpverleningscapaciteit en het gebrekkige zicht op de mate van voorbereiding op grote incidenten zijn de BES eilanden mogelijk sterk afhankelijk van bijstand en zelfredzaamheid. Daarnaast is naar aanleiding van inspecties handhaving opgestart voor alle geïnspecteerde bedrijven (Inspectie Justitie en Veiligheid, 2016). De combinatie van beperkte hulpverleningscapaciteit en de noodzaak tot handhaving maakt dat de situatie van risico- en crisisbeheersing ten aanzien van de BES eilanden blijvend aandacht behoeft. Dat kan onder andere tot uiting komen in een voortzetting van de vele gezamenlijke oefeningen waaraan RWS en IenW deelnemen.

[5] *De petrochemische opslag is eigendom van het Amerikaanse bedrijf NuStar Energy. Op Bonaire zijn de petrochemische bedrijven Curoil en BOPEC actief. BOPEC heeft een terminal op Bonaire, deze is eigendom van het Venezolaanse bedrijf PDVSA.*

[6] *Bedoeld is hier de term crisisbeheersing voor de algemene kolom (kortweg: openbare orde); zie artikel 1 van de Veiligheidswet BES.*

5 Organisatorische aanpassingen en verbeteringen voor de crisisorganisatie

5.1 Aanbevelingen voor de crisisorganisatie

De prioriteiten die uit de Veiligheidsanalyse en de SWOT-analyse volgen vormen een concrete basis om het nieuwe beleidsprogramma verder in te vullen. Op een aantal vlakken is aangetoond dat organisatorische zaken al behoorlijk goed geregeld zijn, met name in het domein watermanagement (zie ook figuur 2).
Ook zijn er domeinen waarbij uit de analyse blijkt dat ze geen topprioriteit vormen voor IenW, maar niettemin extra aandacht behoeven. Dit betreft bijvoorbeeld hoe om te gaan met de BES-eilanden, maar ook bijvoorbeeld transportongevallen en de impact van migratie, allemaal onderwerpen die de komende jaren in belang kunnen – en waarschijnlijk zullen – gaan toenemen. Stuk voor stuk zijn dit thema's waarbij vooral naar organisatorische verbeterpunten moet worden gekeken.

Bij thema's als infectieziekten humaan, dierziekten, voedselveiligheid, voedselzekerheid, verlies biodiversiteit, luchtvervuiling, en andere blijkt dat de waarschijnlijkheid en/of de impact van deze kwesties relatief beperkt is, zelfs als die organisatorisch relatief goed belegd zijn. Hier zou dus ruimte kunnen liggen om nog eens meer specifiek te kijken naar wat de taken van IenW zijn op deze vlakken, en of de rol van het ministerie mogelijk beperkt kan worden, zodat er meer op de hoofdtaken kan worden gefocust.

Eén initiatief om het nieuwe Beleidsplan Crisisbeheersing te profileren is om een specifieke oefening (bijvoorbeeld met *serious gaming*) te creëren op het vlak van keteneffecten.[7] Hierbij kan niet alleen meer inzicht worden verkregen in keteneffecten en hoe dit verschillende maatschappelijke spelers raakt (burgers, bedrijfsleven), maar ook hoe hier op organisatorisch vlak het beste op kan worden gereageerd. Hierbij zullen ook cyberelementen en een terrorisme-dimensie meegenomen worden, alsook de rol van de sociale media en de mate van zelfredzaamheid van burgers.

Daarnaast kan meer specifiek worden ingegaan op de impact van aantasting van het internet, gekoppeld aan een kwetsbaar onderdeel van de vitale infrastructuur, bijvoorbeeld waterkeringen. Ook kan hiermee meer inzicht worden verkregen in de mate van afhankelijkheid inzake de vitale infrastructuur en hoe de verschillende stakeholders met elkaar interacteren. Het betrekken van de veiligheidsregio's of internationale stakeholders/verantwoordelijken in een dergelijke studie of oefening is daarbij van belang. Ook kan de rol van sociale media hierbij worden meegenomen in de opzet.

[7] *Om kennis en kunde adequaat uit te kunnen wisselen met ketenpartners is oefenen een vereiste. Oefenen biedt de mogelijkheid om op basis van een casus of scenario gezamenlijk na te gaan of de verwachtingen ten aanzien van de rol, taken en verantwoordelijkheden bij de ander ook daadwerkelijk ingevuld worden. Daarnaast zorgt oefenen voor persoonlijk contact en helpt het bij het opbouwen van onderling vertrouwen. Dit vertrouwen is essentieel voor het efficiënt delen van informatie tijdens crisissituaties. Daarbij wordt opgemerkt dat de druk van informatievoorziening op taakuitvoering groot is. Informatiedeling met ketenpartners is belangrijk maar moet zo worden georganiseerd dat het niet ten koste gaat van de eigen taakuitvoering.*

5.2 Algemene suggesties ten aanzien van de organisatie

Uit de interviews, de online SWOT-analyse en de LEF sessie met crisispartners zijn vier organisatorische thema's naar voren gekomen:

1. Hoe kan organisatorisch beter worden samengewerkt binnen IenW en met de crisis- en ketenpartners?
2. Hoe kunnen wij beter omgaan met de dreigingen maar ook mogelijkheden die ICT en cyber bieden?
3. Hoe kunnen wij beter met sociale media omgaan en de positieve bijdrage ervan tot nut maken?
4. Op welke kerntaken kan IenW meer focus leggen om zo een optimale verdeling van taken en verantwoordelijkheden te waarborgen?

Deze thema's geven aanleiding tot het formuleren van de volgende leidraden voor de crisisorganisatie als geheel ten aanzien van de beleidsterreinen van IenW:

1. Blijvend aandacht besteden aan de verdeling van taken en verantwoordelijkheden;
2. Intensivering van de samenwerking met en tussen crisispartners;
3. Meer aandacht voor de rol van sociale media bij risico- en crisiscommunicatie;
4. Meer 'doen'; gezamenlijke activiteiten.

De eerste drie aanbevelingen volgen direct uit de organisatorische thema's. Het thema 'gebruik van ICT en digitale middelen' is in verschillende mate van toepassing op al deze vier leidraden ter ondersteuning aan samenwerking of informatie-uitwisseling. Het idee om meer te 'doen' middels gezamenlijke activiteiten is ook in den brede toe te passen. Gezamenlijke activiteiten – bijvoorbeeld gezamenlijk oefenen maar ook wederzijds werkbezoeken afleggen of uitwisseling van medewerkers – helpen om meer begrip te kweken, om bekendheid met elkaars verantwoordelijkheden en behoeftes te vergroten en om samenwerking te stimuleren.

Duidelijke verdeling van verantwoordelijkheden

Hoewel de verdeling van verantwoordelijkheden tussen de crisispartners op de beleidsterreinen van IenW over het algemeen duidelijk is, is er een aantal specifieke onderwerpen waarvoor dit niet het geval is. Dit betreft met name de crisisbeheersing voor Caribisch Nederland en crisisbeheersing in het geval van cyberincidenten. Voor deze twee onderwerpen is expliciet behoefte geuit aan verduidelijking van verantwoordelijkheden. In meer algemene zin zal ook de behoefte aan verduidelijking van de relatie tussen het DCC IenW en de beleidsdirecties, de relatie tussen IenW en het ministerie van Justitie en Veiligheid en de relatie tussen IenW en de veiligheidsregio's worden geadresseerd. In alle gevallen geldt dat de verdeling van verantwoordelijkheden niet alleen feitelijk moet zijn vastgelegd, maar dat crisispartners hier ook van op de hoogte zijn. Zo liggen voor crises op regionaal niveau duidelijke draaiboeken klaar die doorgaans ook worden opgevolgd. Bij echt grote crises wordt vaak teruggegrepen op persoonlijke contacten, waardoor communicatielijnen verward kunnen raken. In een aantal gevallen lijkt onduidelijkheid voort te komen uit onbekendheid.

Intensieve samenwerking

Samenwerking tussen crisispartners wordt steeds belangrijker. In een complexe samenleving is samenwerking noodzakelijk, niet alleen om het optreden ten tijde van crisis af te stemmen maar ook door gezamenlijk op te trekken. Voor effectieve samenwerking is het nodig dat crisispartners over de eigen organisatie heen kunnen kijken en ketenafhankelijkheden begrijpen. Alleen dan kan adequaat op elkaars informatiebehoefte worden ingespeeld. Een voorbeeld hiervan is informatie-uitwisseling en netcentrisch werken; dit werkt alleen wanneer organisaties weten welke informatiebehoefte crisispartners hebben. Bij crises kan een teveel aan informatie leiden tot een verkeerde focus of diagnostiek. Het is daarom van belang dat informatiedistributie waar nodig wordt herzien. Hieraan gelieerd is de kwestie van toegang tot informatie – voor, tijdens en na een crisis. Gezien de toenemende gevoeligheid van informatie en de meervoudige impact die ongeautoriseerde toegang tot informatie tot gevolg kan hebben wordt beveiliging hiervan een belangrijke(re) kwestie. Tegelijkertijd is het ook noodzakelijk dat informatie in crisistijden snel kan worden achterhaald, en niet teveel versleuteld is.

Dit vergt een nieuwe manier van denken. ICT middelen kunnen samenwerking en informatie-uitwisseling ondersteunen. Zowel binnen IenW als bij de crisispartners wordt de behoefte geuit daar meer gebruik van te willen maken. De inzet van ICT middelen heeft echter alleen effect wanneer crisispartners op elkaar zijn ingespeeld en de juiste *mindset* aanwezig is.

De rol van sociale media

Sociale media en de rol die zij kunnen vervullen bij risico-en crisiscommunicatie wordt in toenemende mate erkend als een kans om meer direct contact met burgers te hebben. Dit contact kan zowel in de koude fase ten aanzien van risicobeheersing en risicoperceptie van belang zijn als tijdens crisissituaties wanneer burgers snel moeten worden geïnformeerd. Direct contact via sociale media kan ook helpen om de zelfredzaamheid van burgers te stimuleren door het bieden van het juiste handelingsperspectief of door de kwaliteit van informatievoorziening te vergroten. Hierbij moet worden bepaald in welke gevallen IenW directe crisiscommunicatie kan uitvoeren en wanneer IenW vooral als spin in het web tussen de verschillende crisispartners kan of moet functioneren. Een voorbeeld is het in paragraaf 4.2 genoemde sociale media beheer van de NS. IenW zou tijdens crisissituaties naar dergelijke 7x24-teams kunnen doorverwijzen.

Meer 'doen'

Meer 'doen', bijvoorbeeld in de vorm van oefenen, wederzijdse werkbezoeken of uitwisseling van medewerkers, versterkt wederzijds begrip en samenwerking tussen crisispartners. Voor IenW heeft gezamenlijk oefenen meerwaarde voor het versterken van samenwerking met ketenpartners en het verbeteren van het gebruik van (nieuwe) ICT middelen. Oefenen en meer 'doen' resulteert in een permanent netwerk van ketenpartners en verbetert samenwerking door het verkrijgen van meer inzicht in elkaars belangen, verantwoordelijkheden en behoeftes. Het waarborgen van het veiligheids- en risicobewustzijn, met name in de *koude* fase, is van vitaal belang ter voorbereiding op crises. Proactief netwerkmanagement is een voorwaarde voor effectieve en efficiënte crisisbeheersing, zodat men, in tijden van crises, belangrijke contacten reeds heeft gelegd. De verbinding moet al zijn gemaakt voordat de noodzaak daarvan zich aandient.

Gezamenlijke activiteiten vergen wel capaciteit. Zowel voor risico- als voor crisisbeheersing wordt opgemerkt dat de capaciteit nochtans beperkt is. Daarnaast wordt de tendens van toenemende risico's en een terugtredende overheid geconstateerd. In deze context is het van belang te benadrukken dat gezamenlijke activiteiten niet altijd door IenW zelf georganiseerd hoeven te worden. IenW kan ook optreden als een aanjager of facilitator van gezamenlijke activiteiten, of anders extra capaciteit hiervoor ter beschikking te stellen.

6 Beleidsagenda 2018-2022

De hieronder opgenomen beleidsagenda is voor de komende twee jaren. Eind 2018 wordt wederom gekeken naar de dan actuele situatie van de crisisbeheersing bij IenW om voor de jaren 2019-2021 een actuele beleidsagenda op te stellen.

Voor de onderwerpen uit de beleidsagenda geldt uiteraard dat er aangesloten wordt op lopende activiteiten/projecten indien van toepassing; dit geldt bijvoorbeeld voor de Cyber meldplichten en de ketenafhankelijkheden. Hiervoor lopen (inter)departementale activiteiten.

De onderwerpen uit de beleidsagenda zijn enerzijds inhoudelijk (ketenafhankelijkheid, stralingsongevallen, Cyber en Caribisch Nederland) en anderzijds organisatorisch (samenwerking, verantwoordelijkheden, crisiscommunicatie en digitale informatievoorzieningen).

Voor de geprioriteerde onderwerpen uit de beleidsagenda zal het soms noodzakelijk zijn een apart project uit te voeren om e.e.a. te realiseren, maar het kan ook door verstandig en slim gebruik te maken van lopende projecten/ontwikkelingen of IenW accenten/prioriteiten in te brengen. Bijvoorbeeld kan bij oefeningen de nadruk gelegd worden op de geprioriteerde inhoudelijke onderwerpen, maar kan ook gericht gebruik gemaakt worden van de ICT middelen zodat ook daarvan de gebruikservaring en kennis toeneemt.

Onderwerp	Te ondernemen acties	Verantwoordelijke	Planning
Ketenafhankelijkheden vitale sectoren IenW en Business Impact niet-vitale sectoren IenW	Per vitale sector ketenafhankelijkheid benoemen en risico's in beeld brengen én risico's niet-vitale IenW sectoren in beeld brengen. Ontbrekende samenwerkingsverbanden organiseren.	Vitale en niet-vitale sectoren IenW. Dossier wordt gevolgd door DG/MI Veiligheid en Risico's in Stuurgroep Nationale Veiligheid en in de Interdepartementale Werkgroep Vitaal, beide o.v.v. min JenV.	2018-2019
Cybersecurity: kritieke ICT IenW-breed en meldloket IenW inrichten	Meldloket IenW inrichten voor de IenW verantwoordelijkheid voor de nationale meldplicht en de EU richtlijn cyberincidenten. Inzicht en overzicht realiseren van kritieke ICT IenW-breed en de sectoren/processen waar IenW politiek verantwoordelijk voor is.	CIO IenW i.s.m. CIO RWS, NCSC, Expertgroep Cyber IenW, DCC-IenW.	2017-2018
Stralingsongevallen	Gehele crisisbeheersing en -organisatie trainen en beoefenen.	DCC-IenW i.s.m. ANVS	2017-2018
Caribisch Nederland	Rollen en verantwoordelijkheden bij crises op een aantal punten duidelijker krijgen bij alle betrokkenen.	DCC-IenW, ILT, RWS, KNMI, beleids DG'en, Rijksvertegenwoordiger, eilandelijke rampenstaf, Kustwacht Caribisch Gebied	2017-2019
Crisiscommunicatie	Risico- en crisiscommunicatie beter aansluiten op crisisbeheersing en specifiek qua middelen inzetten op IenW-stakeholders, burgers, social media e.d.	DCO i.s.m. RWS/BS en DCC-IenW	2018-2019
Points of Contact voor crises IenW beleidsterreinen	Verwachtingen IenW en ketenpartners afstemmen op DCC-IenW 24x7 mogelijkheden.	DCC-IenW i.s.m. ketenpartners en NCC	2018
Samenwerking, verantwoordelijkheden en digitale informatievoorziening	LCMS aansluiting realiseren voor IenW en RWS. Crisisinformatiesystemen doorlichten. Verkennen/uitwerken mogelijkheden van het inzetten/gebruiken van een informatieteam, een informatietafel en/of een All Source Information Cell.	DCC-IenW, min JenV	2017-2019

Figuur 4: Overzicht van Beleidsagenda 2017-2021

7 Hoe nu verder?

Een eerste stap richting heroverweging van het Beleidsplan Crisisbeheersing in het licht van de veelheid van veiligheidsdreigingen is om bewustzijn te kweken over wat er op ons af komt. Het gaat hierbij dus niet alleen om 'traditionele' dreigingen die bijvoorbeeld met klimaatverandering of de gevolgen van zware ongelukken te maken hebben, maar ook de impact van geopolitieke dreigingen of terrorisme. Op dit soort dossiers moet vervolgens worden gekeken in hoeverre de kennisbasis moet worden aangescherpt, maar ook in hoeverre het ministerie op relevante kwesties leidend wil, kan of moet zijn. Hier ligt dus ruimte voor het herijken van bestaande inhoudelijke prioriteringen, en om de organisatie en samenwerking met ketenpartners navenant op bij te stellen.

Qua kennisopbouw met name voor het risicomanagement is het hierbij van belang om bijvoorbeeld een mogelijke *failure of the imagination* te onderkennen. Dit verwijst naar een tekort in verbeeldingsvermogen ten aanzien van potentiële dreigingen. In een veranderende veiligheidsomgeving dienen zich continue nieuwe dreigingen aan. Hierbij kan een (fluïde) onderscheid worden gemaakt tussen dreigingen die men redelijkerwijs had kunnen voorspellen (*known unknowns*) en dreigingen die zich moeilijker laten voorspellen (*unknown unknowns*). Om goed op de hoogte te blijven van zulke ontwikkelingen en hierop beter te kunnen anticiperen is continue informatiedeling en kennis uitwisseling binnen het departement maar ook met crisispartners een vereiste.

In organisatorische zin staan drie issues centraal: de noodzaak om een duidelijker beeld te hebben over verdeling van verantwoordelijkheden in tijden van crisis; betere benutting van de mogelijkheden die ICT biedt, niet alleen voor communicatie tussen stakeholders, maar ook met de bevolking, met name via de sociale media; en de noodzaak om op nieuwe(re) thema's door oefeningen meer kennis en inzichten op te bouwen en waar mogelijk verbeteringen aan te brengen.

Tenslotte is het van belang dat dit crisisbeheersplan een 'levend' document wordt dat niet pas na vier jaar wordt geëvalueerd, maar waarvan de effectiviteit doorlopend wordt getoetst. Dit zal onder meer gebeuren door nieuwe inzichten uit de omgeving en uit wetenschappelijk- en beleidsonderzoek constant in het operationele beleid te integreren. Hiermee kan op regelmatige basis een accentverschuiving plaatsvinden, hetzij wat betreft relevante thema's, dan wel hoe zaken georganiseerd dienen te worden. Het voortdurend betrokken houden van bestaande stakeholders binnen en buiten het ministerie, maar ook het openstaan richting mogelijk nieuwe stakeholders, moet hier onderdeel van zijn. Op deze manier kan IenW met het DCC-IenW als spin in het web op de juiste manier en binnen de juiste proporties de meest relevante veiligheidsdreigingen die in de nabije toekomst op ons af komen aanpakken.

Bijlagen

Bijlage A Rapport HCSS/TNO 'Veiligheidsontwikkelingen'

Zie de apart bijgevoegde rapportage.

Bijlage B In- en externe deskundigen/betrokkenen bij de verschillende fasen voor het opstellen van het beleidsplan

Voor fase 1 'opstellen rapport Veiligheidsontwikkelingen' zijn de volgende personen geïnterviewd:
Sabine Gielens *(VEWIN)*
Dick Jung *(IenW/DGMI Directie Veiligheid en Risico's)*
Rob Hagman *(DCC-IenW, hoofd)*
Hans de Vries *(RWS/VWM vz. LCO)*
Wim Holthuis *(LVNL)*
Rob Huyser *(IenW/DGB Luchtvaart)*
Jan van den Heuvel *(ANVS, algemeen directeur)*
Bastiaan Maltha *(IenW/DGB Maritiem)*
Teus de Kruijf *(ProRail)*

Voor fase 2 'SWOT analyse crisisbeheersing IenW en ketenpartners' is gebruik gemaakt van de interactieve (met discussie mogelijkheden) webapplicatie Synmind. Aan deze interactieve SWOT analyse hebben zo'n 50 deskundigen/betrokkenen deelgenomen uit het ministerie van IenW en vanuit alle crisispartners van IenW.

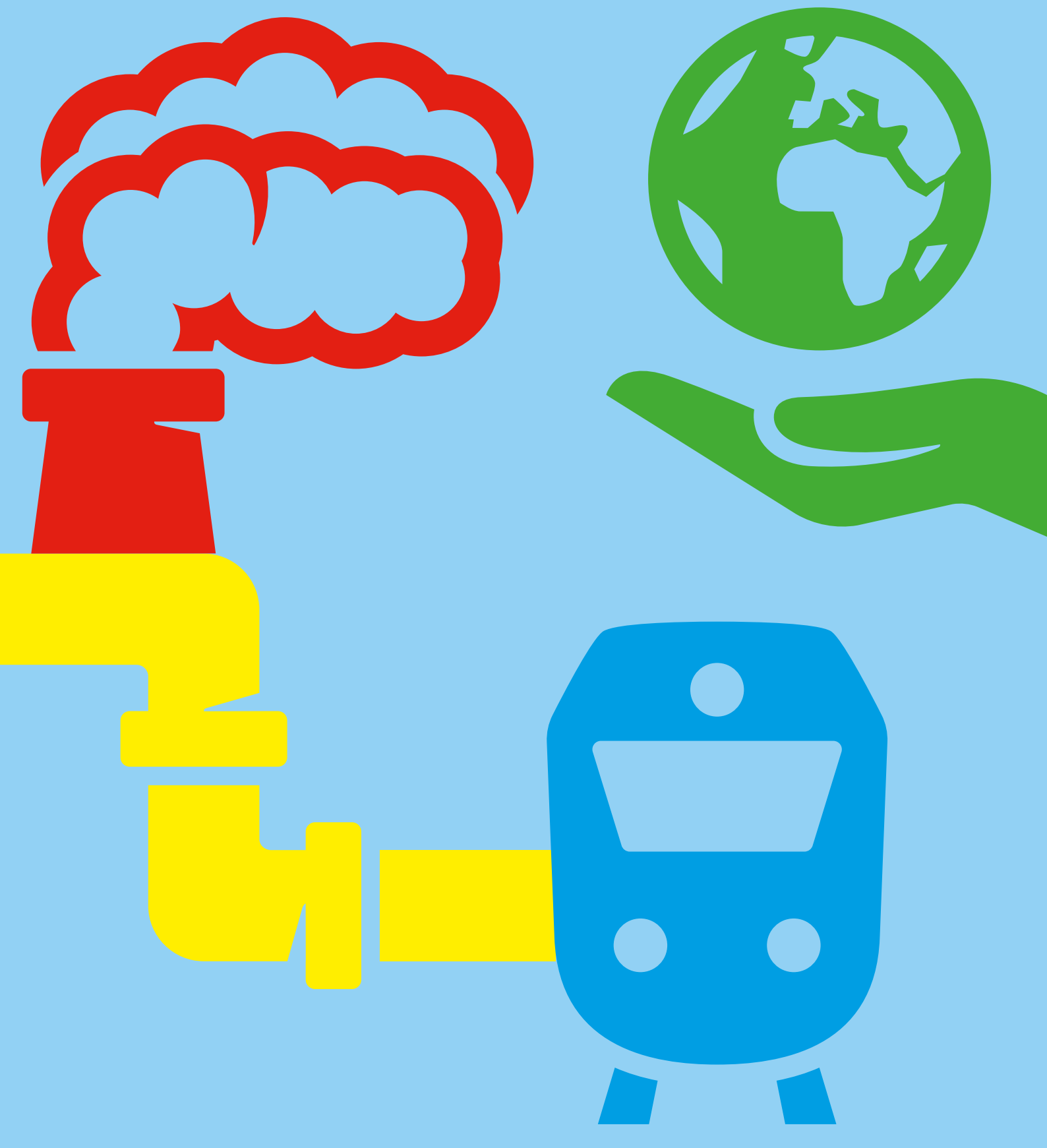
Bij fase 3 'Afsluitende consoliderende sessie in het LEF Future Center' waren de volgende personen aanwezig:
Leonie Bolwidt, *RWS/VWM*
Sabine Gielens, *VEWIN*
Rob Hagman, *hoofd DCC-IenW*
Johan Tintel, *IenW/ILT*
Frank Kroonenberg, *KNMI*
Henny Langendijk, *IenW/HBJZ*
Ellen Moens, *VCNL*
Wim Holthuis, *LVNL*
Annemarie van Wezel, *KWR*
Jos van Wesemael, *IenW/CIO*
Gijs de Kruijff, *JenV hoofd NCC*
Tony Hoogendoorn, *DCC-IenW*
Edith Kuijper, *DCC-IenW,*
Anita Wehmann, *IenW/IBI*
Stoffel Bos, *ProRail security officer*
Bert van Munster, *WMCN*
Rob Duba, *IenW/DGMI*
Marc Bökkerink, *JenV/NCTV*
Marcia van Hugten, *NS*
Peter Tesselaar, *RWS*
Geerd Drost, *RWS*
Raymond Voogt, *IenW/ILT*
Bert Kort, *RWS/VWM*
Alisa Heaver, *RWS/VWM*

Colofon

Uitgegeven door	Departementaal Coördinatiecentrum Crisisbeheersing
Informatie	dcc@minienm.nl
Telefoon	088 – 797 02 22
Datum	Januari 2018
Status	Definitief, akkoord in BSR 22 januari 2018.
Versie	1.5

Auteurs: Willem Oosterveld, Paul Sinning, Erik Frinking, Reinier Bergema (HCSS); Theo van Ruijven, Lisa Ziekenoppasser (TNO); Joaquim de Witte (Synmind).

Met medewerking van: Harold Bousché (TNO); Myrthe van der Gaast, Joost Kraak, Abel Hendriks (HCSS); medewerkers ministerie van Infrastructuur en Waterstaat.



Dit is een uitgave van het

Ministerie van Infrastructuur
en Waterstaat

Postbus 20901 | 2500 EX Den Haag
www.rijksoverheid.nl/ienw

December 2017