Auditdienst Rijk
Ministerie van Financiën

-

Onderzoeksrapport
Beleidsdoorlichting Artikel 36.2
Nationale veiligheid en terrorismebestrijding

Definitief

Colofon

Titel	Beleidsdoorlichting Artikel 36.2 Nationale veiligheid en terrorismebestrijding
Uitgebracht aan	Ministerie van Veiligheid en Justitie
Datum	22 november 2017
Kenmerk	2017-0000210580

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Samenvatting

Inleiding

De Regeling Periodiek Evaluatieonderzoek bepaalt dat elke vier tot zeven jaar een doorlichting plaats moet vinden van ieder beleidsartikel (of onderdeel daarvan) van de begroting van een ministerie. Het artikel van deze beleidsdoorlichting betreft artikel 36.2 van de begroting van het ministerie van Justitie en Veiligheid (JenV; voorheen ministerie van Veiligheid en Justitie). Dit artikel omvat alle beleidsterreinen van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). De NCTV is in 2011 opgericht en dit is daarom de eerste beleidsdoorlichting op het beleid van de NCTV, die wordt aangeboden aan de Tweede Kamer.
De doorlichting is uitgevoerd door de Auditdienst Rijk op basis van een synthese van beschikbare informatie en eerder uitgevoerde onderzoeken. In de bijlage is een overzicht van het bronnenmateriaal opgenomen. Centraal in de doorlichting staan de realisatie van de met het beleid beoogde doelen, de implementatie van de beleidsinstrumenten en de bijbehorende uitgaven en de indicaties over de effectiviteit en doelmatigheid van het beleid. De focus ligt op de periode 2011 tot en met 2015.

Hoofdstuk 1

Hoofdstuk 1 behandelt de afbakening van de beleidsdoorlichting. Hierin wordt uiteengezet dat met het beleid van de NCTV wordt beoogd bij te dragen aan een veilig en stabiel Nederland door het voorkomen en beperken van maatschappelijke ontwrichting. Hiervoor is het beleid gericht op het onderkennen van dreigingen, het verhogen van de weerbaarheid van burgers, bedrijfsleven en overheidsorganen en het versterken van de bescherming van vitale belangen. Daarbij geldt wel dat de NCTV te maken heeft met fenomenen, waarvoor niet eerder beleid is opgesteld en het feit dat effecten van maatregelen om fenomenen als terrorisme te bestrijden, zich maar moeilijk laten bepalen. De causaliteit tussen ingezette beleidsinstrumenten en de doeltreffendheid ervan is volgens de NCTV lastig vast te stellen, omdat nog vele andere factoren van invloed kunnen zijn geweest op het uiteindelijk effect. Daarom heeft de begeleidingscommissie van deze beleidsdoorlichting ervoor gekozen het onderzoek naar doeltreffendheid te richten op dat wat de minister van JenV, werkende via de NCTV, vanuit zijn coördinerende functie bij de publieke en private partners wil bereiken.

Hoofdstuk 2

Dit hoofdstuk beschrijft de motivering van het gevoerde beleid (aanleiding, doel en legitimiteit). Gezien de recente gebeurtenissen en actuele dreigingen was en is de motivering voor het gevoerde en te voeren beleid nog immer legitiem. In het afgelopen decennium is gebleken dat Nederland kwetsbaar is voor rampen, aanslagen en andere incidenten. Daarbij hebben zich in het afgelopen decennium de verschillende incidenten, rampen en aanslagen in Europa, maar ook specifiek in Nederland voorgedaan. Wat in de ons omringende landen gebeurt, kan ook in Nederland gebeuren. De kans op een aanslag in Nederland is en blijft reëel. Het dreigingsniveau staat daarom al gedurende lange tijd op ‘substantieel’, ook in de periode waar deze beleidsdoorlichting op ziet. Het blijft dus belangrijk om doorlopend alert te zijn op nieuwe dreigingen ten aanzien van de (nationale) veiligheid, zoals de toenemende dreiging die uitgaat van het jihadisme en cybercrime. Op basis van het inzicht op nieuwe dreigingen kunnen zowel preventieve als repressieve acties plaatsvinden. Daarnaast is het belangrijk om klaar te staan als het onverhoopt mis gaat.

Deze beleidsdoorlichting richt zich op de beleidsdoelstellingen van alle beleidsterreinen die binnen het Ministerie van JenV zijn ondergebracht bij de NCTV. De NCTV is ondergebracht bij het ministerie van JenV aangezien de minister van JenV een coördinerende verantwoordelijkheid heeft op de domeinen nationale veiligheid en crisisbeheersing, terrorismebestrijding en cybersecurity. Elk domein heeft een eigen doelstelling, welke uiteindelijk dient bij te dragen aan een veilig en stabiel Nederland. De beleidsdoelstellingen per taakdomein zijn:

- *Contraterrorisme*: het voorkomen van aanslagen, verminderen van de vrees voor aanslagen en beperken van gevolgen van een eventuele aanslag;
- *Nationale veiligheid en crisisbeheersing*: het voorkomen en beperken van maatschappelijke ontwrichting door rampen en crises;
- *Cybersecurity*: het versterken van de veiligheid van de digitale samenleving om daarmee het vertrouwen in het gebruik van ICT door burger, bedrijfsleven en overheid te verhogen.

Hoofdstuk 3

Dit hoofdstuk geeft een uitwerking van de aard en samenhang van de ingezette beleidsinstrumenten en de daarmee samenhangende uitgaven. De NCTV heeft in de periode 2011-2015 op de drie taakdomeinen zeer veel instrumenten ingezet. Hieronder geven wij per taakdomein en bijbehorende beleidsdoelstellingen, de subdoelstellingen weer, waaronder de verschillende instrumenten zijn beschreven. Voor een totaaloverzicht van alle ingezette beleidsinstrumenten verwijzen wij naar de beleidsbomen in bijlagen 1 tot en met 4 .

Contraterrorisme

De hoofddoelstelling *'het voorkomen van aanslagen, verminderen van de vrees voor aanslagen en beperken van gevolgen van een eventuele aanslag'* kent in de periode 2011-2015 de volgende subdoelstellingen waaronder het beleid verder is uitgewerkt:

- *Verstoren van dreigingen en verijdelen aanslagen door beperken van toegang tot middelen en tegengaan van reisbewegingen*
  - Ontwikkelen, ondersteunen en beschikbaar stellen van instrumenten voor partners
  - Coördineren en faciliteren van lokale, nationale en internationale samenwerkingsverbanden

- *Voorkomen van aanwas door ondermijning aanbod propaganda en verhogen weerbaarheid kwetsbare groepen*
  - Coördineren en faciliteren van het netwerk aan partijen waarbinnen activiteiten ter voorkoming van aanwas moeten plaatsvinden

- *Beschermen van personen, objecten en vitale processen tegen terroristische aanslagen*
  - Verder professionaliseren van het stelsel Bewaken en Beveiligen
  - Intensiveren van de aanpak gericht op solistische dreigers
  - Toekomstbestendig maken van de beveiligingscontroles op de luchthavens.

Nationale veiligheid en crisisbeheersing

De hoofddoelstelling 'het voorkomen en beperken van maatschappelijke ontwrichting door rampen en crises' kent in de periode 2011-2015 de volgende subdoelstellingen waaronder het beleid verder is uitgewerkt:

- *Verbeteren van het functioneren van het stelsel van crisisbeheersing door coördinatie en het vereenvoudigen van besluitvorming*
  - Versterken nationale crisisorganisatie

- Versterken presterend vermogen veiligheidsregio's en Caribisch Nederland
- Versterken samenwerking met verschillende partijen
- Versterken van de informatievoorziening en crisiscommunicatie
- Behoud historisch erfgoed

- *Vergroten weerbaarheid van vitale belangen*
  - Versterken weerbaarheid ten behoeve van de nationale veiligheid
  - Versterken economische veiligheid
  - Verhogen weerbaarheid Rijk tegen spionage

Cybersecurity
De hoofddoelstelling 'het versterken van de veiligheid van de digitale samenleving om daarmee het vertrouwen in het gebruik van ICT door burger, bedrijfsleven en overheid te verhogen' kent in de periode 2011-2015 de volgende subdoelstellingen waaronder het beleid verder is uitgewerkt:

- *Versterken integrale aanpak cybersecurity door publieke en private partijen*
  - Duidelijke verdeling van taken, verantwoordelijkheden en bevoegdheden
  - Bouwen aan coalities voor vrijheid, veiligheid en vrede in het digitale domein

- *Nederland zorgt voor adequate en actuele dreiging- en risicoanalyses*
  - Gezamenlijk integraal beeld van actuele dreigingen en kwetsbaarheden ICT
  - Versterken van onderzoeks- en analysecapaciteit

- *Versterken weerbaarheid tegen ICT-verstoringen en cyberaanvallen*
  - Vergroten en ontwikkelen van cybersecurity experts
  - Stimuleren van onderzoek op het vlak van cybersecurity
  - Vergroten kennis over en veiligheidsbewustzijn van ICT-producten en diensten bij de gebruikers (burgers en bedrijven)
  - Bewerkstelligen dat publieke en private leveranciers voldoen aan minimumeisen op het gebied van continuïteitsdienstverlening en spionage

- *Versterken responscapaciteit om ICT-verstoringen en cyberaanvallen te pareren*
  - Zorgen voor een duidelijke crisisstructuur bij cyberincidenten
  - Informeren van de burger en bedrijven bij cyberincidenten
  - Stimuleren van kennis(deling) en oefening

Uitgaven
In tabel is een overzicht opgenomen van de programma uitgaven op artikel 36.2 over de periode 2013 tot en met 2015. In deze tabel is te zien dat het overgrote deel van de uitgaven op artikel 36.2 van de begroting van het ministerie van JenV bestaat uit de Brede Doeluitkering rampenbestrijding (BDUR). Op basis van het Besluit Veiligheidsregio's worden de veiligheidsregio's mede op basis van deze bijdrage in staat gesteld uitvoering te geven aan het beleid met betrekking tot brandweer, geneeskundige hulpverlening, rampenbestrijding en crisisbeheersing.
Het merendeel van de overige beleidsinstrumenten is niet direct te koppelen aan gelabelde uitgaven. Het betreft instrumenten waarbij de realisatie ervan vooral afhankelijk is van de inzet van medewerkers van de NCTV.

Tabel 1: Totaal realisatie programma uitgaven (x €1.000) [1]

	2013	2014	2015
Programma uitgaven	**196.333**	**245.945**	**247.430**
Bijdragen aan medeoverheden			
Brede Doeluitkering rampenbestrijding (BDUR)	128.461	177.293	176.097
Overige Nationale Veiligheid en terrorismebestrijding	9.529	6.275	11.520
Bijdragen ZBO/RWT			
IFV (Instituut Fysieke Veiligheid)	34.441	31.045	30.736
Opdrachten			
Project NL-Alert	3.254	6.284	6.702
Opdrachten NCSC	4.489	4.123	2.743
Overig terrorisme bestrijding	1.469	1.066	685
Overig Nationale Veiligheid	8.774	13.724	11.964
Subsidies			
Nationaal Veiligheidsinstituut	934	2.053	1.340
Nederlands Rode Kruis	1.827	1.786	1.611
Onderwijs Veiligheidregio's	250	0	0
Overige Nationale Veiligheid en terrorismebestrijding	2.905	2.296	4.032
Bijdrage agentschappen			
Overig bijdragen Agentschappen	0	0	0

De structurele verhoging van de uitgaven BDUR met € 65,7 miljoen sinds 2014 wordt veroorzaakt doordat de veiligheidsregio's, in tegenstelling tot de gemeenten, geen gebruik kunnen maken van het btw -compensatiefonds.

Hoofdstuk 4

Dit hoofdstuk biedt een overzicht van de bevindingen over de doeltreffendheid en doelmatigheid van het gevoerde beleid per taakveld van de NCTV. Naast een toelichting op het beschikbare onderzoek naar doeltreffendheid en doelmatigheid van het beleid biedt dit hoofdstuk inzicht in de realisatie en werkzaamheid van de ingezette beleidsinstrumenten. Tevens bevat dit hoofdstuk een uiteenzetting in hoeverre het mogelijk is op basis van het beschikbare onderzoek uitspraken te doen over doeltreffendheid de doelmatigheid van het gevoerde beleid.

Contraterrorisme

In de periode 2011-2015 zijn door de NCTV veel beleidsinstrumenten ingezet op het gebied van terrorismebestrijding. Het merendeel van deze beleidsinstrumenten is ook gerealiseerd. Alleen de realisatie van de geïnitieerde wetgevingstrajecten heeft meestal pas plaatsgevonden na de periode van de doorlichting. Wel zijn de werkzaamheden ter voorbereiding op deze wetgeving uitgevoerd in de periode 2011-2015.

Ten aanzien van de evaluatie van het gevoerde beleid zijn in de afgelopen jaren een aantal onderzoeken verschenen op het terrein van terrorismebestrijding. De meest veelomvattende onderzoeken daarbij zijn de Evaluatie Contraterrorisme-strategie 2011-2015, de Evaluatie van het Actieprogramma Integrale Aanpak Jihadisme en de Evaluatie van het Stelsel Bewaken en Beveiligen.

1 Voor het jaar 2012 zijn de uitgaven niet meer duidelijk te achterhalen, omdat de programma uitgaven voorheen ongespecificeerd onderdeel uit maakten van diverse begrotingsartikelonderdelen.

Uitspraken over de doeltreffendheid van specifieke beleidsinstrumenten is echter niet mogelijk. Zo stelt de evaluatie van de contraterrorisme-strategie dat de effecten van het contraterrorismebeleid niet rechtstreeks te evalueren zijn. De gevolgen van maatregelen zijn namelijk bijzonder moeilijk vast te stellen, omdat de ogenschijnlijke effecten van het beleid ook door andere oorzaken tot stand kunnen zijn gekomen.

De gevolgde contraterrorisme-strategie van de afgelopen jaren kenmerkt zich door een integrale aanpak; partners zetten instrumenten gecombineerd en tegelijkertijd in. De evaluatie van deze strategie heeft zich daarom gericht op het zogeheten gezamenlijke interventievermogen; de gedeelde capaciteit van de betrokken organisaties om een doelgerichte, legitieme en robuuste bijdrage te leveren aan de doelen van de strategie.
De NCTV heeft zich hierbij vanuit haar rol, gericht op het equiperen en ondersteunen van de betrokken partners, zowel op lokaal, nationaal en internationaal niveau door vanuit een coördinerende rol te investeren op de onderlinge samenwerking, een versterking van de informatie-uitwisseling en kennisdeling, verruiming van de mogelijkheden om (potentiële) terroristen en extremisten aan te pakken én de advisering omtrent signalering en interventies.

Uit de evaluatie van de contraterrorisme-strategie blijkt verder dat de beleidskeuze voor een integrale lokale aanpak valide is en het interventievermogen in potentie kan versterken. De integrale lokale aanpak zoals die staat in 2015 wordt betiteld als krachtig door de brede betrokkenheid van verschillende partners; gezamenlijk kunnen ze steeds een maatwerkpakket van veiligheidsgerichte en sociaalgerichte interventies waarmaken.
Informatiedeling is een sleutelonderdeel van de samenwerking tussen de verschillende partijen in de gedeelde aanpak van contraterrorisme. Door informatiedeling kunnen partijen perspectieven uitwisselen om steun of legitimiteit te versterken.

De wetenschappelijke literatuur onderschrijft ook grotendeels het belang van coördinatie voor een doelgericht interventievermogen. Door de structurele samenwerking en coördinatie is het gehele stelsel robuust voorbereid op mogelijke dreigingen.

De NCTV wordt gewaardeerd en gerespecteerd als coördinator van de samenwerking. De NCTV is van grote waarde bij het opbouwen van een goede informatiepositie door het bieden van beleidsmatige ondersteuning, kennis, expertise en trainingen. Ondanks de waardering voor de coördinatie vanuit de NCTV, blijkt wel dat rolconflicten blijven terugkomen. Deze rolconflicten zijn onvermijdelijk voor elke coördinator in een complex netwerk, maar de rol van de NCTV als onafhankelijk makelaar tussen praktijk en politiek zal actief beschermd moeten worden. Daarnaast is het tevens van belang attent te blijven op het feit dat de benodigde coördinatie onbedoeld kan doorschieten in strakke, starre aansturing, die het interventievermogen ten aanzien van ongekende, onbekende dreigingen juist weer ondermijnt.

De evaluatie van de contraterrorisme -strategie benoemt verder nog een aantal aspecten die het interventievermogen van het netwerk (kunnen) beïnvloeden:
- De brede oriëntatie van de strategie biedt onbedoeld ruimte voor selectieve aandacht. De strategie wil alle partners een ‘kompas’ bieden voor al hun acties, maar wordt onbedoeld een ‘beleidscatalogus’ om vrij uit te kiezen.
- Partners drijven van elkaar weg in tijden van verminderde aandacht. In tijden van verminderde aandacht zetten veiligheidsgerichte spelers nog redelijk actief in op het contraterrorisme beleid, maar zien sociaalgerichte partners geen expliciete rol voor zichzelf in het beleid.

- De capaciteit van landelijke partners fluctueert sterk. Wanneer de dreiging niet zichtbaar is of minder politieke aandacht krijgt, lukt het niet om kennis, contacten en menskracht op peil te houden.
- De integrale lokale aanpak is in potentie krachtig, maar ook de capaciteit van lokale partners heeft gefluctueerd. In afwezigheid van zichtbare dreiging neemt de capaciteit op radicalisering en terrorisme af bij lokale partners tot een enkele medewerker of valt alle menskracht weg.

Door het feit dat evaluatie op het niveau van afzonderlijke instrumenten op het terrein van terrorismebestrijding beperkt tot niet mogelijk is, is het ook niet mogelijk uitspraken te doen over de doelmatigheid van afzonderlijke beleidsinstrumenten. Daarnaast doen de evaluaties ook geen uitspraken over de doelmatigheid van de instrumenten in zijn geheel. Wat wel in de evaluatie van de contraterrorisme-strategie naar voren komt, is dat lokale partijen unaniem aangeven dat zij over voldoende instrumenten beschikken om te doen wat nodig is. De behoefte gaat veeleer om meer expertise en capaciteit om alle mogelijkheden te benutten.

Ten aanzien van het bewaken en beveiligen van personen, objecten en vitale infrastructuur zijn geen evaluaties beschikbaar die uitspraken doen over de doeltreffendheid en doelmatigheid van de ingezette beleidsinstrumenten. Wel hebben uitgevoerde evaluaties geleidt tot verbeteringen en aandachtspunten, die vervolgens door de NCTV en de betrokken partijen zijn vertaald in acties en nieuwe beleidsinstrumenten.

Nationale veiligheid en crisisbeheersing
De in de periode 2011-2015 door de NCTV ingezette beleidsinstrumenten ten aanzien van nationale veiligheid en crisisbeheersing zijn volledig of (groten)deels gerealiseerd. In de afgelopen jaren zijn ook verschillende onderzoeken uitgevoerd op het terrein van crisisbeheersing in Nederland. Zo hebben er de nodige evaluaties van specifieke crises en rampen in de periode van deze beleidsdoorlichting plaatsgevonden. Daarnaast zijn ook evaluaties uitgevoerd die algemener ingaan op het functioneren van crisisbeheersing en rampenbestrijding. Dit betreffen: de evaluatie van Wet Veiligheidsregio's in 2013, de Staat van de rampenbestrijding 2013 en 2016, het rapport van de evaluatiecommissie Hoekstra uit 2013 en het onderzoek van de Algemene Rekenkamer 'Zicht overheden op beschermen burgers en bedrijven' uit 2014.

Deze evaluatieonderzoeken zijn meestal in algemene zin gericht op het functioneren van crisisbeheersing en rampenbestrijding in Nederland en gaan niet of beperkt in op de plausibiliteit of doeltreffendheid van de specifieke beleidsinstrumenten. Wel doen de evaluaties uitspraken over effecten van het gevoerde beleid in zijn algemeenheid. Zo komt uit de evaluaties naar voren dat het ontwikkelen van de veiligheidsregio's in het algemeen een gunstig effect heeft gehad op de kwaliteit en effectiviteit van de rampenbestrijding en dat de invoering van de Wet veiligheidsregio's heeft gezorgd voor een vergroting van expertise, een versterking van operationele slagkracht en vergroting van de effectiviteit. Dankzij de wet zijn verbeteringsprikkels gecreëerd en is de mogelijkheid ontstaan om op een hoger dan gemeentelijk niveau te werken aan een goede voorbereiding op rampen en crises. De veiligheidsregio's hebben in de afgelopen jaren een positieve ontwikkeling doorgemaakt en zijn in toenemende mate taakvolwassen geworden. Zo is de samenwerking tussen de verschillende hulpverleningsdiensten sterk verbeterd, net als de samenwerking tussen veiligheidsregio's en andere crisispartners.

Naast deze positieve ontwikkelingen is ook ruimte voor verbetering. Zo richt de Wet veiligheidsregio's zich vooral op de klassieke rampenbestrijding en is het effect van

de wet minder goed te zien op andere gebieden waar verbetering nodig was: een betere (aansturing van de) brandweerzorg en een effectievere beheersing van crises waarmee de samenleving wordt geconfronteerd. De daadwerkelijke taakuitvoering bij de aanpak van incidenten en oefeningen is op meerdere punten nog voor verbetering vatbaar. Ook kwaliteitszorg is in de veiligheidsregio's nog volop in ontwikkeling.
De uitgevoerde evaluaties hebben in alle gevallen geleid tot aandachtspunten en/of aanbevelingen om hier invulling aan te geven. Deze aandachtspunten en aanbevelingen zijn op hun beurt in de periode 2011-2015 veelal vertaald in nieuwe beleidsinstrumenten of aanpassing van bestaande instrumenten.

Naast beleid ten aanzien van verbetering van de crisisbeheersing en rampenbestrijding heeft de NCTV ook de nodige beleidsinstrumenten ingezet voor het vergroten van de weerbaarheid van de vitale infrastructuur. Deze beleidsinstrumenten zijn ook grotendeels dan wel volledig gerealiseerd. Er zijn echter geen evaluaties beschikbaar die uitspraken doen over in hoeverre deze beleidsinstrumenten hebben bijgedragen aan het vergroten van de weerbaarheid van de vitale infrastructuur.

Op basis van de beschikbare evaluaties is het ook niet mogelijk uitspraken te doen over de doelmatigheid van de afzonderlijke beleidsinstrumenten of het gevoerde beleid in bredere zin.

Cybersecurity
Op het gebied van cybersecurity heeft de NCTV in de afgelopen jaren veel beleidsinstrumenten ingezet, gericht op het versterken van de veiligheid van de digitale samenleving. Er zijn in de afgelopen jaren echter maar een beperkt aantal onderzoeken verschenen op gebied van Cybersecurity. Daarnaast komt de relatie tussen het gevoerde beleid en de gewenste effecten niet duidelijk naar voren in de uitgevoerde evaluaties. Wel geeft het onderzoek naar Cyber Readiness enig inzicht in de mate waarop Nederland is voorbereid op cyberrisico's. Het laat zien dat het gehele cyberstelsel in Nederland, waar ook de door de NCTV ingezette beleidsinstrumenten onderdeel van uitmaken, zich in de afgelopen jaren tot een bepaald volwassenheidsniveau ontwikkeld heeft. Hoewel belangrijke stappen zijn gezet, laat het onderzoek ook zien dat Nederland zich nog verder kan ontwikkelen. Recent onderzoek van het Rathenau instituut stelt zelfs dat de weerbaarheid van het gehele cyberstelsel in Nederland onvoldoende op orde is.

Net als voor de andere taakvelden is het ook voor cybersecurity niet mogelijk om te bepalen wat de invloed is van het gevoerde beleid om de digitale weerbaarheid te verhogen ten aanzien van de eventuele kosten die zich voordoen als dat beleid ontbreekt. Uit het rapport over Cyber Readiness blijkt wel dat Nederland minder dan 0,01 procent van zijn Bruto Binnenlands Product uitgeeft aan cybersecurity en dat is relatief gezien beduidend minder dan andere ontwikkelde landen, zoals de Verenigde Staten, Verenigd Koninkrijk, Australië, Duitsland en Frankrijk. Een kanttekening hierbij is overigens wel dat uitgaven aan cybersecurity in Nederland mogelijk hoger zijn, maar niet altijd als zodanig zichtbaar dan wel benoemd zijn.

Hoofdstuk 5
Op basis van de bevindingen van deze beleidsdoorlichting presenteren wij in dit hoofdstuk een samenvattend beeld met bijbehorende aanbevelingen.

De NCTV heeft in de periode 2011-2015 veel werk verzet. De NCTV heeft veel beleidsinstrumenten ingezet en gerealiseerd om het beleid op deze taakvelden over deze periode vorm te geven.

In alle drie de taakdomeinen zijn evaluaties uitgevoerd. Wel verschilt per taakdomein in hoeverre de uitgevoerde evaluaties inzicht geven in de plausibiliteit en effectiviteit van het gevoerde beleid.
Zo komt uit de evaluatie van de CT-strategie naar voren dat uitspraken over de doeltreffendheid van beleid niet mogelijk is, maar het wel plausibel is dat het ingezette beleid op het gebied van contraterrorisme gerechtvaardigd is.

Uit de evaluaties op het gebied van crisisbeheersing blijkt dat, hoewel verbetering mogelijk is, de kwaliteit en doeltreffendheid van de crisisbeheersing en rampenbestrijding in Nederland in de afgelopen jaren is verbeterd.
De uitgevoerde evaluaties doen echter maar beperkt uitspraken over de relatie tussen de ingezette beleidsinstrumenten en de gerealiseerde effecten. Wel hebben de diverse uitgevoerde evaluaties geleid tot aandachtspunten en/of aanbevelingen. Deze aandachtspunten en aanbevelingen zijn op hun beurt in de periode 2011-2015 veelal vertaald in nieuwe beleidsinstrumenten of aanpassing van bestaande instrumenten.

Op het gebied van cybersecurity zijn maar beperkt evaluaties aanwezig.
Door het achterblijven hiervan zijn nu nog maar zeer beperkt uitspraken over de plausibiliteit en effecten op dit beleidsterrein mogelijk. Echter hebben enkele evaluaties die zijn uitgevoerd ook geleid tot aandachtspunten en/of aanbevelingen die vervolgens door de NCTV zijn opgepakt.

De meeste uitgevoerde evaluatieonderzoeken zijn algemeen van aard en/of evalueren ingezette beleidsinstrumenten in gezamenlijkheid. De doeltreffendheid en doelmatigheid van de afzonderlijke beleidsinstrumenten kan op basis van het beschikbare onderzoek daarmee niet worden aangetoond. In sommige gevallen is evaluatie van (afzonderlijke) instrumenten echter ook niet mogelijk. Zo zijn de effecten van het contraterrorismebeleid niet rechtstreeks te evalueren, omdat de ogenschijnlijke effecten van het beleid ook door andere oorzaken tot stand kunnen zijn gekomen.

Daarnaast ontbreekt het aan onderzoek naar wat de NCTV vanuit haar coördinerende rol wil bereiken[2]. Hoewel beperkt, doen enkele evaluaties wel uitspraken over de rolinvulling van de NCTV. Zo blijkt uit bijvoorbeeld de evaluatie van de CT-strategie dat de NCTV wordt gewaardeerd en gerespecteerd als coördinator van de samenwerking[3]. Ook het onderzoek van de inspectie VenJ naar het gebruik van de beveiligingsadviezen van het NCSC geeft enig inzicht in de rol van de NCTV. Daaruit blijkt dat de betrokken partijen de kennis en expertise van het NCSC, als onderdeel van de NCTV, waarderen[4]. De uitgevoerde evaluaties doen echter geen uitspraken over wat de NCTV wil bereiken bij haar partners, maar zijn meer gericht op de maatschappelijke impact van instrumenten die door de publieke en private partners in gezamenlijkheid zijn ingezet.

Ten aanzien van de doelmatigheid van de afzonderlijke beleidsinstrumenten of het gevoerde beleid in bredere zin geldt voor alle drie de taakdomeinen dat het op basis van de beschikbare evaluaties niet mogelijk is hier uitspraken over te doen. Het overgrote deel van de ingezette beleidsinstrumenten is niet direct te koppelen aan gelabelde uitgaven. Het betreft instrumenten waarbij de realisatie

2 Zoals toegelicht in de inleiding van dit rapport is er voor deze beleidsdoorlichting een alternatieve onderzoeksvraag geformuleerd voor wat betreft de doeltreffendheid van het gevoerde beleid Door de begeleidingscommissie van deze beleidsdoorlichting is gekozen dit te richten op dat wat de minister van VenJ, werkende via de NCTV, vanuit zijn coördinerende functie bij de publieke en private partners wil bereiken. Reden hiervoor is dat de causaliteit tussen ingezette beleidsinstrumenten en de doeltreffendheid lastig is vast te stellen, omdat nog vele andere factoren van invloed kunnen zijn geweest op het uiteindelijke effect
3 Evaluatie CTstrategie 2011 -2015: Gericht, gedragen en geborgd interventievermogen?, USBO Advies, 8 april 2016, p. 103,123,132
4 Rapport Inspectie Veiligheid en Justitie, Gebruik van veiligheidsadviezen van het Nationaal Cyber Security Centrum, mei 2015.

ervan vooral afhankelijk is van de inzet van medewerkers van de NCTV. Op het niveau van beleidsinstrumenten is nu niet inzichtelijk hoeveel tijd medewerkers aan instrumenten hebben besteed. Aparte kostprijzen voor het merendeel van de ingezette beleidsinstrumenten kunnen dan ook niet worden berekend.

Op basis van onze bevindingen zijn wij van mening dat meer mogelijk is op het gebied van het inzichtelijk maken van (effecten van) het beleid van de NCTV . Wij achten het daarom van belang dat meer en/ of beter gericht materiaal beschikbaar komt om goede (effect)evaluaties mogelijk te maken met als doel beter inzicht te krijgen in de kwaliteit van het gevoerde en voorgenomen beleid en lessen te kunnen trekken over de doelmatigheid en doeltreffendheid van het beleid.

Wij adviseren de NCTV daarom eerst explicieter uit te werken wat de NCTV vanuit haar rol bij ketenpartners wil bereiken. Dit betekent dat de NCTV vanuit de verschillende ketenbrede strategieën per taakdomein, zoals bijvoorbeeld de CT-strategie, een vertaling zal moeten maken naar wat de NCTV vanuit haar rollen bij haar partners wil realiseren. Definieer vanuit de beleidsdoelstellingen de gewenste resultaten[5] waarbij de kernvraag is hoe de beleidsinterventie geacht wordt te werken. Met een goed beargumenteerde en onderbouwde beleidstheorie zal de NCTV beter in staat zijn haar eigen beleid te laten evalueren en zal een onderzoek ook specifieker inzicht kunnen geven in het functioneren en het effect van het beleid van de NCTV. Een dergelijk inzicht is van belang om als organisatie (beter) te kunnen leren en te verbeteren, maar ook om beter te kunnen verantwoorden over inspanningen die zijn geleverd.

Daarnaast adviseren wij om vervolgens, in aansluiting op meer concreet geformuleerd NCTV beleid, te inventariseren welke en hoe ingezette beleidsinstrumenten kunnen worden geëvalueerd op hun doeltreffendheid en doelmatigheid. Bij nieuwe beleidsinitiatieven adviseren wij steeds de mogelijkheid te onderzoeken of er eerst een experiment kan worden uitgevoerd en daarbij een zodanige vorm te zoeken dat effectevaluaties mogelijk zijn. Uiteraard moet wel recht gedaan worden aan de complexiteit van het beleid op de verschillende taakgebieden, waarbij veelal geen sprake is van een ondubbelzinnige één–op -één-relatie tussen de inzet van een beleidsinstrument en het beoogde doel.

Hoofdstuk 6

Dit hoofdstuk betreft de verantwoording van deze beleidsdoorlichting.
Het onderzoek is uitgevoerd door onderzoekers van de ADR die zijn aan te merken als onafhankelijke deskundigen zoals bedoeld in de RPE. De doorlichting is uitgevoerd op basis van een synthese van beschikbare informatie en eerder uitgevoerde onderzoeken. Bij het onderzoek is de ADR ondersteund door een begeleidingscommissie die beschikbare informatie en aanvullende inzichten heeft aangedragen. De begeleidingscommissie bestond uit medewerkers van de NCTV van het ministerie van JenV, medewerker directie Financieel Economische Zaken (DFEZ) van het ministerie van JenV, de Inspectie der Rijksfinanciën (IRF) en het Wetenschappelijk Onderzoek- en Documentatie Centrum van het ministerie van JenV (WODC).
Het onderzoek naar de besparingsmogelijkheden is uitgevoerd door de NCTV en de directie FEZ van het ministerie van JenV. De resultaten hiervan zijn opgenomen in de beleidsreactie bij dit rapport.

5 SMART geformuleerd: Specifiek, Meetbaar, Acceptabel, Realistisch en Tijdgebonden

Inleiding

De comptabiliteitswet schrijft voor dat de doeltreffendheid en doelmatigheid van het beleid periodiek wordt geëvalueerd[6]. De nadere regels hiervoor zijn uitgewerkt in de Regeling Periodiek Evaluatieonderzoek (RPE)[7]. Deze regeling bepaalt dat elke vier tot zeven jaar een beleidsdoorlichting dient plaats te vinden van ieder beleidsartikel (of onderdeel daarvan) van de begroting van een ministerie.

Het artikel van deze beleidsdoorlichting betreft artikel 36.2 van de begroting van het ministerie van Justitie en Veiligheid (JenV; voorheen ministerie van Veiligheid en Justitie). Dit artikel omvat alle beleidsterreinen van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). De NCTV is in 2011 opgericht en dit is daarom de eerste beleidsdoorlichting op het beleid van de NCTV, die wordt aangeboden aan de Tweede Kamer. Daarbij merken wij op dat in het verleden wel beleidsdoorlichtingen hebben plaatsgevonden in het domein Nationale Veiligheid, zoals de beleidsdoorlichting van artikel 15 crisisbeheersing[8] van de begroting van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties(BZK). De NCTV is de voortzetting van de in 2004 opgerichte Nationaal Coördinator Terrorismebestrijding (NCTb).

De beantwoording van de vraag in hoeverre het beleid doeltreffend en doelmatig is, geschiedt aan de hand van de vragen die zijn opgenomen in de RPE. De beantwoording van deze vragen vindt plaats op basis van syntheseonderzoek, zoals benoemd in de RPE; bij de beantwoording van de vragen is uitsluitend gebruik gemaakt van de bestaande onderzoeken en evaluaties uit de afgelopen jaren en ander relevant feitenmateriaal, zoals begrotings- en realisatiecijfers. De voorgeschreven vragen komen geclusterd aan de orde in de navolgende hoofdstukken.

Hoofdstuk 1 behandelt de afbakening van het beleids- c.q. onderzoeksterrein en gaat in op de onderzoeksvragen:
1. Welk artikel (onderdeel) wordt behandeld in de beleidsdoorlichting?
2. Indien van toepassing: wanneer worden/zijn de andere artikelonderdelen doorgelicht?

Tevens gaat dit hoofdstuk kort in op de onderzoeksaanpak.

Hoofdstuk 2 beschrijft de motivering van het gevoerde beleid – aanleiding, doel en legitimiteit. Het hoofdstuk gaat in op de onderzoeksvragen:
3. Wat was de aanleiding voor het beleid? Is deze aanleiding nog actueel?
4. Welk doel of doelen heeft het beleid en wat is de verantwoordelijkheid van de rijksoverheid daarbij?

Hoofdstuk 3 geeft een uitwerking van de aard en samenhang van de ingezette instrumenten en de daarmee samenhangende uitgaven. Het hoofdstuk gaat in op de onderzoeksvragen:
5. Wat is de aard en samenhang van de ingezette instrumenten?
6. Met welke uitgaven gaat het beleid gepaard, inclusief kosten op andere terreinen of voor andere partijen?

6 Comptabiliteitswet 2001, artikel 20, tweede lid
7 Staatscourant 25 september 2014 nr. 27142
8 Beleidsdoorlichting crisisbeheersing, 20 maart 2009, KPMG

7. Wat is de onderbouwing van de uitgaven? Hoe zijn deze te relateren aan de componenten volume/gebruik en aan prijzen/tarieven?

De ingezette beleidsinstrumenten zijn in dit hoofdstuk geclusterd naar de drie hoofdtaakgebieden van de NCTV, namelijk contraterrorisme, cybersecurity en nationale veiligheid & crisisbeheersing. Het beleid van de NCTV op het gebied van verwerving van dreigingsinformatie en het maken van risico- en dreigingsanalyses zijn opgenomen onder deze drie hoofdtaakvelden.

Informatie en bevindingen over het beleid en de activiteiten van de NCTV ten aanzien van het bewaken en beveiligen van personen, objecten en vitale infrastructuur zijn, gezien de vertrouwelijkheid van deze informatie, beperkt opgenomen in dit rapport[9].

Hoofdstuk 4 biedt een overzicht van de beschikbare onderzoeken naar doeltreffendheid en doelmatigheid en de mate waarin deze dekkend zijn voor het onderzochte beleidsterrein. Dit aan de hand van de onderzoeksvragen:

8. Welke evaluaties (met bronvermelding) zijn uitgevoerd, op welke manier is het beleid geëvalueerd en om welke redenen?
9. Welke beleidsonderdelen zijn (nog) niet geëvalueerd? Inclusief uitleg over de (on)mogelijkheid om de doeltreffendheid en doelmatigheid van het beleid in de toekomst te evalueren.
10. In hoeverre maakt het beschikbare onderzoeksmateriaal uitspraken over de doeltreffendheid en doelmatigheid van het beleidsterrein mogelijk?

Daarnaast worden in dit hoofdstuk bevindingen opgenomen ten aanzien van de doeltreffendheid en doelmatigheid van het gevoerde beleid aan de hand van de onderzoeksvragen:

11. Welke effecten heeft het beleid gehad? Zijn er positieve en/of negatieve neveneffecten?
12. Hoe doeltreffend is het beleid geweest?
13. Hoe doelmatig is het beleid geweest?

De antwoorden zijn wederom per taakgebied van de NCTV uitgewerkt.

Hierbij merken wij op dat de beantwoording van de vraag over doelmatigheid en doeltreffendheid van het beleid in relatie tot het effect ervan op de nationale veiligheid zich lastig laat bepalen. Gezien deze beperking heeft de begeleidingscommissie van deze beleidsdoorlichting ervoor gekozen het onderzoek naar doeltreffendheid te richten op dat wat de NCTV vanuit haar coördinerende functie bij haar publieke en private partners wil bereiken[10].

De laatste twee vragen die zijn opgenomen in de RPE zijn, gaan over mogelijke verbetervoorstellen en beleidsalternatieven voor besparingen. Het betreft specifiek de volgende twee vragen:

14. Welke maatregelen kunnen worden genomen om de doelmatigheid en doeltreffendheid verder te verhogen?
15. In het geval dat er significant minder middelen beschikbaar zijn (-/- circa 20% van de middelen op het (de) beleidsartikel(en)), welke beleidsopties zijn dan mogelijk?

Deze twee vragen zal de NCTV, mede op basis van de uitkomsten van dit onderzoek, zelf beantwoorden en uitwerken in de beleidsreactie behorend bij dit rapport.

9 Beleid en bevindingen met een vertrouwelijk karakter worden onder rubricering opgenomen in een aparte bijlage bij dit rapport

10 Opdrachtbevestiging Beleidsdoorlichting Nationale Veiligheid (art 36 2) definitief

1 Afbakening van de beleidsdoorlichting

Dit hoofdstuk gaat in op de afbakening van de beleidsdoorlichting. Daarmee geeft dit hoofdstuk antwoord op de eerste twee vragen van de RPE:

1. Welk artikel (onderdeel) wordt behandeld in de beleidsdoorlichting?
2. Indien van toepassing: wanneer worden/zijn de andere artikelonderdelen doorgelicht?

1.1 Beleidsdoorlichting van artikel 36.2: Nationale veiligheid en terrorismebestrijding

Het begrotingsartikel van deze beleidsdoorlichting is artikel 36.2 Nationale veiligheid en terrorismebestrijding (voorheen Contraterrorisme en nationaal veiligheidsbeleid). Dit artikel betreft alle beleidsterreinen van de NCTV.
De algemene doelstelling van de NCTV luidt: '*Bijdragen aan een veilig en stabiel Nederland door het voorkomen en beperken van maatschappelijke ontwrichting door dreigingen te onderkennen, de weerbaarheid van burgers, bedrijfsleven en overheidsorganen te verhogen en de bescherming van vitale belangen te versterken*'.

De begroting 2014 -2015 van het ministerie van VenJ vermeldt over artikel 36.2 het volgende:

- De Minister van VenJ heeft een regisserende rol op het gebied van nationale veiligheid en crisisbeheersing, terrorismebestrijding en cyber security[11]. De taken worden namens de Minister uitgevoerd door de NCTV.
- Daarnaast is bij koninklijk besluit vastgelegd dat de Minister van VenJ doorzettingsmacht heeft wanneer het gaat om het voorkomen van terroristische misdrijven.
- De maatschappelijke effecten van het beleid ter bescherming van de nationale veiligheid (o.a. crisis- en cybersecuritybeleid en terrorismebestrijding) laten zich door het grote aantal activiteiten en instrumenten, de afhankelijkheid van derden bij de realisatie van de doelstellingen en met name de onvoorspelbaarheid van gebeurtenissen die de nationale veiligheid bedreigen, niet (altijd) in prestatie-indicatoren of kengetallen uitdrukken. Kwalitatieve indicatoren zijn te vinden in de voortgangsrapportages en inspectierapportages met betrekking tot contraterrorisme en -extremisme, cyber security en nationale veiligheid/ crisisbeheersing, die periodiek aan de Tweede Kamer worden aangeboden.

1.2 Onderzoek naar doeltreffendheid richt zich op wat de NCTV vanuit haar rol bij haar publieke en private partners wil bereiken

In de aankondigingsbrief van deze beleidsdoorlichting is opgenomen dat onderzoek naar de doeltreffendheid (effectiviteit) van het gevoerde beleid complex is en aandacht vereist. Uitgangspunt in het kader van de nationale veiligheid is dat risico- c.q. dreigingsgericht (op basis van potentiële risico's en dreigingen) beleidsmaatregelen worden getroffen. Dreiging is echter continu in ontwikkeling en de NCTV heeft te maken met fenomenen waarvoor niet eerder

11 De verantwoordelijkheid van de Minister is vastgelegd in het Besluit Ministeriële Commissie Crisisbeheersing (MCCB), de Wet veiligheidsregio's (verantwoordelijkheid voor het stelsel van brandweerzorg, geneeskundige hulpverlening in de regio (GHOR), rampenbestrijding en crisisbeheersing), de Politiewet 2012 (bewaken en beveiligen), de Luchtvaartwet (beveiliging burgerluchtvaart) en het koninklijk besluit van 14 december 2005 (terrorismebestrijding).

beleid is opgesteld. Daarnaast hebben verschillende wetenschappers[12] gewezen op het feit dat effecten van maatregelen om fenomenen als terrorisme te bestrijden, zich maar moeilijk laten bepalen. De NCTV is daarbij van mening dat dit ook geldt voor andere dreigingen voor de nationale veiligheid, waarbij het beleid een groot aantal voornemens, interventies en maatregelen omvat en vele partijen betrokken zijn. De causaliteit tussen ingezette beleidsinstrumenten en de doeltreffendheid ervan is volgens de NCTV lastig vast te stellen, omdat nog vele andere factoren van invloed kunnen zijn geweest op het uiteindelijk effect. Gezien voorgenoemde beperkingen heeft de begeleidingscommissie van deze beleidsdoorlichting ervoor gekozen het onderzoek naar doeltreffendheid te richten op dat wat de minister van JenV, werkende via de NCTV, vanuit zijn coördinerende functie bij de publieke en private partners wil bereiken. De maatschappelijke impact (uiteindelijk bereikte veranderingen in de maatschappij) blijft buiten beschouwing.

1.3 De beleidsdoorlichting gaat over het beleid van de periode 2011-2015

In de beleidsdoorlichting wordt de periode 2011 tot en met2015 in beschouwing genomen. Deze tijdspanne is gekozen in verband met het besluit van het toenmalige kabinet Rutte I om de veiligheidsportefeuille te concentreren bij de Minister van Veiligheid en Justitie. Begin 2011 zijn de eerste (organisatorische) contouren zichtbaar geworden van de nieuwe integrale benadering van de veiligheidsvraagstukken en zijn de desbetreffende begrotingsartikelen (de voorlopers van het huidige artikel 36.2) geïntegreerd in de begroting van het Ministerie van Veiligheid en Justitie. In 2012 is de huidige organisatie van de NCTV gevormd om de optimale samenhang te realiseren tussen de samenhangende domeinen: crisisbeheersing, rampenbestrijding, aanpak fysieke onveiligheid, cybersecurity, bestrijding terrorisme en extremisme en crisiscoördinatie en -communicatie[13].
Hierbij merken wij op dat wij in een aantal gevallen gebruik hebben gemaakt van recentere bronnen om meer inzicht te kunnen geven in de realisatie van instrumenten en de effecten van het gevoerde beleid in de periode 2011 tot en met 2015.

12 Nelen, Leeuw, Bogaerts, Antiterrorismebeleid en evaluatieonderzoek - framework, toepassingen en voorbeelden, 2010.
13 Evaluatie NCTV organisatie 2012, eindrapport, 15 september 2016

2 Motivering van het gevoerde beleid: aanleiding, doel en legitimiteit

Dit hoofdstuk gaat in op de aanleiding, het doel en de legitimiteit van het gevoerde beleid van de NCTV. Daarmee geeft dit hoofdstuk antwoord op de volgende twee vragen van de RPE:

3. Wat was de aanleiding voor het beleid? Is deze aanleiding nog actueel?
4. Wat is de verantwoordelijkheid van de rijksoverheid?

2.1 Aanleiding en legitimiteit gevoerde beleid is nog immer actueel

De aanleiding voor het beleid op contraterrorisme en het beleid ten aanzien van de nationale veiligheid is nog immer actueel. In het afgelopen decennium is gebleken dat Nederland kwetsbaar is voor rampen, aanslagen en andere incidenten. Daarbij hebben zich in het afgelopen decennium de volgende incidenten in Nederland voorgedaan:

- de aanslag tijdens Koninginnedag op 30 april 2009;
- de brand bij Chemiepack te Moerdijk in op 5 januari 2011;
- het schietincident in Alphen a/d Rijn op 9 april 2011;
- de hack bij Diginotar in 2011[14]; en
- de ramp met vlucht MH17 in 17 juli 2014;

Daarnaast hebben zich binnen Europa verschillende incidenten, rampen en aanslagen voorgedaan, waaronder:

- aanslag in een uitgaansgebied in Parijs op 13 november 2015 (Bataclan).
- aanslag op een kerstmarkt in Berlijn op 19 december 2016;
- aanslag bij het parlement in Londen op 22 maart 2017;
- aanslag in Stockholm op 7 april 2017;
- aanslag op de Champs Elysees in Parijs op 20 april 2017;
- aanslag op de Ramblas in Barcelona op 17 augustus 2017;
- grote aanval met gijzelsoftware, genaamd Wannacry in maart 2017;
- wereldwijde aanval op bedrijven met Petya virus in juni 2017;
- verwoesting van Sint Maarten door orkaan Irma in september 2017;
- vluchtelingencrisis die ontstond in 2015.

Wat in de ons omringende landen gebeurt, kan ook in Nederland gebeuren. De kans op een aanslag in Nederland is en blijft reëel. Het dreigingsniveau staat daarom al gedurende lange tijd op 'substantieel', ook in de periode waar deze beleidsdoorlichting op ziet. Dat blijkt uit opeenvolgende Dreigingsbeelden Terrorisme Nederland (DTN) van de NCTV[15].
Uit de Cybersecuritybeelden Nederland (CBSN) van de afgelopen jaren blijkt dat ook de dreiging van cybercrime nog steeds actueel is en toeneemt. Het afgelopen jaar vonden verschillende grootschalige aanvallen plaats met een hoge organisatiegraad, gericht op diefstal van geld en kostbare informatie. Naast de overheid waren bedrijven en burgers hiervan in toenemende mate het slachtoffer.

Het blijft dus belangrijk om doorlopend alert te zijn op nieuwe dreigingen ten aanzien van de (nationale) veiligheid, zoals de toenemende dreiging die uitgaat

14 DigiNotar, een bedrijf dat voor de beveiliging van overheidswebsites zorgt, kreeg in juli 2011 te maken met een hack. Hierdoor kreeg een externe partij de mogelijkheid valse SSL-certificaten uit te geven. Het gevolg was dat er meer dan 500 valse certificaten werden uitgegeven.
15 44e Dreigingsbeeld Terrorisme Nederland (DTN), april 2017 NCTV

van het jihadisme en cybercrime. Op basis van dit inzicht op nieuwe dreigingen kunnen zowel preventieve als repressieve maatregelen worden getroffen om de kans op een incident, aanslag of ramp voor zover mogelijk te beperken. Daarnaast is het belangrijk om klaar te staan als het onverhoopt toch mis gaat. Gezien de recente gebeurtenissen en actuele dreigingen was en is de motivering voor het gevoerde en te voeren beleid, nog immer legitiem.

2.2 Wat is de verantwoordelijkheid en de rol van de NCTV?

Met de oprichting van de NCTV is binnen de Rijksoverheid één organisatie verantwoordelijk voor de coördinatie van terrorismebestrijding, cybersecurity, nationale veiligheid en crisisbeheersing. Hiermee is uitvoering gegeven aan de wens om de optimale samenhang te realiseren tussen de domeinen: crisisbeheersing, rampenbestrijding, aanpak fysieke onveiligheid, cybersecurity, bestrijding terrorisme en extremisme en crisiscoördinatie en -communicatie. Tot een gecoördineerde integrale aanpak op deze domeinen is besloten, omdat de aanpak per domein gelijksoortig van karakter is: dezelfde organisatie voert in de zogenaamde 'koude fase' als de 'warme fase' de regie. Als er geen incident is, in de koude fase, zet de NCTV zich in om alle relevante publieke en private spelers maximaal toe te rusten om de dreigingen te kunnen weerstaan, te monitoren op situaties die kunnen leiden tot een crisis, incident en/ of ramp en de effecten van crises, incidenten en/ of rampen te minimaliseren. De organisatie is open en gericht op het prepareren en versterken van het netwerk. In de warme fase, als er een incident is, is de organisatie een crisismanager die besluiten voorbereidt en neemt én tevens het netwerk leidt[16].

De NCTV is ondergebracht bij het ministerie van JenV, aangezien de minister van JenV een coördinerende verantwoordelijkheid op de domeinen nationale veiligheid en crisisbeheersing, terrorismebestrijding en cybersecurity heeft. De minister vervult vanuit zijn coördinerende verantwoordelijkheid op deze domeinen drie rollen:

- een sturende rol, door directe toepassing van bevoegdheden;
- een richtinggevende rol, waarin wordt gezorgd dat de betrokken publieke en private partijen met in acht name van uitoefening van hun eigen bevoegdheden en verantwoordelijkheden één richting kiezen en een gezamenlijke aanpak ten uitvoer brengen, ook als de belangen uiteenlopen;
- een faciliterende rol, waarin publieke of private partijen worden ondersteund. Het is de verantwoordelijkheid van deze partijen om een afweging te maken en te besluiten of zij gebruik maken van deze ondersteuning.

Vanwege de coördinerende verantwoordelijkheid van de Minister van JenV voor de domeinen nationale veiligheid en crisisbeheersing, terrorismebestrijding en cybersecurity en de coördinerende rol daarbij van de NCTV, zijn er samenwerkingsverbanden en relaties met verschillende andere betrokken ministeries, medeoverheden en private organisaties. Samen met deze partners uit het veiligheidsdomein maakt de NCTV zich sterk voor een veilig en stabiel Nederland.

De NCTV gaat hierbij uit van de kracht van samenwerking om de Nederlandse vitale belangen te beschermen. Overheden, bedrijven, kennisinstellingen en maatschappelijke organisaties beschikken over een schat aan kennis en ervaring. Alleen door die te mobiliseren, kan slagvaardig opgetreden worden en kunnen dreigingen worden tegengegaan en kan eventuele schade en leed, wanneer een dreiging zich in een incident manifesteert, worden beperkt. De NCTV wil de verbindende schakel zijn binnen de veiligheidsgemeenschap. Een betrouwbare partner die met kennis van zaken partijen bij elkaar brengt, oplossingen aanreikt

16 Evaluatie NCTV organisatie 2012, Eindrapport, 15 september 2016

en partijen verder helpt. De NCTV richt zich erop om vanuit een centrale plek in de veiligheidswereld alle betrokkenen ondersteuning en advies te bieden. Dat betekent initiatieven bij elkaar brengen, kennis delen en samen reacties ontwikkelen op nieuwe dreigingen.

Voor de domeinen zijn inhoudelijke strategische kaders opgesteld waarbinnen de NCTV haar regierol en hoofdopdrachten uitvoert: de Nationale Contraterrorisme strategie, de Strategie Nationale Veiligheid en de Nationale Cyber Security Strategie. Deze drie strategieën zijn door de NCTV met haar partners[17] opgesteld. Daarnaast worden periodiek drie dreigings- en risico-inschattingen opgesteld, te weten het Dreigingsbeeld Terrorisme Nederland, het Nationaal Veiligheidsprofiel (voorheen de Nationale Risico Beoordeling) en het Cyber Security Beeld Nederland. Zij vormen elk de grondslag voor politieke en beleidsmatige keuzes, zoals onder meer te treffen maatregelen.

De NCTV voert de regie binnen de genoemde strategische kaders en wet– en regelgeving. De NCTV heeft hiervoor verschillende instrumenten, variërend van directe aansturingsbevoegheden en het uitvoeren van projecten en programma's tot het vervullen van een faciliterende expertrol. De NCTV voert regie op beleid, analyse (kennis op het gebied van risico's en dreigingen), uitvoering van wettelijke taken en communicatie binnen de drie domeinen.
De werkwijze is steeds dezelfde. Eerst wordt bezien welke dreigingen en risico's er zijn en deze worden gewogen. Op basis van deze inschattingen wordt bezien welke lange en korte termijn maatregelen kunnen en moeten worden getroffen ter directe bescherming van de belangen of ter verhoging van het weerstandsvermogen van personen, objecten, burgers en bedrijven. Dit kunnen acute maatregelen zijn, maar ook strategische programma's om bijvoorbeeld sectoren te versterken.

De NCTV vervult in de drie taakdomeinen zowel een coördinerende, adviserende als (deels) beleidsbepalende rol. In enkele gevallen vervult de NCTV ook een uitvoerende rol, zoals bijvoorbeeld binnen het taakdomein Cybersecurity, waar het Nationaal Cyber Security Centrum (NCSC) van de NCTV de taak als Computer Emergency Response Team (Cert) voor de Rijksoverheid en de vitale infrastructuur uitvoert[18].

2.3 Doelstellingen zijn gericht op een veilig en stabiel Nederland

In de begroting 2014-2015 van het ministerie van VenJ is onder artikel 36 de volgende doelstelling geformuleerd:

Bijdragen aan een veilig en stabiel Nederland door het voorkomen en beperken van maatschappelijke ontwrichting door dreigingen te onderkennen, de weerbaarheid van burgers, bedrijfsleven en overheidsorganen te verhogen en de bescherming van vitale belangen te versterken.

De NCTV is actief op de drie[19] eerder genoemde domeinen: contraterrorisme, nationale veiligheid en crisisbeheersing en cybersecurity. Elke domein heeft een eigen doelstelling, welke uiteindelijk dient bij te dragen aan het hoofddoel.

17 Het gaat hier om publieke en private partijen, kennisinstellingen en maatschappelijke organisaties die in het betreffende taakdomein een rol spelen.
18 Binnen het Cyberdomein levert NCSC ook bijdragen aan andere activiteiten. Echter is de verantwoordelijkheid van deze activiteiten vaak belegd bij andere partijen.
19 Het bewaken en beveiligen van personen, objecten en vitale processen maakt onderdeel uit van het taakdomein Contra terrorisme

De subdoelstellingen zijn:

- **Contraterrorisme**: het voorkomen van aanslagen, verminderen van de vrees voor aanslagen en beperken van gevolgen van een eventuele aanslag.
- **Nationale veiligheid en crisisbeheersing**: het voorkomen en beperken van maatschappelijke ontwrichting door rampen en crises.
- **Cybersecurity**: het versterken van de veiligheid van de digitale samenleving om daarmee het vertrouwen in het gebruik van ICT door burger, bedrijfsleven en overheid te verhogen.

2.3.1 *Beleidsdoelstellingen contraterrorisme*

Conform de Nationale contraterrorisme-strategie 2011-2015 is het hoofddoel van het contraterrorisme beleid: '..het verminderen van het risico op en de vrees voor terroristische aanslagen en het beperken van de mogelijk schade na een eventuele aanslag'[20].

Voor de uitwerking van het beleid heeft de NCTV sinds 2001 een brede benadering gehanteerd. Dat wil zeggen dat bij beleidsinitiatieven zowel aandacht is voor preventieve als voor repressieve maatregelen. In de periode 2011 -2015 kent het contraterrorisme beleid de volgende drie beleidsdoelstellingen:

1. *Verstoren van dreigingen en verijdelen van aanslagen*
   Om dreigingen te verstoren en mogelijke aanslagen te verijdelen, is het van belang om een zo goed mogelijk inzicht te hebben in de risico's die uitgaan van terroristen/ extremisten en deze te reduceren. Hierbij gaat het dan om de aanpak van onder andere jihadgangers door zowel het beperken van de toegang tot aanslagmiddelen, financiën en capaciteiten, als het tegengaan van reisbewegingen van potentiële terroristen/extremisten.

2. *Voorkomen van aanwas*
   Het doel van voorkomen van aanwas is vroegtijdig te interveniëren. Dit kan door radicaliseringprocessen bij bepaalde groepen of individuen zo vroeg mogelijk te onderkennen, zodat kan worden voorkomen dat personen doorradicaliseren en mogelijk overgaan tot terroristische daden[21] .

3. *Beschermen van personen, objecten en vitale processen tegen terroristische aanslagen*
   De NCTV heeft een bijzondere verantwoordelijkheid voor de beveiliging van een gelimiteerd aantal personen, objecten en diensten. Daarnaast voert de NCTV de landelijke coördinatie van het stelsel bewaken en beveiligen. Het doel van het stelsel bewaken en beveiligen is het voorkomen van (terroristische) aanslagen op personen, objecten en diensten door het treffen van beveiligingsmaatregelen, waarmee het veilig en ongestoord functioneren wordt beoogd van degene tot wie de dreiging zich richt.

Inlichtingen- en informatieverwerving vormen de basis voor contraterrorisme beleid. Een snelle beschikbaarheid van objectieve en betrouwbare inlichtingen dient als fundament voor alle mogelijke contraterrorisme maatregelen of inspanningen in binnen- en buitenland[22].

De beleidstheorie achter de contraterrorisme inzet van de NCTV is in de periode waarover deze beleidsdoorlichting gaat, voor een belangrijk deel ingekaderd door de Nationale contraterrorisme-strategie 2011-2015.

20 Nationale Contraterrorisme strategie 2011-2015, p. 17
21 Nationale Contraterrorisme strategie 2011-2015, p. 63
22 Nationale Contraterrorisme strategie 2011-2015, p. 53

Daarnaast werd in de zomer van 2014 aanvullend een Actieprogramma integrale aanpak jihadisme[23] opgesteld om een impuls te geven aan de bestrijding van de jihadistische dreiging waarmee Nederland zich geconfronteerd zag. In het Actieprogramma werden de op dat moment bestaande en belangrijkste beleidsinstrumenten en -initiatieven samengebracht en verder geïntensiveerd. Tevens werden enkele nieuwe beleidsinstrumenten en maatregelen voorgesteld.

2.3.2 *Beleidsdoelstellingen nationale veiligheid en crisisbeheersing*

Het hoofddoel van crisisbeheersing is om *maatschappelijke ontwrichting door een crisis of ramp te voorkomen en te beperken* door dreigingen te onderkennen, de weerbaarheid van burgers, bedrijfsleven en overheidsorganen te verhogen en bescherming van vitale belangen te versterken[24.]

Prioritaire subthema's in het domein van crisisbeheersing, rampenbestrijding en brandweerzorg waren de afgelopen jaren het versterken van het samenhangend stelsel van crisisbeheersing en het beschermen van de vitale infrastructuur in Nederland. In de periode 2011 -2015 kende het beleid ten aanzien van nationale veiligheid en crisisbeheersing de volgende beleidsdoelstellingen:

1. *Verbeteren van het functioneren van het stelsel van crisisbeheersing*
   De minister van Veiligheid en Justitie is verantwoordelijk voor het goed functioneren van het gehele stelsel van crisisbeheersing, rampenbestrijding en brandweerzorg en gedeeltelijke financiering[25] van de veiligheidsregio's. Voor een goed functionerend stelsel is het essentieel dat taken en verantwoordelijkheden bestuurlijk duidelijk zijn toebedeeld en randvoorwaarden helder zijn omschreven. Dubbelingen en hiaten in het stelsel zijn niet wenselijk. Ook is zicht op dreigingen een belangrijk onderdeel in het stelsel crisisbeheersing. In het verlengde van verantwoordelijkheden en passend bij de benoemde dreigingen en crises moet immers de bijbehorende operationalisering worden vorm gegeven. Daarbij moet elke verantwoordelijke (organisatie) de passende uitvoering regelen, maar moet ook de afstemming tussen en samenwerking van de diverse organisaties kloppen. De organisaties moeten op hun taak zijn berekend.

2. *Vergroten van de weerbaarheid van de vitale infrastructuur*
   De minister van VenJ heeft een coördinerende verantwoordelijkheid bij het beschermen van de Nederlandse nationale veiligheid om maatschappelijke ontwrichting te voorkomen. Om deze te beschermen, richt de minister, via de NCTV, zich naast het aanpakken van dreigingen ook op het verhogen van de weerbaarheid.
   De NCTV heeft zich hierbij met name gericht op versterken van de weerbaarheid van de vitale infrastructuur, economische veiligheid en de weerbaarheid van het Rijk tegen spionage

2.3.3 *Beleidsdoelstellingen cybersecurity*

Dit beleidsterrein is vanaf 2012 opgenomen binnen de VenJ-organisatie en de VenJ-begroting. Het betreft een relatief jong beleidsterrein dat nog volop in ontwikkeling is. De Nationale Cybersecurity Strategie[26] is richtinggevend voor de activiteiten van de bij cybersecurity betrokken organisaties en de onderlinge samenwerking. Het door de NCTV jaarlijks uitgebrachte dreigingsbeeld van cybersecurity benadrukt de *sense of urgency* voor het versneld instellen van

23 Actieprogramma integrale aanpak Jihadisme, 29 augustus 2014
24 Factsheet Strategie Nationale Veiligheid 2013
25 Circa 90% van de financiering van de veiligheidsregio's verloopt via het Gemeentefonds.
26 Nationale Cybersecurity Strategie 1, 22 februari 2011 en Nationale Cybersecurity Strategie 2, 28 oktober 2013; in de NCSS zijn activiteiten van meerdere ministeries opgenomen die binnen de verantwoordelijkheid van deze Ministeries worden uitgevoerd; de NCTV vervult een tevens een coördinerende rol in de totstandkoming van de NCSS

maatregelen om voldoende weerbaarheid tegen de huidige cybersecurity dreiging te bieden, alsook de kansen te benutten van de digitale economie in Nederland.

Conform de eerste nationale cybersecurity strategie[27] is het hoofddoel van het cybersecurity beleid: '*het versterken van de veiligheid van de digitale samenleving om daarmee het vertrouwen in het gebruik van ICT door burger, bedrijfsleven en overheid te verhogen*. Daartoe wil de Nederlandse overheid met andere partijen slagvaardiger werken aan de veiligheid en de betrouwbaarheid van een open en vrije digitale samenleving. Dit met als doel de economie te stimuleren en de welvaart en het welzijn te verhogen door een goede rechtsbescherming in het digitale domein te garanderen en maatschappelijke ontwrichting te voorkomen, dan wel dat adequaat wordt opgetreden als het toch mis gaat.

In de tweede nationale cybersecurity strategie[28] wordt een beweging van bewust naar bekwaam gemaakt. Als visie is gesteld: Nederland zet samen met zijn internationale partners in op een veilig en open cyberdomein, waarin de kansen die digitalisering onze samenleving biedt volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd. Dit sluit aan op het doel van de eerste strategie.
Qua beleid kan de eerste strategie worden beschouwd als inventariserend en geeft de tweede strategie een concretere invulling van de bijdrage aan de doelstelling.

Om het doel van de NCSS te bereiken, zijn de volgende actielijnen gekozen:
- Nederland zorgt voor een integrale aanpak van cybersecurity door publieke en private partijen;
- Nederland zorgt voor adequate en actuele dreiging- en risicoanalyses;
- Nederland versterkt de weerbaarheid tegen ICT-verstoringen en cyberaanvallen;
- Nederland versterkt responscapaciteit om ICT-verstoringen en cyberaanvallen te pareren;
- *Nederland intensiveert opsporing en vervolging van cybercrime;*
- *Nederland stimuleert onderzoek en onderwijs.*

De eerste vier actielijnen vormen de basis voor de uitwerking van de beleidstheorie in deze beleidsdoorlichting. Opsporing en vervolging van cybercrime behoort niet tot het taakveld van de NCTV en zij heeft dus ook zeer beperkte invloed op de intensivering hiervan. Het maakt geen deel uit van artikel 36.2 van de begroting van het ministerie van JenV en dus ook niet van deze beleidsdoorlichting. De laatste actielijn is gericht op stimuleren van onderzoek en onderwijs. Dit aspect hebben wij geplaatst onder versterken van de weerbaarheid, zoals in hoofdstuk 3 verder zal worden toegelicht. Een kanttekening is dat de eerste twee actielijnen - integrale aanpak en een betere dreiging- en risicoanalyses - ook invloed hebben op de actielijnen gericht op het versterken van de weerbaarheid en responscapaciteit.

27 Nationale Cybersecurity Strategie 1, 22 februari 2011, p.4
28 Nationale Cybersecurity Strategie 2, 28 oktober 2013, p.17

3 Aard en samenhang van ingezette instrumenten en samenhangende uitgaven

Dit hoofdstuk geeft antwoord op de volgende vragen van de RPE:
5. Wat is de aard en samenhang van de ingezette instrumenten?
6. Met welke uitgaven gaat het beleid gepaard, inclusief kosten op andere terreinen of voor andere partijen?
7. Wat is de onderbouwing van de uitgaven? Hoe zijn deze te relateren aan de componenten volume/gebruik en aan prijzen/tarieven?

In paragraaf 3.1 t/m 3.3 beantwoorden we de eerste vraag. Mede uit oogpunt van eenheid van overzichtelijkheid en presentatie hanteren wij de indeling van de drie taakvelden van de NCTV - contraterrorisme, nationale veiligheid en crisisbeheersing en cybersecurity - als uitgangspunt voor de indeling bij het beschrijven van de beleidsinstrumenten. Elk taakveld heeft zijn eigen doelstelling en bijbehorend specifiek beleid. Uiteindelijk dient het geheel bij te dragen aan het hogere doel en bijbehorende beleidsdoelstellingen van de NCTV zoals eerder omschreven in hoofdstuk 2.
In paragraaf 3.4 beantwoorden we de andere twee RPE-vragen.

3.1 Instrumenten Contraterrorisme zijn gericht op drie doelstellingen

Zoals beschreven in hoofdstuk 2 zijn de door de NCTV ingezette instrumenten in het kader van het contraterrorismebeleid over de periode 2011 -2015 te verdelen over drie beleidsdoelstellingen:
1. Verstoren van dreigingen en verijdelen van aanslagen
2. Voorkomen van aanwas
3. Beschermen van personen, objecten en vitale processen tegen terroristische aanslagen

Hieronder worden per beleidsdoelstelling CT de beleidsinstrumenten uiteengezet.
N.B.: Voor een gedetailleerd en volledig overzicht van alle ingezette beleidsinstrumenten in het kader van het contraterrorismebeleid verwijzen wij naar bijlage 2.

3.1.1 *Verstoren van dreigingen en verijdelen aanslagen door beperken van toegang tot middelen en tegengaan van reisbewegingen*

Om te voorkomen dat onderkende dreigingen tot geweld of aanslagen leiden, zet de NCTV in op het beperken van de toegang van potentiële terroristen en extremisten tot aanslagmiddelen, financiën en capaciteiten, en het tegengaan van potentiële reisbewegingen. Hiervoor is het beleid van de NCTV gericht op twee soorten instrumenten, die hierna nader zijn toegelicht.

A. Ontwikkelen, ondersteunen en beschikbaar stellen van instrumenten voor partners

De NCTV equipeert en ondersteunt partners binnen het netwerk om zo goed mogelijk hun rol te kunnen uitvoeren door het ontwikkelen van instrumentarium (‘gereedschapskist’) dat toegepast kan worden om dreiging die van personen en netwerken uitgaat te verminderen en om geweld/terrorisme/aanslag te voorkomen. Met de inzet van de (straf-, vreemdelingen- en bestuursrechtelijke) instrumenten wordt onder meer mogelijk gemaakt dat eerder maatregelen kunnen worden genomen om (potentiële) terroristen/ extremisten aan te pakken

en potentiële uitreizen te voorkomen of bemoeilijken. Hierna is uiteengezet welke initiatieven de NCTV in de periode 2011- 2015 heeft ondernomen.

Aanjagen van en bijdragen aan wijzigingen in wet- en regelgeving
De NCTV jaagt als beleidscoördinator vooral aan dat wetten worden aangepast en nieuwe bevoegdheden worden gecreëerd op het moment dat gaten in de aanpak worden geconstateerd. De NCTV draagt daarnaast bij aan de onderbouwing van de memorie van toelichting. Het gaat om wetsvoorstellen met nieuwe bevoegdheden om de risico's die uitgaan van potentiële terroristen en extremisten te beperken en terrorisme te bestrijden. Hierbij gaat het onder andere om de Tijdelijke wet bestuurlijke maatregelen terrorismebestrijding (TWMBT), wijziging van de Paspoortwet en een wetsvoorstel beëindiging grond uitkeringen bij deelname aan een terroristische organisatie.

Ontwikkelen van, adviseren over én toepassen van maatregelen en interventies
Om risico's van jihadistische personen te reduceren en terrorisme te bestrijden worden (proces)afspraken gemaakt met ketenpartners en adviseert de NCTV de partners over, en ondersteunt bij, de inzet van specifieke interventies. Hieronder vallen onder andere de volgende activiteiten:
- Afspraken met DGSenB, DJI en OM dat alle verdachten en veroordeelden voor een terroristisch misdrijf conform regelgeving direct geplaatst worden op een Terroristen Afdeling (TA).
- Onderzoeken van de juridische kaders voor uitwisselen informatie over personen in het casusoverleg en opstellen van een landelijk beschikbaar modelconvenant samen met partners voor casusoverleggen jihadisme op lokaal niveau.
- Afspraken met de IND dat onderkende uitreizigers met een niet EU nationaliteit ongewenst vreemdeling worden verklaard (voor het Schengengebied).

Versterken informatie-uitwisseling voor detectie en tegengaan van reisbewegingen
Voor het volgen en tegengaan van reisbewegingen is de detectiecapaciteit en informatie-uitwisseling van wezenlijk belang. De NCTV heeft hiervoor onder andere ingezet op de volgende activiteiten in dit kader :
- Identificeren van hiaten in de Europese (en internationale) informatie-uitwisseling. Daartoe heeft een kopgroep van EU-lidstaten dat het meest getroffen is door jihadgangers onder leiding van Nederland een Europees actieplan opgesteld dat is gepresenteerd in de JBZ Raad (december 2014).
- Onderkende uitreizigers worden geplaatst in de internationale en Europese signaleringssystemen.
- De realisatie vande technische voorziening reisgegevens Travel Information Portal (TRIP). TRIP is belangrijk voor de ontsluiting en verwerking van bestaande stromen van passagiersgegevens op basis van bestaande wetgeving.

B. Coördineren en faciliteren van lokale, nationale en internationale samenwerkingsverbanden

Inlichtingen- en informatieverwerving vormen de basis voor het contraterrorisme beleid. Een snelle beschikbaarheid van objectieve en betrouwbare inlichtingen dient als fundament voor alle mogelijke contraterrorisme maatregelen of inspanningen in binnen- en buitenland[29]. Om het netwerk te coördineren en te faciliteren, wordt een structuur opgezet. Deze structuur is ten eerste nodig om tijdig zicht te krijgen op dreigingen en ten tweede om het stelsel aan partijen te versterken. Daarnaast wordt geïnvesteerd in kennis, kunde en samenwerkingsverbanden op lokaal, nationaal en internationaal niveau om de effectiviteit van de betrokken organisaties te optimaliseren. De NCTV heeft zich hiervoor gericht op activiteiten zoals hieronder uiteengezet.

29 Nationale Contraterrorisme strategie 2011-2015, p. 53

Opzetten (samenwerkings)structuur en verbeteren informatie-uitwisseling
De NCTV heeft ingezet op het opzetten van een lokale en nationale (samenwerkings)structuur en het verbeteren van de (operationele) informatie-uitwisseling. Ondernomen activiteiten in dit kader zijn:

- Verwerking van inlichtingenproducten en vervaardiging van analyseproducten en het monitoren en analyseren op trendniveau van dreigingen om anderen in staat te stellen te kunnen handelen (onder meer door uitbrengen DTN en diverse monitoring – en analyseproducten).
- De NCTV stelt adviseurs beschikbaar voor de betrokken gemeenten. De adviseurs ondersteunen gemeenten bij kennis en kunde over het dreigingsniveau en het fenomeen jihadisme en de aanpak ervan. Ondermeer door het verstevigen van samenwerkingsverbanden, het wegnemen van barrières voor informatie-uitwisseling en advisering over handelingsperspectief (van preventie tot repressie, van projecten tot individuen).
- Intensivering van de samenwerking in de vreemdelingenketen door awareness bijeenkomsten te organiseren samen met de IND, COA en DT&V en de Vreemdelingenketen en het CT-netwerk op onderdelen te verbinden.
- Het verlenen van consulaire bijstand in aangrenzende landen van personen die uit eigen beweging terug keren naar Nederland, omdat zij uit jihadistische beweging of terroristische organisatie willen stappen.

Intensivering van de internationale samenwerking en aanpak jihadgangers
Om de internationale samenwerking en aanpak te versterken, worden internationale afspraken gemaakt over het delen van informatie over concrete activiteiten. Hierbij vervult de NCTV de rol van trekker of deelnemer aan internationale gremia en werkgroepen. Zoals vervulling van het co-leadership van de workstream Foreign Terrorist Fighters (samen met Marokko) in het verband van het Global CounterTerrorism Forum (GCTF).

3.1.2 *Voorkomen van aanwas door ondermijning aanbod propaganda en verhogen weerbaarheid kwetsbare groepen*

Rekrutering tot de jihadistische beweging richt zich op vatbare jongeren, vaak in het sociale netwerk van de harde kern leden. Een effectieve preventieve aanpak is daarom een gerichte aanpak ter versterking van de weerbaarheid van kwetsbare jongeren en de ondersteuning van volwassenen om hen heen om signalen van (door)radicalisering vroegtijdig te herkennen en ontsporingen te voorkomen.
Het contraterrorismebeleid is daarom gericht op het ondermijnen van het aanbod terroristische en extremistische propaganda en het verhogen van de weerbaarheid van kwetsbare groepen en hun omgeving.

De NCTV richt zich op het coördineren en faciliteren van het netwerk aan partijen (lokaal en landelijk) waarbinnen activiteiten ter voorkoming van aanwas moeten plaatsvinden.

A. Coördineren en faciliteren van het netwerk aan partijen waarbinnen activiteiten ter voorkoming van aanwas moeten plaatsvinden

Om radicalisering te voorkomen, signaleren en effectief aan te pakken, is deskundigheid nodig: up-to-date kennis over fenomenen en praktische expertise over interventies. Inlichtingen- en informatieverwerving vormen de basis voor contraterrorismebeleid. Een snelle beschikbaarheid van objectieve en betrouwbare inlichtingen dient als fundament voor alle mogelijke contraterrorisme maatregelen of inspanningen in binnen- en buitenland.

Om het netwerk te coördineren en te faciliteren, wordt een structuur opgezet om tijdig zicht te krijgen op dreigingen en om het stelsel aan partijen en professionals te versterken. Hieronder is uiteengezet waar de NCTV in de periode 2011 – 2015 op heeft ingezet.

Opzetten structuur en verbeteren informatie-uitwisseling
De NCTV heeft ingezet op het opzetten van een structuur (informatie en dreigingsanalyse) om tijdig zicht te krijgen op (potentiële) dreigingen, maar ook voor het duiden van (potentiële) dreigingen. Dit wilde de NCTV bereiken door in te zetten op de volgende activiteiten:

- Versterking van de vroegsignalering en monitoring van radicalisering, in het bijzonder gericht op wijken met de grootste kwetsbaarheid;
- Verwerking van inlichtingenproducten en vervaardiging van analyseproducten;
- Het monitoren en analyseren op trendniveau van dreigingen om anderen in staat te stellen te kunnen handelen (onder meer door uitbrengen DTN endiverse monitorings– en analyseproducten);
- Oprichting van een nationaal meldpunt radicalisering voor alle vormen van extremisme en terrorisme;
- De NCTV stelt adviseurs beschikbaar voor de betrokken gemeenten. De adviseurs ondersteunen gemeenten bij kennis en kunde over dreigingsniveau en fenomeen jihadisme en de aanpak ervan. Ondermeer door het verstevigen van samenwerkingsverbanden, het wegnemen van barrières van informatie-uitwisseling en advisering over handelingsperspectief (van preventie tot repressie, van projecten tot individuen);
- Zorgen dat betrokken burgers radicaliserende, haatzaaiende jihadistische content op internet en social media kunnen melden en dat producenten en verspreiders van online jihadistische propaganda – en de digitale platforms die zij misbruiken – worden geïdentificeerd. Daarnaast wordt deze informatie actief gedeeld met de handelingsbevoegde instanties en relevante dienstverleners.

Versterken van het netwerk lokaal en landelijk gericht op ingrijpen bij radicalisering
De NCTV wilde het stelsel aan partijen en professionals, lokaal en landelijk, die tijdig moeten ingrijpen bij radicalisering en deradicalisering beter equiperen en versterken. Hiervoor heeft de NCTV ingezet op:

- Deskundigheidsbevordering in de uitvoering door onder andere gerichte voorlichting en ontwikkeling van specialistische trainingen en vakopleidingen, de ondersteuning van onderwijsinstellingen en de oprichting van een expertcentrum dat de informatiepositie van het Rijk en de gemeenten over radicalisering versterkt;
- Oprichting van een EXIT-faciliteit in Nederland, die personen die uit een jihadistische beweging of terroristische organisatie willen stappen, onder strenge voorwaarden hierbij begeleidt;
- Oprichting van een ondersteuningsfaciliteit waarmee familie of vrienden van geradicaliseerde individuen en uitreizigers worden ondersteund.

- Samenwerking met de islamitische gemeenschap door periodiek overleg met imams.
- Ondersteuning bij het versterken van bestaande netwerken van lokale en landelijke sleutelfiguren die het alternatieve geluid uitdragen en stelling nemen tegen jihadisme.
- Versterking van netwerken rond jongeren en hun opvoeders. Daarbij wordt een laagdrempelig aanbod van professionele opvoedondersteuning gestimuleerd.
- Stimulering van het maatschappelijke debat over de grenzen van de rechtstaat.
- Mobilisering van de maatschappelijke tegengeluiden en versterking van de weerbaarheid tegen radicalisering en spanningen door onder andere kleinschalige initiatieven te ondersteunen. Bijvoorbeeld lokale voorlichtingsbijeenkomsten in betrokken gemeenschappen over ronseling en

online gevaren voor jongeren en initiatieven gericht op de dialoog binnen de gemeenschappen over radicalisering en normoverschrijdend gedrag.

3.1.3 *Beschermen van personen, objecten en vitale processen tegen terroristische aanslagen*

De NCTV heeft een bijzondere verantwoordelijkheid voor de beveiliging van een aantal personen, objecten en diensten die voorkomen op de zogenoemde limitatieve lijst. De NCTV draagt zorg voor het stelsel bewaken en beveiligen en is verantwoordelijk voor de beveiliging van de burgerluchtvaart.
Hieronder worden de beleidsinstrumenten waarop de NCTV in de periode 2011 - 2015 heeft ingezet nader toegelicht.

A. Verder professionaliseren van het stelsel Bewaken en Beveiligen

Het dreigingsbeeld, de aard en de omvang van dreiging en aanslagen en incidenten leggen een bepaalde druk op het stelsel bewaken en beveiligen. Daarmee is een duidelijke noodzaak om het stelsel te blijven (door)ontwikkelen en professionaliseren. Hiervoor heeft de NCTV ingezet op het uitvoeren van een evaluatie van het stelsel B&B en opstellen van een werkwijze voor Nationale Evenementen.

Uitvoeren van een evaluatie van het stelsel Bewaken en Beveiligen

Een onderzoek naar de werking van de kritische (werk)processen die binnen en tussen de verschillende partners plaatsvinden en die direct van invloed zijn op de effectiviteit van het stelsel.

Opstellen van een werkwijze voor Nationale Evenementen

Met de werkwijze wordt beoogd Nationale Evenementen veilig en ongestoord te laten verlopen, zonder afbreuk te doen aan het karakter van het evenement. Het doel van de werkwijze is dat alle partners, die in de voorbereiding en uitvoering betrokken zijn bij bewakings- en beveiligingsaspecten, te informeren en te voorzien van een duidelijke handreiking.

B. Intensiveren van de aanpak gericht op solistische dreigers

Doel is de dreiging die uitgaat van bepaalde groepen dreigers zoveel als mogelijk weg te nemen, zodat minder (dan wel geen) beveiligingsmaatregelen noodzakelijk zijn. Hierdoor is de impact op de te beveiligen persoon minder groot en kan de te beveiligen persoon behalve veilig ook zo ongestoord mogelijk functioneren. Hiervoor heeft de NCTV ingezet op het project solistische dreigers.

C. Toekomstbestendig maken van de beveiligingscontroles op de luchthavens

De strategische inzet voor het domein beveiliging burgerluchtvaart is gericht op mogelijke toepassing van nieuwe technologieën om nieuwe vormen van dreiging tegen te gaan, met bijzondere aandacht voor de ontwikkelingen in de burgerluchtvaart (ofwel aandacht voor maatwerk en rekening houdend met het belang van passagier en luchthaven). Hiertoe heeft de NCTV in de periode 2011-2015 ingezet op het verschillende projecten gericht op het beveiligingsproces en aanpassing van de internationale regelgeving

Projecten gericht op een efficiënter en effectiever beveiligingsproces

De kern van de activiteiten is gericht op de ontwikkeling van een proof of concept van een beveiligingsinfrastructuur, die risk based security mogelijk maakt. Inzet was daarom om met Schiphol en fabrikanten te werken aan beveiligingsapparatuur die een risicogebaseerde screening mogelijk maakt.
Er zijn verschillende door de NCTV geïnitieerde projecten uitgevoerd die tot doel hebben om het beveiligingsproces, zowel in het geheel als op onderdelen

effectiever in termen van detectiemogelijkheden, efficiënter en passagiersvriendelijker te laten verlopen.

Aanpassing internationale regelgeving
Aanpassing van de Europese regelgeving vormt een essentiële voorwaarde om nieuwe technologieën toe te kunnen passen. De NCTV heeft presentaties over deze projecten gehouden voor o.a. partner organisaties, de Europese Commissie, IATA en lidstaten tijdens overleggen, seminars, congressen en bezoeken om hiervoor draagvlak te creëren en concrete aanpassingen in de Europese regelgeving te realiseren.

3.2 Instrumenten nationale veiligheid en crisisbeheersing gericht op twee doelstellingen

Zoals beschreven in hoofdstuk 2 zijn de door de NCTV ingezette instrumenten in het kader van nationale veiligheid en crisisbeheersing over de periode 2011 - 2015 te verdelen over de beleidsdoelstellingen:
1. het verbeteren van het functioneren van het stelsel van crisisbeheersing
2. het vergroten van de weerbaarheid van de vitale infrastructuur.

Op het terrein van de crisisbeheersing, de rampenbestrijding en de brandweerzorg zijn nog vele ontwikkelingen gaande voortvloeiend uit de evaluatie van het functioneren van de Wet veiligheidsregio's in 2013[30].

Hieronder worden per beleidsdoelstelling de beleidsinstrumenten uiteengezet.
N.B.: Voor een gedetailleerd en volledig overzicht van alle ingezette beleidsinstrumenten in het kader van nationale veiligheid en crisisbeheersing verwijzen wij naar bijlage 3.

3.2.1 *Verbeteren van het functioneren van het stelsel van crisisbeheersing door coördinatie en het vereenvoudigen van besluitvorming*

De ingezette instrumenten rond het crisisbeheersingsstelsel hebben zich voornamelijk gericht op coördinatie, het flexibiliseren en het vereenvoudigen van besluitvorming op het gebied van crisisbeheersing. Meer in het bijzonder hadden de instrumenten betrekking op het opbouwen, onderhouden en/of versterken van de nationale en decentrale (veiligheidsregio's) crisisorganisatie en de samenhang daartussen, de samenwerking en de informatievoorziening.

A. Versterken nationale crisisorganisatie
Het doel van het versterken van de nationale crisisorganisatie is het realiseren van een (rijksbrede) crisisorganisatie die op professionele en effectieve wijze om kan gaan met (potentiële) nationale en internationale crises. Hierbij wordt uitgegaan van een rolvaste aanpak, gebaseerd op een heldere verdeling van verantwoordelijkheden van de betrokken partijen binnen de rijksoverheid en daarbuiten. Om het voorgaande te realiseren, heeft de NCTV in de periode 2011-2015 ingezet op onderstaande aspecten.

Vergroten van de efficiency en effectiviteit van de crisisbesluitvorming
Hiervoor is ingezet op het vereenvoudigen en flexibiliseren van de nationale crisisbeheersingsorganisatiestructuur.

Vergroten van het inzicht in risico's en capaciteiten
Om op een systematische manier inzicht te krijgen in mogelijke dreigingen voor de Nederlandse samenleving en de mate waarin de Nederlandse maatschappij zich te weer kan stellen tegen deze dreigingen, wordt de werkwijze Strategie

30 Evaluatie Wet Veiligheidsregio's, Andersson Elffers Felix, 3 juli 2013

Nationale Veiligheid[31] toegepast, stelt het Analistennetwerk Nationale Veiligheid een Nationale Risicobeoordeling (NRB) op en wordt de weerbaarheid van de maatschappij door middel van capaciteitenanalyses in kaart gebracht.

(Laten) ontwikkelen nationale crisisplannen
Mede op basis van de risico's in de NRB worden specifieke crisisplannen ontwikkeld.

Rijksbreed systeem van opleiden, trainen, oefenen, evalueren en leren
Dit om te zorgen voor (rolgerichte) opleidingen en trainingen voor crisisprofessionals en blijvend te leren en structureel lessen te trekken uit incidenten, crises en oefeningen wordt de Nationale Academie voor Crisisbeheersing (NAC) opgericht en onderhouden.

Realiseren voorzieningen om continuïteit van de Rijkscrisisfunctie te waarborgen
Om 24 uur per dag, 365 dagen per jaar beschikbaarheid te waarborgen, wordt een uitwijklocatie voor de crisisfunctie gerealiseerd op een veilige, snel bereikbare locatie, voor de gevallen waarin de Rijkscrisisfunctie niet op de hoofdlocatie uitgeoefend kan worden.

Onderhoud Nationaal Crisiscentrum (NCC)
Snelheid en zorgvuldigheid zijn essentieel in crisisbesluitvorming. Het NCC is het rijksbrede crisiscentrum dat werkt voor en met departementen. Juist in crisistijd kunnen departementale grenzen vervagen als de situatie daarom vraagt. Dan gelden andere vormen van interdepartementale samenwerking. Onderhoud van het NCC is belangrijk om aansluiting te houden bij de actuele behoefte.

Onderhoud opgeschaald Landelijk Operationeel Coördinatiecentrum (LOCC)
De NCTV investeert onder andere in de aansluiting van het LOCC op de 112 centrale en Operations van de Nationale Politie. Hierdoor kan bij een crisis het landelijke veiligheidsbeeld permanent worden gemonitord.

B. Versterken presterend vermogen veiligheidsregio's en Caribisch Nederland

De veiligheidsregio is verantwoordelijk voor de uitvoering van de taken risicobeheersing, brandweerzorg, geneeskundige hulpverlening en crisisbeheersing. Op decentraal niveau vormt de veiligheidsregio het hart van de crisisbeheersingsorganisatie, ook bij openbare ordeproblemen.
Doelstelling voor de NCTV is taakvolwassen regionale organisatie(s) voor brandweerzorg en crisisbeheersing te (laten) realiseren, die invulling kunnen geven aan hun wettelijke taken[32]. Om het voorgaande te realiseren, heeft de NCTV ingezet op onderstaande aspecten.

Evalueren van de Wet veiligheidsregio's[33]
Een evaluatieonderzoek naar de Wet veiligheidsregio's om te bezien in hoeverre de wet in de praktijk aan de verwachtingen voldoet wat betreft het functioneren van het stelsel (de realisatie van de aannames over het bijdragen aan een efficiënte en kwalitatief hoogwaardige organisatie van de brandweerzorg, geneeskundige hulpverlening, rampenbestrijding en crisisbeheersing onder één regionale bestuurlijke regie) en hoe actoren dat ervaren. Aan de Evaluatiecommissie Hoekstra is vervolgens gevraagd te adviseren over de werking van de Wet veiligheidsregio's en het Nederlandse stelsel van rampenbestrijding en crisisbeheersing.

31 Werkwijze Nationale Veiligheid, BZK, 2010
32 Wet Veiligheidsregio's, 11 februari 2010
33 Evaluatie Wet Veiligheidsregio's, Andersson Elffers Felix, 3 juli 2013

Verbeteren van de regelgeving voor veiligheidsregio's
Mede op basis van de uitkomsten van de evaluatie op de Wet Veiligheidsregio's de regelgeving aanpassen en actualiseren.

Verbeteren van de ondersteuning van veiligheidsregio's
Ter ondersteuning van de regio's is het Instituut Fysieke Veiligheid (IFV) opgericht.

Brede Doeluitkering (BDUR) aan de veiligheidsregio's en de herijking en actualisatie daarvan
Met een bijdrage op basis van het Besluit Veiligheidsregio's worden de veiligheidsregio's mede in staat gesteld uitvoering te geven aan het beleid met betrekking tot brandweer, geneeskundige hulpverlening, rampenbestrijding en crisisbeheersing

Verhogen presterend vermogen veiligheidspartners
Het presterend vermogen van de veiligheidspartners verhogen door te bevorderen dat het Veiligheidsberaad[34] een eigen strategische agenda uitvoert ten aanzien van bevolkingszorg, kwaliteit en vergelijkbaarheid en bovenregionale operationele besluitvorming.

Versterken brandweer
Het verhogen van het prestatievermogen van de brandweer door onder meer:
- een verplichte regionalisering van de brandweer;
- een verdere professionalisering van de operationele inzet door onderzoek opkomsttijden en variabele voertuigbezetting;
- verbetering van de brandweerstatistiek door onderzoek;
- sluiten van een convenant met onder andere het Veiligheidsberaad ter verbetering van het brandweeronderwijs.

Versterken GHOR
Verhogen van het prestatievermogen van de GHOR door het vastleggen van bekwaamheidseisen GHOR-functionarissen in het Besluit Personeel Veiligheidsregio's (BPV) en het maken van afspraken over de rol van het Rode Kruis bij rampen en crisis en over de Grootschalige Geneeskundige Bijstand.

Versterken en verbeteren crisisbeheersing Caribisch Nederland
Verbeteren van de crisisbeheersing in Caribisch Nederland door de invoering en bevordering van de implementatie van wet- en regelgeving crisisbeheersing en brandweerzorg Caribisch Nederland. Dit door onder andere ondersteuning te bieden bij de planvorming.

C. Versterken samenwerking met verschillende partijen
De NCTV opereert in een omvangrijk netwerk van partijen, zowel publiek als privaat, op (inter) nationaal, regionaal en lokaal niveau. Dit zijn bijvoorbeeld andere ministeries, veiligheidsregio's, Nationale Politie (NP), waterschappen, Rode Kruis, en private partijen in de vitale processen en internationale organisaties zoals de EU en de NATO.
Het is de uitdaging van de NCTV om met deze partijen te zorgen dat voldaan wordt aan alle vereisten om op de juiste wijze te kunnen functioneren in het stelsel van crisisbeheersing. De NCTV zorgt voor de samenhang en integrale aanpak van risico- en crisisbeheersing.

De NCTV maakt daarbij gebruik van diverse instrumenten variërend van harde (bijvoorbeeld sturen door middel van regelgeving) tot zachte (bijvoorbeeld een

34 De voorzitters van de 25 veiligheidsregio's vormen samen het Veiligheidsberaad. Dit landelijke overleg is opgericht in februari 2007 en komt vier keer per jaar bijeen.

collegiaal gesprek) instrumenten met alles wat daartussen zit (bijvoorbeeld faciliteren, ondersteunen, adviseren en richting geven).
Hierna is uitgewerkt waar de NCTV in de periode 2011- 2015 op heeft ingezet om de samenwerking te verbeteren.

Versterking van de aansluiting Rijk – regio
Versterking van de bovenregionale samenwerking en de samenwerking tussen regio's en het Rijk door middel van:
- Bevorderen van een opschalingsstructuur van de veiligheidsregio's en de wettelijke verankering daarvan;
- Instellen c.q. versterken van crisisexpertteams;
- En een betere afstemming tussen de Nationale Risicobeoordeling en de risicoprofielen van de veiligheidsregio's.

Bevorderen samenwerking door gezamenlijke vaststelling en uitvoering prioriteiten en doelstellingen
Bevorderen dat onder andere het Rijk en de veiligheidsregio's gezamenlijk uitvoering geven aan gezamenlijke doelstellingen op het gebied van water en evacuatie, stralingsincidenten en continuïteit van de samenleving.
Tevens stimuleren van de veiligheidsregio's, de vitale sectoren en politie om afspraken te maken over samenwerking tijdens een crisis en de voorbereiding daarop. Deze afspraken worden vastgelegd in convenanten. Daarna dienen de afspraken beoefend te worden.

Versterking van de civiel-militaire samenwerking
Voor de verdere professionalisering van de crisisorganisatie wordt intensievere samenwerking gezocht met Defensie als structurele veiligheidspartner. Hiertoe worden:
- Kansrijke mogelijkheden tot versterking van de civiel-militaire samenwerking geanalyseerd;
- Een catalogus civiel militaire samenwerking ontwikkeld;
- Een taskforce OTOTEL[35]Sim ingesteld om de samenwerking op het terrein van OTOTEL te versterken;
- Een Nationaal Trainingscentrum (NTC) CBRN gerealiseerd.

Versterken van de themagerichte aanpak
Realisatie hiervan door:
- Het ontwikkelen van producten voor grootschalige evacuaties in het project Grootschalige Evacuatie;
- Het versterken van de organisatorische voorbereiding op de 'nafase' met specifieke aandacht voor de opvang en zorg voor getroffenen en herstel en wederopbouw;
- Het versterken van de CBRN[36] –respons door de multidisciplinaire samenwerking bij CBRN te bevorderen en het versterken van (generieke) CBRN capaciteiten in het kader van het EU Actieplan[37].

Versterking samenwerking Reddingsbrigade Nederland en veiligheidsregio's
Verbeteren van deze samenwerking door afspraken te maken met de Reddingsbrigade Nederland over opbouw van de Regionale Voorziening Reddingsbrigades; dit zijn samenwerkingsverbanden van reddingsbrigades op de schaal van de veiligheidsregio's.

Bevorderen van de internationale samenwerking

35 De afkorting OTOTEL staat voor Opleiden, trainen, oefenen, testen, evalueren en leren
36 De afkorting CBRN staat voor chemische, biologische of radiologische/nucleaire stoffen
37 EU CBRN Action Plan, 24 juni 2009

Door onder andere te participeren in Europese activiteiten en bij te dragen aan EU mechanisme, NATO en bilateraal, de internationale samenwerking bevorderen.

D. Versterken van de informatievoorziening en crisiscommunicatie

Vanzelfsprekend behoort ook de informatievoorziening en crisiscommunicatie tot de basiselementen in het crisisbeheersingsstelsel. Doelstelling van een goed functionerende informatievoorziening is het realiseren van een kwalitatief hoogwaardige informatiepositie en informatie-uitwisseling tussen veiligheidspartners. Kwaliteitsverbetering van de crisiscommunicatie is gericht op een eenduidige communicatie over risico's, crises en handelingsperspectief. Het betreft communicatie voor en tijdens een crisis tussen overheid, burger en bedrijfsleven, waarbij aangesloten wordt op de informatiebehoefte van de samenleving. Om dit te bereiken heeft de NCTV sinds 2011 ingezet op onderstaande aspecten.

Streven naar uniformiteit

Om de uniformiteit in de informatievoorziening en crisiscommunicatie te bevorderen, heeft de minister van VenJ overleg met de besturen van de veiligheidsregio's. In deze overleggen gaat het over de wijze waarop kan worden geborgd dat alle veiligheidsregio's gebruik maken van dezelfde standaarden, zodat informatie zowel interregionaal als bovenregionaal kan worden uitgewisseld.

Beter alarmeren en informeren van de bevolking

Zorg dragen voor een modern alarmeringsstelsel opdat de bevolking tijdig en adequaat gealarmeerd en geïnformeerd kan worden bij rampen en crises. De implementatie van het alarmmiddel NL-Alert en het verhogen van het bereik van NL-Alert. Het verhogen van het bereik wil de NCTV realiseren door de verzending van NL-Alertberichten door de telecomoperators verplicht te stellen via de Telecomwet[38], afspraken te maken met toestelleveranciers en publiekscampagnes te voeren rondom de landelijke controleberichten.

Verbeteren van de risico- en crisiscommunicatie

Om de communicatie rondom risico's en gedurende een crisis te verbeteren heeft de NCTV zich in de periode 2011-2015 gericht op:

- Denk Vooruit Campagne uitvoeren om de zelfredzaamheid van de burger te vergroten
- Doorontwikkelen van crisiscommunicatiemiddelen als 0800-1351 en www.crisis.nl
- Oprichting van een Nationaal Kernteam Crisiscommunicatie (NKC)
- Inzetbaar maken van een bovenregionaal expertteam crisiscommunicatie voor ondersteuning van de veiligheidsregio's.

Versterken van de operationele en bestuurlijke informatievoorziening bij rampen en crises

Hiervoor wordt netcentrisch werken ingevoerd, ondersteund met een Landelijk Crisismanagement Systeem (LCMS).

Verbeteren van de noodcommunicatie

Verbetering van de noodcommunicatie door zorg te dragen voor een functionerend noodcommunicatiesysteem dat als last resortvoorziening voor de crisisorganisatie dient als geen gebruik gemaakt kan worden van de reguliere communicatiemiddelen. De NCTV stimuleert organisaties om aangesloten te zijn en brengt het belang ervan onder de aandacht, maar het is een eigen

38 Telecommunicatiewet, 1998

verantwoordelijkheid van de organisaties die een rol kunnen hebben in de crisisbeheersing om aangesloten te zijn op het noodcommunicatiesysteem.

E. Behoud historisch erfgoed

Als (gedelegeerd) stelselverantwoordelijke op het gebied van crisisbeheersing heeft de NCTV in de betreffende periode subsidie verstrekt voor de oprichting van het Nationaal Veiligheidsinstituut (NVI). Deze organisatie heeft een platformfunctie voor historisch erfgoed dat betrekking heeft op veiligheid en hulpverlening in Nederland. Het NVI heeft naast het behoud van erfgoed als doel om burgers meer risicobewust en weerbaar te maken. Het gewenste effect is dat de burger daardoor medeproducent van veiligheid wordt.

3.2.2 *Vergroten weerbaarheid van vitale belangen*

Om de Nederlandse nationale veiligheid te beschermen, richt de NCTV zich naast het aanpakken van dreigingen ook op het verhogen van de weerbaarheid.
De NCTV heeft zich hierbij met name gericht op versterken van de weerbaarheid van de vitale infrastructuur, de economische veiligheid en de weerbaarheid van het Rijk tegen spionage.

A. Versterken weerbaarheid ten behoeve van de nationale veiligheid

De continuïteit van vitale producten en diensten is cruciaal voor de nationale veiligheid. Bescherming van deze zogenoemde vitale infrastructuur is dan ook een doel, waar overheid en bedrijfsleven beide een belangrijke rol hebben.
Om dit te realiseren is in de periode 2011- 2015 ingezet op onderstaande aspecten.

Herijking van de interdepartementale strategie en het beleid over de bescherming van vitale infrastructuur

Onder regie van de Stuurgroep nationale veiligheid wordt de strategie nationale veiligheid geëvalueerd en doorontwikkeld, onder andere door het onderwerp vitaal integraler in de strategie op te nemen.

In publiek- private samenwerking ontwikkelen van 'roadmaps'

De NCTV stimuleert gezamenlijke ontwikkeling (door vakministeries en vitale partners) van roadmaps voor de optimalisering van de weerbaarheid van de als vitaal geïdentificeerde processen.

Stroomlijnen van de (overheids)inzet

Inzetten op het zoveel mogelijk samenbrengen van specifieke initiatieven en instrumenten, zoals het Alerteringssysteem Terrorismebestrijding (Atb)[39] en het maken van crisisafspraken, zodat samenwerking met vitale organisaties tijdens incidenten, rampen en crisis wordt versterkt.

Signalering van mogelijk nieuwe vitale processen

Er is een veelheid en diversiteit aan processen en objecten die vanuit verschillende invalshoeken (terrorisme, continuïteit, cyber en CBRN security) aandacht krijgen ten behoeve van het verhogen van hun weerbaarheid. In dit kader is nadere definiëring van het begrip 'vitale infrastructuur' nodig, evenals het aanbrengen van focus in de inspanningen van de NCTV om de vitale infrastructuur te beschermen. Door het aanbrengen van focus kunnen instrumenten zo effectief mogelijk worden ingezet.

39 Het Alerteringssysteem Terrorismebestrijding (ATb) is een Nederlands alerteringssysteem, bedoeld om in geval van nood of dreiging alle benodigde personen en diensten te kunnen waarschuwen. Het Alerteringssysteem Terrorismebestrijding is sinds 16 juni 2005 operationeel.

Aansluiting en opleiding vitale aanbieders op de nationale crisisbesluitvorming
Aanbieders van vitale producten en diensten aan laten sluiten op de nationale crisisbesluitvorming inclusief de deelname aan opleiden, trainen en oefenen.

B. Versterken economische veiligheid
Het is belangrijk dat er een juiste balans is tussen economische belangen en aspecten van nationale veiligheid. Aandacht voor potentiële risico's voor de nationale veiligheid bij veranderende geopolitieke machtsverhoudingen en bij economische beleidsafwegingen ten aanzien van vitale sectoren, is voor de NCTV dan ook van belang. Om hier invulling aan te geven heeft de NCTV zich in de periode 2011- 2015 gericht op instrumenten zoals hieronder uiteengezet.

Ex ante analyses van vitale sectoren
Beoordelen van het huidige overheidsinstrumentarium (de weerstand) voor het beschermen van de nationale veiligheid bij buitenlandse investeringen in de als vitaal aan te merken sectoren.

Verkenning van het bredere thema economische veiligheid voor concrete beleidstoepassing
Beleidsontwikkeling op het gebied van economische veiligheid, met hierbij geprioriteerde deelonderwerpen: buitenlandse investeringen in vitale sectoren, beperkte toegang tot grondstoffen/ bescherming handelsroutes en (digitale) spionage.

C. Verhogen weerbaarheid Rijk tegen spionage
Spionage is een thema met politieke prioriteit vanwege het afbreukrisico. Om de weerbaarheid tegen spionage te verhogen heeft de NCTV in de periode 2011-2015 ingezet op de volgende instrumenten.

Uitvoeren zelfanalyse Spionage en monitoring implementatie aanbevelingen
Het uitvoeren van een zelfevaluatie van de Rijksoverheid naar de gevoeligheid van kernbelangen voor spionage en de implementatie van de aanbevelingen hieruit. Tevens onderzoek van de rijksinspecties naar de mate waarin aanbevelingen uit de evaluatie zijn doorgevoerd.

3.3 Instrumenten cybersecurity gericht op 4 doelstellingen uit de nationale cybersecurity strategieën

Zoals beschreven in hoofdstuk 2 zijn de Nationale Cybersecurity strategieën richtinggevend geweest voor de door de NCTV ingezette instrumenten in het kader van cybersecurity. Hierin zijn de volgende doelstellingen/ actielijnen gekozen:

1. Nederland zorgt voor een integrale aanpak van cybersecurity door publieke en private partijen;
2. Nederland zorgt voor adequate en actuele dreiging- en risicoanalyses;
3. Nederland versterkt de weerbaarheid tegen ICT-verstoringen en cyberaanvallen;
4. Nederland versterkt responscapaciteit om ICT-verstoringen en cyberaanvallen te pareren;
5. *Nederland intensiveert opsporing en vervolging van cybercrime;*
6. *Nederland stimuleert onderzoek en onderwijs.*

De eerste vier doelstellingen vormen de basis voor de uitwerking van de beleidstheorie van de NCTV voor deze beleidsdoorlichting.
Opsporing en vervolging van cybercrime behoort niet tot het taakveld van de NCTV en t maakt geen deel uit van artikel 36.2 van de begroting van het ministerie van VenJ. De laatste actielijn is gericht op stimuleren van onderzoek

en onderwijs. Dit aspect hebben wij geplaatst onder versterken van de weerbaarheid.

Hieronder worden per beleidsdoelstelling de beleidsinstrumenten uiteengezet.
N.B.: Voor een gedetailleerd en volledig overzicht van alle ingezette beleidsinstrumenten in het kader van het cybersecurity beleid verwijzen wij naar bijlage 4.

3.3.1 *Versterken integrale aanpak cybersecurity door publieke en private partijen*

De zorg voor digitale veiligheid is in Nederland belegd bij veel verschillende partijen. (Operationele) samenwerking, samenhang tussen het geheel van goede beleidsinitiatieven en voorlichting is belangrijk.

A. Duidelijke verdeling van taken, verantwoordelijkheden en bevoegdheden

Met een duidelijkere rolverdeling kunnen doublures worden verwijderd en initiatieven worden gebundeld. In de periode 2011 -2015 heeft de NCTV hiervoor ingezet op:

Oprichten van Cyber Security Raad

Oprichten van een Cyber Security Raad, waarin op strategisch niveau vertegenwoordigers van alle relevante partijen zitting hebben en waarin afspraken worden gemaakt over uitvoering en uitwerking van deze strategie. De Raad geeft gevraagd en ongevraagd advies aan het kabinet en heeft daarnaast als taak het toezien op de uitvoering van de Nationale Cyber Security Strategie.

Oprichten en versterken Nationaal Cyber Security Centrum

Wens van het kabinet is dat publieke en private partijen, op basis van hun eigen taken en binnen de wettelijke mogelijkheden, informatie, kennis en expertise in een op te richten Nationaal Cyber Security Centrum bij elkaar brengen, zodat inzicht kan worden verkregen in ontwikkelingen, dreigingen en trends, en ondersteuning kan worden geboden bij incidentafhandeling en crisisbesluitvorming. Het kabinet zal het huidige GOVCERT.NL uitbreiden, versterken en inbrengen in dit Centrum. GOVCERT.NL richt zich op versterking van de informatiebeveiliging binnen de Nederlandse overheid en doet dat door het monitoren van bronnen via internet, het uitgeven van adviezen over ICT-kwetsbaarheden en waarschuwingen bij dreigingen en door ondersteuning te bieden aan overheidsorganisaties bij de afhandeling van ICT-gerelateerde incidenten. De positie van het NCSC wordt verstevigd door een versterkte structuur te bieden voor vertrouwde informatiedeling en -analyse en door in te zetten op een rol als kennisautoriteit. Het NCSC geeft vanuit deze expertrol gevraagd en ongevraagd advies aan aangesloten private en publieke partijen. Ten slotte verbreedt het NCSC zich op basis van de eigen detectiecapaciteit en de triagerol bij crises ook naar een Nationaal Cyber Security Operations Center (CSOC)3, naast zijn rol van Computer Emergency Respons Team (CERT).

B. Bouwen aan coalities voor vrijheid, veiligheid en vrede in het digitale domein

Het beschermen van fundamentele rechten en waarden vergt inzet van vele partijen en dient in (inter)nationaal verband te gebeuren. De aanpak die wordt voorgestaan, is het ontwikkelen van internationale normen en standaarden. Naast overheden is hier een belangrijke rol weggelegd voor partijen uit de private sector en maatschappelijke organisaties.

Versterkt participeren in multistakeholder evenementen (Cyberspace conferenties en het IGF)
Of het nu gaat om standaarden in ICT, fundamentele rechten, de bestrijding van cybercrime of het bevorderen van de internationale rechtsorde in cyberspace, een internationale beleidsagenda is een belangrijk onderdeel van een geïntegreerd nationaal cybersecuritybeleid.
De internationale visie van de Nationale Cyber Security Strategie 2 gaat uit van een geïntegreerde aanpak van veiligheid, waarin naast het belang van defence en development, in de vorm van capaciteitsopbouw, ook middels diplomacy wordt bijgedragen aan meer stabiliteit in het cyberdomein.

De NCTV neemt deel verschillende internationale werkgroepen en heeft (samen met BZ) het Global Forum on Cyber Expertise (GFCE) gerealiseerd.

3.3.2 *Nederland zorgt voor adequate en actuele dreiging- en risicoanalyses*

Het versterken van de veiligheid begint met inzicht in kwetsbaarheden en dreigingen. Door kennis en informatie van (inter)nationale publieke en private organisaties bij elkaar te brengen en te analyseren, ontstaat een beter inzicht in actuele en mogelijke nieuwe kwetsbaarheden en dreigingen. Hierbij wordt aangesloten bij de werkwijze van de strategie nationale veiligheid; dat wil zeggen: risico's in kaart brengen en capaciteiten identificeren die versterkt moeten worden om dreigingen te voorkomen en op verstoringen te kunnen reageren. Met deze kennis kunnen alle doelgroepen maatregelen treffen in de gehele keten van preventie tot respons en opsporing en vervolging. Voor de periode 2012 -2015 heeft de NCTV zich gericht op het realiseren van de onderstaande doelstellingen en beleidsinstrumenten:

A. Gezamenlijk integraal beeld van actuele dreigingen en kwetsbaarheden ICT

De NCSC heeft sinds haar oprichting ingezet op de verschillende activiteiten om te zorgen voor een integraal en actueel beeld van dreigingen en kwetsbaarheden ICT. Deze activiteiten zijn hieronder toegelicht.

Risico's in kaart brengen van legacy systemen in vitale processen en diensten
Legacy systemen zijn systemen die zijn gebouwd met technologie die niet of nauwelijks meer wordt ondersteund door externe leveranciers en/of de eigen organisatie. Qua beschikbaarheid, integriteit en vertrouwelijkheid zijn legacysystemen in vergelijking met modernere systemen kwetsbaarder en daarmee onveiliger. Als het gaat om systemen bij organisaties in vitale sectoren kan deze kwetsbaarheid grote gevolgen hebben, zowel voor de eigen organisatie als voor de maatschappij. Het is dan ook van belang dat organisaties zich bewust zijn van deze relatieve onveiligheid en dat deze organisaties weten bij welke systemen dergelijke onveiligheden zich voordoen en om welke specifieke onveiligheden het gaat. Maar ook dat zij beschikken over strategieën voor het wegnemen of verkleinen van de risico's. Om organisaties hierbij te helpen is ingezet op de ontwikkeling van een self-assessment.

Coördineren, faciliteren, samenvoegen en delen dreigings- en risicoanalyses
Naast het in kaart brengen van risico's is het vergaren van inzichten binnen het cyberdomein vanuit andere partijen een belangrijke taak. Daarom heeft de NCSC ook een coördinerende en faciliterende rol om informatie te verkrijgen voor een integraal dreigingsbeeld. De AIVD en de MIVD brengen kennis in ten behoeve van dit beeld, maar ook private partijen doen dat. Deze inspanningen vinden hun weerslag in het Cybersecurity Beeld Nederland (CSBN).

B. Versterken van onderzoeks- en analysecapaciteit

De dreiging en risicoanalyses konden ook adequater en actueler worden gemaakt door te investeren in onderzoeks- en analysecapaciteit. Hiervoor zette de NCTV in op verschillende instrumenten die hierna worden toegelicht.

NCSC uitbreiden met meer analisten en inventariseren van samenwerkingsmogelijkheden

NCSC heeft ingezet op de inzet van meer analisten en het verder verkennen en uitwerken van de samenwerkingsmogelijkheden met de inlichtingendiensten. Dit om de onderzoeks- en analysecapaciteit te vergroten.

Oprichten nationaal detectie- en responsnetwerk

Inzet van NCSC om in samenwerking met haar partners een nationaal detectie- en responsnetwerk op te richten voor de Rijksoverheid en overige vitale sectoren. Met deze netwerken wordt, omkleed met waarborgen op het gebied van onder meer vertrouwelijkheid en privacy, toegewerkt naar het real-time analyseren en delen van dreigingsinformatie. Het detectie en responsnetwerk is voor de Rijksoverheid en overige vitale sectoren.

3.3.3 *Versterken weerbaarheid tegen ICT-verstoringen en cyberaanvallen*

Maatschappelijke ontwrichting door ICT-verstoringen of cyberaanvallen moet worden voorkomen. Verschillende partijen hebben daarbij een verantwoordelijkheid, van burger tot leverancier. De gebruiker moet erop kunnen vertrouwen dat een ICT-product of –dienst veilig gebruikt kan worden. De leverancier moet daarom een voldoende veilig ICT-product of -dienst aanbieden. De gebruiker moet ook zelf de nodige veiligheidsmaatregelen treffen. Om de weerbaarheid te vergroten, heeft de NCSC zich in de periode 2011 -2015 gericht op verschillende subdoelen die in de volgende subparagrafen zijn uitgewerkt.

A. Vergroten en ontwikkelen van cybersecurity experts

Goede scholing op alle niveaus is noodzakelijk om betrouwbare ICT te kunnen blijven maken en weerstand te kunnen blijven bieden aan dreigingen. Versterking van scholing op alle niveaus is noodzakelijk om weerstand te kunnen blijven bieden aan dreigingen en betrouwbare ICT te kunnen blijven maken en is een voorwaarde voor de groei van de digitale economie in Nederland.

Ontwikkelplan gericht op kwalificering en certificering

Voor de beroepsgroepen en het onderwijsveld wordt een plan ontwikkeld voor het uitbreiden van het aandeel van ICT-veiligheid in de daarvoor geschikte opleidingen. Ook wordt voortgebouwd op een onderzoek naar de mogelijkheden van certificering en kwalificering van informatiebeveiliging professionals.

Oprichten PPS taskforce Cybersecurity

In de tweede Cybersecurity strategie is als actie opgenomen om een PPS taskforce Cybersecurity in te stellen, die zich richt op advisering van het cybersecurity onderwijsaanbod.

B. Stimuleren van onderzoek op het vlak van cybersecurtity

Wetenschappelijk en toegepast onderzoek en het stimuleren van de ontwikkeling van innovatieve veiligheidsoplossingen zijn een aanjager voor cybersecurity. Voor het stimuleren van onderzoek heeft de NCSC in de periode 2011 -2015 op onderstaande ingezet.

Afstemmen onderzoeksprogramma's via de research cyber security agenda

Het kabinet zal onderzoeksprogramma's van in ieder geval de overheid en waar mogelijk van wetenschappelijke onderzoekscentra en het bedrijfsleven beter op

elkaar afstemmen in de Nationale Cyber Security Raad. Hieruit volgt de research cyber security agenda.

Ondersteunen bij aanboren onderzoeksgelden
De overheid gaat de genoemde partijen nog actiever dan nu begeleiden bij het aanboren van multiplicerende onderzoeksgelden bij bijv. Europese en Euregionale fondsen.

Lanceren van cybersecurity platform
Lanceren van cybersecurity platform voor nieuwe en gevestigde bedrijven, studenten en onderzoekers.

C. *Vergroten kennis over en veiligheidsbewustzijn van ICT-producten en diensten bij de gebruikers (burgers en bedrijven)*

De overheid zet in op het vergroten van de digitale weerbaarheid van overheid, burgers en bedrijfsleven. Dit vereist dat burgers en bedrijven over een basiskennisniveau beschikken van de veiligheid van ICT-producten en -diensten. De NCTV wil dit ten eerste bereiken door informatie over veiligheid van ICT-producten en -diensten bij de gebruiker beter beschikbaar te maken. Als tweede instrument is ingezet op de gezamenlijke (overheid en leveranciers) ontwikkeling van doelgerichte, nationale en actuele campagnes voor burgers, gebruikers en overheid. Daartoe is geïnvesteerd in de campagne in het kader van Alert online en de website www.veiliginternetten.nl.

D. *Bewerkstelligen dat publieke en private leveranciers voldoen aan minimumeisen op het gebied van continuïteitsdienstverlening en spionage*

Maatschappelijke ontwrichting door ICT-verstoringen of cyberaanvallen moet worden voorkomen. De gebruiker moet erop kunnen vertrouwen dat een ICT-product of –dienst veilig gebruikt kan worden. De leverancier moet daarom een voldoende veilig ICT-product of -dienst aanbieden. De gebruiker moet ook zelf de nodige veiligheidsmaatregelen treffen.

Stimuleren minimale ICT beveiligingsstandaarden op basis van good practices
De overheid gaat samen met de vitale organisaties het gebruik van de gangbare minimale ICT beveiligingsstandaarden op basis van good practices stimuleren. Het kabinet werkt met vitale sectoren aan het verkrijgen van inzicht in mogelijke maatregelen tegen verstoring van hun vitale ICT-voorzieningen. Op basis hiervan dringt de overheid er bij vitale sectoren op aan om de geïdentificeerde maatregelen ook te treffen.

Beschikbaar stellen handleiding Kwetsbaarhedenanalyse Spionage
Specifiek ter voorkoming van (digitale) spionage heeft het kabinet een maatregelenpakket ontwikkeld. Voor bedrijven is er een handleiding Kwetsbaarhedenanalyse Spionage beschikbaar waarmee zij hun weerbaarheid tegen spionage kunnen vergroten.

Inzetten voor internationale afspraken over veilige hard- en software en zorgen dat Nederland actief deelneemt in het Internet Governance Forum
Het kabinet wil in overleg met de ICT-leveranciers zoeken naar mogelijkheden om de veiligheid van hard- en software te verbeteren en zet zich ervoor in om ook op internationaal niveau afspraken te maken over veilige hard- en software. Daarnaast neemt Nederland actief deel in het Internet Governance Forum dat door de Verenigde Naties wordt gefaciliteerd. Doel hiervan is om een actieve rol te spelen om in de mondiale context van een open en transparante dialoog onderwerpen aan te snijden die kunnen bijdragen aan deze strategie, zoals de spelregels op het internet te verbeteren en misbruik tegen te gaan.

Haalbaarheidsonderzoek gescheiden netwerk vitaal
Er wordt een verkenning uitgevoerd in hoeverre het realiseren van een gescheiden ICT-netwerk voor (publieke en private) vitale processen op technisch en organisatorisch vlak mogelijk en wenselijk is. Met een gescheiden netwerk nemen de mogelijkheden om de continuïteit van vitale processen te borgen toe. Ook kunnen binnen het gescheiden netwerk eigen dataopslag of een cloud worden ontwikkeld. Hierdoor kan de privacy/integriteit van de data in deze opslag of cloud worden verbeterd.

3.3.4 ***Versterken responscapaciteit om ICT-verstoringen en cyberaanvallen te pareren***

Om adequaat te kunnen reageren op verschillende dreigingen en om bij een verstoring of aanval terug te kunnen keren naar een stabiele situatie zijn verschillende responsactiviteiten nodig. ICT-incidenten die leiden tot een inbreuk op de beschikbaarheid, integriteit of exclusiviteit van de netwerk- en informatie-infrastructuur pakt de betreffende organisatie in eerste instantie zelf aan. Daar waar incidenten kunnen leiden tot maatschappelijke ontwrichting of aantasting van vitale objecten, processen of personen, zal de overheid adequaat reageren.

A. Zorgen voor een duidelijke crisisstructuur bij cyberincidenten

Om te zorgen voor een duidelijke crisisstructuur voor cyberincidenten heeft de NCSC in de periode van de beleidsdoorlichting ingezet op verschillende activiteiten. Deze zijn hieronder nader toegelicht.

Opstellen Nationaal Crisisplan ICT
Het kabinet levert in de zomer van 2011 het Nationaal Crisisplan ICT op. Onderdeel hiervan is een oefenplan, dat zowel nationale als internationale oefeningen op elkaar afstemt.

ICT Response Board onderbrengen bij NCSC
De ICT Response Board (IRB), een publiek-private samenwerking die de crisisbesluitvormingsorganisaties advies geeft over maatregelen om grootschalige ICT-verstoring tegen te gaan of te bestrijden, wordt in 2011 geoperationaliseerd en als functie ondergebracht in het Nationaal Cyber Security Centrum.

Versterken internationale samenwerking CERT-organisaties
Internationaal wordt ingezet op de versterking van de samenwerking bij de operationele respons tussen de CERT-organisaties in Europa en wordt gestreefd naar versterking van het International Watch and Warning Network (IWWN), dat nu als informeel mondiaal operationeel overleg fungeert bij ICT-incidenten.

Inventarisatie en accreditatie van bedrijven als digitale brandweer
Het gaat hierbij om cybersecuritydienstverleners die andere partijen kunnen bijstaan bij digitale incidenten. Dit naast de eigen verantwoordelijkheid van partijen en de rol die het NCSC heeft als CERT voor de Rijksoverheid en de vitale infrastructuur.

B. Informeren van de burger en bedrijven bij cyberincidenten

De maatschappelijke impact van een grootschalige terroristische aanval op of via het internet kan groot zijn. De NCTV heeft daarom ingezet op uitbreiding van het Alerteringsysteem Terrorismebestrijding (ATb) en cyber component en beoefent deze uitbreiding. Ook wordt informatie verspreid via de website veiliginternetten.nl.

C. Stimuleren van kennis(deling) en oefening

Door kennisdeling en oefenen van cyberscenario's is Nederland beter in staat te reageren op cyberincidenten. De NCSC levert een bijdrage aan een trainingsprogramma voor respons op grootschalige ICT-incidenten.
De NCSC wil ook grote en kleine oefeningen organiseren en daar zelf aan deelnemen.

3.4 Hoogte en onderbouwing uitgaven ten behoeve van het beleid

In deze paragraaf geven wij antwoord op de RPE vragen 5 en 6; wij gaan in op de uitgaven die met het beleid op het gebied van nationale veiligheid en crisisbeheersing, terrorismebestrijding en cyber security gepaard gaan en wat de onderbouwing is van deze uitgaven. Vervolgens beschrijven wij hoe de uitgaven zijn te relateren aan de ingezette beleidsinstrumenten.

Eerst geven wij een overzicht van de uitgaven over de periode van de beleidsdoorlichting. Daarna volgt een korte toelichting op deze uitgaven en tenslotte gaan wij in op in hoeverre de uitgaven te relateren zijn aan de beleidsinstrumenten.

3.4.1 *Overzicht uitgaven*

Wij kunnen enkel een overzicht geven van de uitgaven vanaf 2013. Voor het jaar 2012 zijn de uitgaven niet meer duidelijk te achterhalen, omdat de programma uitgaven voorheen ongespecificeerd onderdeel uit maakten van diverse begrotingsartikelonderdelen. De NCTV is immers opgericht uit een samenvoeging van de NCTb, directie Nationale Veiligheid en Govcert. Ook werd de overgang naar 'Verantwoord Begroten' pas vanaf de begroting 2013 zichtbaar. De NCTV is dus pas sinds 2013 als geheel zichtbaar in de begroting van het Ministerie van VenJ.

Programma uitgaven

De eerste tabel geeft inzicht in de realisatie van de programma uitgaven.

Tabel 1 Totaal realisatie programma uitgaven (x €1.000) [40]

	2013	2014	2015
Programma uitgaven	**196.333**	**245.945**	**247.430**
Bijdragen aan medeoverheden			
Brede Doeluitkering rampenbestrijding (BDUR)	128.461	177.293	176.097
Overige Nationale Veiligheid en terrorismebestrijding	9.529	6.275	11.520
Bijdragen ZBO/RWT			
IFV (Instituut Fysieke Veiligheid)	34.441	31.045	30.736
Opdrachten			
Project NL-Alert	3.254	6.284	6.702
Opdrachten NCSC	4.489	4.123	2.743
Overig terrorisme bestrijding	1.469	1.066	685
Overig Nationale Veiligheid	8.774	13.724	11.964
Subsidies			
Nationaal Veiligheidsinstituut	934	2.053	1.340
Nederlands Rode Kruis	1.827	1.786	1.611
Onderwijs Veiligheidregio's	250	0	0
Overige Nationale Veiligheid en terrorismebestrijding	2.905	2.296	4.032
Bijdrage agentschappen			
Overig bijdragen Agentschappen	0	0	0

Tabel 1 laat zien dat een overgroot deel van de uitgaven bestaat uit de BDUR. De BDUR is vanaf 2014 structureel verhoogd met € 65,7 miljoen. Deze verhoging komt voort uit het feit dat de veiligheidsregio's, in tegenstelling tot de gemeenten, geen gebruik kunnen maken van het btw-compensatiefonds.

40 Bron: Meerjarig uitgavenkaderoverzicht: overzicht met goedgekeurde IBOS uitgavenmutaties vanaf 2007 is bijgewerkt tot en met de stand ontwerpbegroting 2017, DFEZ

Apparaatsuitgaven
Onderstaande tabel geeft inzicht in de gerealiseerde apparaatsuitgaven[41].

Tabel 2 Realisatie apparaatsuitgaven (x €1.000) [42]

	2013	2014	2015
Eigen personeel	24.550	25.723	29.659
Externe inhuur	4.053	3.783	3.596
Materieel ICT	1.815	755	1.131
Materieel SSO's	2.555	769	1.191
Materieel overig	2.152	3.087	2.425
Totaal Apparaat	**35.125**	**34.117**	**38.002**

Versterkingsgelden veiligheidsketen vallen buiten de scope van deze doorlichting
Met het oog op het verwachte langdurige karakter van het huidige dreigingsbeeld, heeft het kabinet in februari 2015 besloten de veiligheidsketen op een aantal punten substantieel te versterken. Het gaat om een pakket van in totaal € 128,8 mln. structureel, dat in een oplopende reeks wordt gerealiseerd. Hiermee kunnen de betrokken diensten en organisaties, bij voortzetting van het huidige dreigingsbeeld, ook de komende jaren doen wat nodig is om de jihadistische dreiging tegen te gaan[43]. Delen van dit budget zijn bij de Voorjaarsnota 2015 aan de betrokken organisaties ter beschikking gesteld; het resterende budget is vanaf 1 januari 2016 beschikbaar gekomen. Slechts een zeer beperkt deel van deze versterking heeft betrekking op begrotingsartikel 36.2. Dit neemt niet weg dat de NCTV de coördinerende organisatie is voor de aanpak van terrorisme in Nederland. Daarnaast is een groot deel van deze versterkingsgelden beschikbaar gekomen in 2016. De hiermee gefinancierde middelen en instrumenten ten behoeve van de bestrijding van terrorisme vallen dus buiten de scope van deze beleidsdoorlichting.

3.4.2 *Toelichting op de gefinancierde instrumenten*

Brede Doeluitkering Rampenbestrijding (BDuR)
De BDuR is een lumpsumbijdrage die wordt verstrekt aan de 25 veiligheidsregio's, regionale samenwerkingsverbanden van brandweer en GHOR, voor de uitvoering van wettelijke taken. Naast deze rijksbijdrage, die ongeveer 10 procent van het totaal behelst, ontvangen de veiligheidsregio's een bijdrage van de gemeenten.

Bijdrage Instituut Fysieke Veiligheid (IFV)
Het IFV verricht taken op het terrein van brandweer, GHOR, rampenbestrijding en crisisbeheersing. De bijdrage is een lumpsum bijdrage en wordt toegekend op grond van artikel 2 van het Besluit rijksbijdragen IFV. Los van de bijdragen van VenJ voor wettelijke taken verricht het IFV tevens op commerciële basis werkzaamheden voor derden, zoals bedrijven, ministeries en gemeenten (ook wel aangeduid als: wettelijk toegestane werkzaamheden).

Project NL-Alert
NL-Alert is het systeem voor rampen- en crisisinformatie per mobiele telefoon. De overheid alarmeert en informeert met dit systeem mensen in de omgeving van een bepaalde zendmast via een bericht op hun mobiele telefoon over een acute crisis. Het Ministerie van VenJ financiert de jaarlijkse beheer- en exploitatiekosten voor dit systeem van onder andere de telecomproviders.

41 Deze apparaatsuitgaven NCTV zijn in de begroting niet opgenomen onder artikel 36.2 maar onder artikel 91
42 Bron: Exceloverzicht Apparaat, NCTV, 7 november 2016
43 Kamerbrief Versterking Veiligheidsketen, ref. 3807309, d.d. 27 februari 2015

Nationaal Cyber Security Centrum (NCSC)
Het NCSC is het centrum in Nederland waar publieke (onder andere het Ministerie van Defensie) en private partijen, wetenschap en onderzoeks-instellingen operationele informatie bijeen brengen rondom cyber security. Daarnaast treedt het NCSC op als Computer Emergency Response Team (CERT) namens de Nederlandse overheid en fungeert in deze hoedanigheid als Nationaal Contactpunt voor cyber security, die meldingen verwerkt en trends en ontwikkelingen op internet waarneemt. Periodiek wordt het Cyber Security Beeld Nederland opgesteld, op basis waarvan beleidsvorming plaatsvindt op het gebied van cyber security.

Subsidie Nationaal Veiligheidsinstituut
Het Nationaal Veiligheidsinstituut ontvangt subsidie om een landelijk expositiecentrum op het terrein van veiligheid te beheren. Deze begrotingsvermelding vormt de wettelijke grondslag voor de hier bedoelde subsidieverlening als bedoeld in artikel 4:23, derde lid, onder c, van de Algemene wet bestuursrecht.

Subsidie Nederlands Rode Kruis
Het Nederlandse Rode Kruis start levensreddende activiteiten bij rampen en conflicten door het bieden van onderdak, voedsel, drinkwater en medische voorzieningen. Jaarlijks ontvangt het Nederlandse Rode Kruis een subsidie van het Ministerie van VenJ voor de inzet bij rampen en crises in Nederland. Deze subsidie wordt toegekend op grond van artikel 8 van het Besluit Rode Kruis.

Subsidies overige Nationale Veiligheid en terrorismebestrijding
Onder dit instrument vallen de subsidies die worden verstrekt met het doel de aantasting van de nationale veiligheid te voorkomen en crisisbeheersing te verbeteren. Onder meer worden in dit kader projecten gefinancierd die het presterend vermogen van veiligheidspartners verhogen door slimmer, sneller en/of efficiënter te gaan werken. Het gaat om incidentele subsidies die worden verstrekt op grond van artikel 48 lid r van de Wet Justitiesubsidies.

3.4.3 *Merendeel beleidsinstrumenten niet te relateren aan specifieke uitgaven*

Enkele in dit hoofdstuk gepresenteerde beleidsinstrumenten zijn direct te koppelen aan de daarvoor gelabelde programma uitgaven. Zoals bijvoorbeeld de BDuR, bijdrage aan het IFV en het NCSC, subsidies aan het Rode Kruis en het Nationaal Veiligheidsinstituut en geld voor het project NL Alert.
Het overgrote deel van de ingezette beleidsinstrumenten is niet direct te koppelen aan gelabelde uitgaven. Het betreft instrumenten waarbij de realisatie ervan vooral afhankelijk is van de inzet medewerkers van de NCTV.
Op het niveau van beleidsinstrumenten is nu niet inzichtelijk hoeveel tijd medewerkers aan instrumenten hebben besteed. Aparte kostprijzen voor het merendeel van de ingezette beleidsinstrumenten kan dan ook niet worden berekend. Indien dit inzicht gewenst is, zal een bijvoorbeeld een tijdsregistratie nodig zijn. Op deze wijze kan middels de tijdsbesteding de kosten van een instrument worden berekend. Dit kan de NCTV helpen om een reëler beeld te krijgen van de totale kosten, die met de inzet van een beleidsinstrument gemoeid zijn.

4 Doeltreffendheid en doelmatigheid van het gevoerde beleid

Dit hoofdstuk bevat een overzicht van het beschikbare onderzoek naar doeltreffendheid en doelmatigheid en de mate waarin dit dekkend is voor het beleidsterrein van de NCTV. Daarmee geeft dit hoofdstuk antwoord op de volgende vragen van de RPE:

8. Welke evaluaties (met bronvermelding) zijn uitgevoerd, op welke manier is het beleid geëvalueerd en om welke redenen?
9. Welke beleidsonderdelen zijn (nog) niet geëvalueerd? Inclusief uitleg over de (on)mogelijkheid om de doeltreffendheid en doelmatigheid van het beleid in de toekomst te evalueren.
10. In hoeverre maakt het beschikbare onderzoeksmateriaal uitspraken over de doeltreffendheid en doelmatigheid van het beleidsterrein mogelijk?

Ook bevat dit laatste hoofdstuk bevindingen ten aanzien van de doeltreffendheid en doelmatigheid van het gevoerde beleid en gaat dit hoofdstuk in op de volgende vragen van de RPE:

11. Welke effecten heeft het beleid gehad? Zijn er positieve en/of negatieve neveneffecten?
12. Hoe doeltreffend is het beleid geweest?
13. Hoe doelmatig is het beleid geweest?

Hierna presenteren wij de bevindingen over de doeltreffendheid en doelmatigheid van het gevoerde beleid per taakveld. Hierbij staat wat de NCTV vanuit haar coördinerende functie bij haar publieke en private partners wil bereiken centraal.

4.1 Doeltreffendheid en doelmatigheid beleid contraterrorisme

In deze paragraaf gaan wij eerst in op de evaluaties die zijn uitgevoerd op dit taakdomein. Daarna beschrijven we de implementatie van de instrumenten. Vervolgens zetten wij, op basis van de beschikbare evaluatie-onderzoeken, uiteen in hoeverre het plausibel is dat er een relatie bestaat tussen de doelstellingen en de ingezette beleidsinstrumenten. Daarbij gaan wij ook in op de rolinvulling van de NCTV. Tot slot zullen wij inzicht geven in wat bekend is over de doelmatigheid van het gevoerde beleid.

4.1.1 *Enkele veelomvattende evaluaties uitgevoerd op het terrein van contraterrorisme*

In de afgelopen jaren zijn een aantal onderzoeken verschenen op het terrein van terrorismebestrijding. De meest veelomvattende onderzoeken daarbij zijn de Evaluatie CT strategie 2011 -2015[44], de Evaluatie van het Stelsel Bewaken en Beveiligen[45] en de Evaluatie van het Actieprogramma Integrale Aanpak Jihadisme[46]. De enkele overige onderzoeken zijn evaluaties en onderzoeken van afzonderlijke aspecten van terrorismebestrijding.

Om inzicht te geven in de effectiviteit van het beleid dat de NCTV heeft gevoerd op het gebied van contraterrorisme geven wij in bijlage 5 een overzicht van de

44 Evaluatie CT strategie 2011 -2015: Gericht, gedragen en geborgd interventievermogen?, USBO Advies, 8 april 2016
45 Evaluatie Stelsel Bewaken en Beveiligen, Inspectie VenJ, 2014
46 Evaluatie van het Actieprogramma Integrale Aanpak Jihadisme, Inspectie Veiligheid en Justitie, 2017

ingezette beleidsinstrumenten over de periode 2011-2015. Daarbij geven wij inzicht in de realisatie en werkbaarheid van de instrumenten. Met werkbaarheid wordt bedoeld of instrumenten ook worden toegepast in de praktijk. Ook geeft de bijlage inzicht of de instrumenten zijn geëvalueerd en in hoeverre uitspraken zijn gedaan over doeltreffendheid en doelmatigheid van de instrumenten.

4.1.2 *Merendeel van de beleidsinstrumenten op het gebied van contraterrorisme geïmplementeerd*

Zoals in bijlage 5 is te zien hebben wij vastgesteld of geplande instrumenten ook zijn gerealiseerd. Uit onze analyse komt naar voren dat de NCTV het merendeel van de instrumenten heeft gerealiseerd. Alleen de realisatie van geïnitieerde wetgevingstrajecten heeft meestal pas plaatsgevonden na de periode van de doorlichting. Wel zijn de werkzaamheden ter voorbereiding op deze wetgeving uitgevoerd in de periode 2011-2015.

In de onlangs gepubliceerde Evaluatie van het Actieprogramma Integrale Aanpak Jihadisme van de Inspectie VenJ komt naar voren dat het grootste deel van de gemeenten bekend zijn met de meeste maatregelen uit het actieprogramma waar het de lokale aanpak betreft. De Evaluatie van de Inspectie VenJ geeft aan dat over het algemeen de preventieve maatregelen vaker worden ingezet dan de repressieve maatregelen. Dit laatste is verklaarbaar, omdat repressieve maatregelen meer afhankelijk zijn van de aanwezige casuïstiek[47].

4.1.3 *Uitspraken doeltreffendheid specifieke beleidsinstrumenten niet mogelijk maar relatie tussen CT-beleid en gewenste effecten is plausibel*

Uitspraken over de doeltreffendheid van specifieke beleidsinstrumenten is niet mogelijk. De evaluatie van de CT-strategie stelt: 'De effecten van contraterrorismebeleid zijn niet rechtstreeks te evalueren. De gevolgen van maatregelen zijn bijzonder moeilijk vast te stellen, omdat de ogenschijnlijke effecten van het beleid ook door andere oorzaken tot stand kunnen zijn gekomen. De strategie is daarbij een integrale aanpak van contraterrorisme; partners zetten instrumenten gecombineerd en tegelijkertijd in. Het is daarmee lastig om een effect (zoals het niet-uitreizen naar Syrië) toe te wijzen aan één specifieke maatregel (bijvoorbeeld het intrekken van een paspoort).
De context van de strategie wordt daarmee gekenmerkt door complexiteit:de ontwikkelingen zijn onvoorspelbaar, een onbegrensde groep van partners binnen en buiten de overheid is betrokken bij de uitvoering van de strategie en er zijn weinig breed ondersteunde wetenschappelijke bevindingen om het beleid aan te toetsen.^De evaluatie van de CT strategie heeft zich daarom gericht op het gezamenlijke interventievermogen; de gedeelde capaciteit van de betrokken organisaties om een doelgerichte, legitieme en robuuste bijdrage te leveren aan de doelen van de strategie'.[48]

Zoals in hoofdstuk drie is opgenomen, heeft de NCTV met name ingezet op een integrale aanpak. Hierbij heeft de NCTV zich gericht op het equiperen en ondersteunen van de betrokken partners, zowel op lokaal, nationaal en internationaal niveau door vanuit een coördinerende rol te investeren op de onderlinge samenwerking, een versterking van de informatie-uitwisseling en kennisdeling, verruiming van de mogelijkheden om (potentiële) terroristen en extremisten aan te pakken én de advisering omtrent signalering en interventies.

De evaluatie van de CT-strategie beschrijft dat de keuze voor een integrale lokale aanpak valide is en het interventievermogen in potentie kan versterken. De evaluatie stelt: 'de aannames binnen de strategie over integrale

47 Evaluatie van het Actieprogramma Integrale Aanpak Jihadisme, Inspectie Veiligheid en Justitie, 2017
48 Evaluatie CT strategie 2011 -2015: Gericht, gedragen en geborgd interventievermogen?, USBO Advies, 8 april 2016, blz. 5

samenwerking kunnen volgens de literatuur in eerste instantie leiden tot een krachtig interventievermogen. De samenwerking tussen verschillende partijen maakt het mogelijk ongetemde problemen als radicalisering en terrorisme van veel kanten te benaderen. Zo ondersteunt de literatuur in grote lijnen de aanname dat met verbindingen met de lokale gemeenschap radicalisering vroegtijdig gesignaleerd kan worden, en ook de voedingsbodem kan worden aangepakt[49].

Tevens blijkt uit de evaluatie van de CT strategie dat informatiedeling een sleutelonderdeel is van de samenwerking tussen de verschillende partijen in de gedeelde aanpak van contraterrorisme. Het belang van informatie- en kennisdeling wordt door de literatuur bevestigd. 'In de eerste plaats is informatiedeling belangrijk voor het goed afstemmen van de samenwerking. In de tweede plaats is het uitwisselen van kennis en signalen belangrijk om een gezamenlijk beeld te ontwikkelen van het probleem, zodat betrokkenen vanuit deze gedeelde basis gecombineerde interventies inzetten'[50]. Dit geldt voor zowel informatie- en kennisdeling op nationaal niveau (signaleren van geradicaliseerde personen met het concrete voornemen tot uitreis), als op internationaal niveau (detecteren van de reisbeweging).
Door informatiedeling kunnen partijen perspectieven uitwisselen om steun of legitimiteit te versterken. Door de structurele samenwerking en coördinatie is het gehele stelsel robuust voorbereid op mogelijke dreigingen.'[51]

De integrale lokale aanpak zoals die staat in 2015 is volgens de geïnterviewde partijen van de evaluatie van de CT-strategie[52]:'krachtig door de brede betrokkenheid van verschillende partners; gezamenlijk kunnen ze steeds een maatwerkpakket van veiligheidsgerichte en sociaalgerichte interventies waarmaken.'

De CT strategie stelt tevens dat door het feit dat veel spelers actief zijn bij terrorismebestrijding, coördinatie en afstemming essentieel zijn. Dit is nodig om de efficiency en de effectiviteit van het beleid van deze actoren te vergroten.
Uit de evaluatie van de CT-strategie blijkt dat de wetenschappelijke literatuur ook grotendeels onderschrijft dat de aanname over het belang van coördinatie kan bijdragen aan een doelgericht interventievermogen. Tegelijkertijd wijzen wetenschappers er wel op dat de benodigde coördinatie onbedoeld kan doorschieten in strakke, starre aansturing, die het interventievermogen ten aanzien van ongekende, onbekende dreigingen juist weer ondermijnt[53].

Uit de evaluatie van de CT-strategie blijkt dat de NCTV wordt gewaardeerd en gerespecteerd als coördinator van de samenwerking[54]. De NCTV is van grote waarde bij het opbouwen van een goede informatiepositie door het bieden van beleidsmatige ondersteuning, kennis, expertise en trainingen.
In de evaluatie van de CT-strategie is wel opgemerkt dat, ondanks de waardering voor de coördinatie vanuit de NCTV, rolconflicten blijven terugkomen. 'Partners benadrukken het belang van coördinatie en zien dat de NCTV moet laveren tussen de eisen van verschillende organisaties en de wensen van de politiek. Organisaties als het OM stellen wel dat de NCTV beter moet balanceren tussen de genuanceerde

49 Evaluatie CT strategie 2011 -2015: Gericht, gedragen en geborgd interventievermogen?, USBO Advies, 8 april 2016, p. 35
50 Evaluatie CT strategie 2011 -2015: Gericht, gedragen en geborgd interventievermogen?, USBO Advies, 8 april 2016, p. 98, 146
51 Evaluatie CT strategie 2011 -2015: Gericht, gedragen en geborgd interventievermogen?, USBO Advies, 8 april 2016, blz. 100, 145
52 Evaluatie CT strategie 2011 -2015: Gericht, gedragen en geborgd interventievermogen?, USBO Advies, 8 april 2016, blz. 180
53 Evaluatie CT strategie 2011 -2015: Gericht, gedragen en geborgd interventievermogen?, USBO Advies, 8 april 2016, p. 100
54 Evaluatie CT strategie 2011 -2015: Gericht, gedragen en geborgd interventievermogen?, USBO Advies, 8 april 2016, p. 103,123,132

praktijk en de nadruk op een cijfermatige, harde stijl van verantwoorden vanuit de politiek. Deze rolconflicten zijn onvermijdelijk voor elke coördinator in een complex netwerk, maar wel is gesteld dat de rol van de NCTV als onafhankelijk makelaar tussen praktijk en politiek actief beschermd moet worden'[55].

In aansluiting op het laatste punt heeft de Inspectie VenJ in de onlangs verschenen Evaluatie van het Actieprogramma Integrale Aanpak Jihadisme opgemerkt dat de huidige meer kwantitatieve verantwoordingssystematiek over het Actieprogramma niet goed aansluit op het werk waarover verantwoording plaatsvindt. In de evaluatie is aangegeven dat ketenpartners zich afvragen of deze wijze van verantwoorden ook betekenisvol is, omdat kwantitatieve gegevens weinig zeggen over de kwaliteit van de aanpak.[56]

De evaluatie van de CT-strategie benoemt verder nog een aantal aspecten die het interventievermogen van het netwerk (kunnen) beïnvloeden:

- De brede oriëntatie van de strategie biedt onbedoeld ruimte voor selectieve aandacht. De strategie wil alle partners een 'kompas' bieden voor al hun acties, maar wordt onbedoeld een 'beleidscatalogus' om vrij uit te kiezen.
- Partners drijven van elkaar weg in tijden van verminderde aandacht. In tijden van verminderde aandacht zetten veiligheidsgerichte spelers nog redelijk actief in op het contraterrorismebeleid, maar zien sociaalgerichte partners geen expliciete rol voor zichzelf in het beleid.
- De capaciteit van landelijke partners fluctueert sterk. Wanneer de dreiging niet zichtbaar is of minder politieke aandacht krijgt, lukt het niet om kennis, contacten en menskracht op peil te houden.
- De integrale lokale aanpak is in potentie krachtig, maar ook de capaciteit van lokale partners heeft gefluctueerd. In afwezigheid van zichtbare dreiging neemt de capaciteit op radicalisering en terrorisme af bij lokale partners tot een enkele medewerker of valt alle menskracht weg.

Ten aanzien van het bewaken en beveiligen van personen, objecten en vitale infrastructuur zijn geen evaluaties beschikbaar die uitspraken doen over de doeltreffendheid en doelmatigheid van de ingezette beleidsinstrumenten. Uitspraken hierover zijn dus niet mogelijk. Wel hebben uitgevoerde evaluaties geleid tot verbeteringen en aandachtspunten, die vervolgens door de NCTV en de betrokken partijen zijn vertaald in acties en nieuwe beleidsinstrumenten.
Zo is bijvoorbeeld naar aanleiding van het onderzoek naar het Stelsel Bewaken en Beveiligen de stuurgroep Bewaken en Beveiligen opgericht waarin de betrokken partijen in gezamenlijkheid verbeteringen ten aanzien van het stelsel hebben geïnventariseerd. Een deel van deze punten komt uit de evaluatie van het Stelsel en deel van deze punten zijn in een eerder stadium geïdentificeerd door betrokken organisaties. Vervolgens heeft de stuurgroep richting gegeven en zorg gedragen voor de realisatie van deze verbeterpunten.[57]
Daarnaast laat de procesevaluatie op de pilot dreigingsmanagement zien dat het belang van dreigingsmanagement door diverse partijen wordt onderschreven. 'De aanzet tot meer integrale, gestructureerde en multidisciplinaire samenwerking tussen politie en zorg wordt als een groot winstpunt gezien. Deze samenwerking leidt naar het oordeel van de meeste respondenten tot meer en betere zorg voor de dreigers, wat volgens hen effectiever en ook goedkoper is dan uitsluitend de weg te bewandelen van strafrechtelijke sanctionering'.[58]

55 Evaluatie CT strategie 2011 -2015: Gericht, gedragen en geborgd interventievermogen?, USBO Advies, 8 april 2016, p.12
56 Inspectie Veiligheid en Justitie, Evaluatie van het Actieprogramma Integrale Aanpak Jihadisme, 2017, p.37
57 Conceptoverzicht verbeterpunten Stelsel Bewaken en Beveiligen, Stuurgroep B&B, 19 november 2014
58 Proces evaluatie Pilot Dreigingsmanagement, de implementatie en wijze van uitvoering onder de loep, Onderzoeksbureau Impact R&D, Universiteit Maastricht, mei 2013, p.6

4.1.4 *Uitspraken over doelmatigheid van het CT beleid niet mogelijk*

Zoals eerder aangegeven komt uit de evaluatie van de CT-strategie naar voren dat evaluatie op het niveau van instrumenten niet mogelijk is. Daarom is het niet mogelijk uitspraken te doen over de doelmatigheid van afzonderlijke instrumenten. Daarnaast doet de evaluatie ook geen uitspraken over de doelmatigheid van de instrumenten in zijn geheel. Wat wel in de evaluatie naar voren komt, is dat lokale partijen unaniem aangeven dat zij over voldoende instrumenten beschikken om te doen wat nodig is. De behoefte gaat veeleer om meer expertise en capaciteit om alle mogelijkheden te benutten[59].

In de Evaluatie van het Actieprogramma Integrale Aanpak Jihadisme van de Inspectie VenJ is ook geconcludeerd dat organisaties geen maatregelen missen om te interveniëren en dat het actieprogramma dus voorziet in de behoefte. Wel zijn een aantal maatregelen in de praktijk moeilijk verenigbaar, waardoor de ene maatregel het beoogde effect van de andere maatregel kan belemmeren. Indien deze situatie zich voordoet, gaat dit ten koste van de doeltreffendheid en daarmee ook de doelmatigheid van de aanpak. [60]

4.2 Doeltreffendheid en doelmatigheid beleid nationale veiligheid en crisisbeheersing

In deze paragraaf gaan wij eerst in op de evaluaties die zijn uitgevoerd op dit taakdomein. Daarna beschrijven we de implementatie van de instrumenten. Vervolgens zetten wij, op basis van de beschikbare evaluatie-onderzoeken, uiteen in hoeverre het plausibel is dat er een relatie bestaat tussen de doelstellingen en de ingezette beleidsinstrumenten. Daarbij gaan wij ook in op de rolinvulling van de NCTV. Tot slot zullen wij inzicht geven in wat bekend is over de doelmatigheid van het gevoerde beleid.

4.2.1 *Diverse evaluaties uitgevoerd op het terrein van crisisbeheersing*

In de afgelopen jaren zijn verschillende onderzoeken uitgevoerd op het terrein van Crisisbeheersing in Nederland. Zo hebben er diverse evaluaties van specifieke crises en rampen[61] in de periode van deze beleidsdoorlichting plaatsgevonden. Daarnaast zijn evaluaties uitgevoerd die algemener ingaan op het functioneren van crisisbeheersing en rampenbestrijding in Nederland in zijn totaliteit. Dit betreffen: de evaluatie van Wet Veiligheidsregio's in 2013, de Staat van de rampenbestrijding 2013 en 2016, het rapport van de evaluatiecommissie Hoekstra (2013)[62] en het onderzoek van de Algemene Rekenkamer 'Zicht overheden op beschermen burgers en bedrijven' uit 2014.

Om inzicht te geven in de effectiviteit van het beleid dat de NCTV heeft gevoerd op het gebied van crisisbeheersing en rampenbestrijding in Nederland geven wij in bijlage 6 eerst een overzicht van de ingezette beleidsinstrumenten over de periode 2011-2015. Daarbij geven wij inzicht in de realisatie en werkbaarheid van de instrumenten. Ofwel of de instrumenten zijn gerealiseerd en ook worden toegepast in de praktijk. Daarnaast geeft de bijlage inzicht of de instrumenten zijn geëvalueerd en in hoeverre in de beschikbare evaluaties uitspraken zijn gedaan over doeltreffendheid en doelmatigheid van de ingezette instrumenten.

59 Evaluatie CT strategie 2011 -2015: Gericht, gedragen en geborgd interventievermogen?, USBO Advies, 8 april 2016, p. 157-160
60 Evaluatie van het Actieprogramma Integrale Aanpak Jihadisme, Inspectie Veiligheid en Justitie, 2017, p.30
61 Zoals evaluaties van bijvoorbeeld vlucht MH17, Diginotar, Brand bij Chemiepack en Project X Haren.
62 De evaluatiecommissie Hoekstra heeft voor haar onderzoek vele betrokkenen gesproken op het gebied van de Wet veiligheidsregio's, de rampenbestrijding en crisisbeheersing en voor haar adviezen vormden de evaluatie Wet Veiligheidsregio's (2013) en de Staat van de rampenbestrijding (2013) een belangrijke basis

4.2.2 *Beleidsinstrumenten nationale veiligheid en crisisbeheersing zijn geïmplementeerd*

Zoals in bijlage 6 is te zien hebben wij vastgesteld of instrumenten ook zijn gerealiseerd. Uit onze analyse komt naar voren dat de NCTV de instrumenten volledig of (groten)deels heeft gerealiseerd.

4.2.3 *Effectiviteit stelsel crisisbeheersing is verbeterd, maar nog geen inzicht in doeltreffendheid beleid vergroten weerbaarheid*

De uitgevoerde evaluaties en onderzoeken gaan niet of beperkt in op de plausibiliteit of doeltreffendheid van de specifieke beleidsinstrumenten. Wel hebben de uitgevoerde evaluaties in alle gevallen geleid tot aandachtspunten en/of aanbevelingen. Deze aandachtspunten en aanbevelingen zijn op hun beurt in de periode 2011- 2015 veelal vertaald in nieuwe beleidsinstrumenten of aanpassing van bestaande instrumenten. Zo heeft de minister van Veiligheid en Justitie bijvoorbeeld bij besluit van 24 mei 2012 een onafhankelijke commissie (Evaluatiecommissie Hoekstra) ingesteld met als taak een integraal advies uit te brengen over de werking van de Wet veiligheidsregio's en over het Nederlandse stelsel van rampenbestrijding en crisisbeheersing. De Evaluatiecommissie heeft bij de uitvoering van haar opdracht veel betrokkenen en deskundigen geraadpleegd op het gebied van de Wet veiligheidsregio's, rampenbestrijding en crisisbeheersing. Daarnaast vormden de evaluatie van de Wet Veiligheidsregio's en de Staat van de rampenbestrijding 2013 een belangrijke basis voor haar adviezen. De aanbevelingen van de Commissie Hoekstra hebben direct geleid tot nieuwe of aangepaste beleidsinstrumenten om de crisisbeheersing en rampenbestrijding in Nederland verder te verbeteren.

De evaluatieonderzoeken die algemener ingaan op het functioneren van crisisbeheersing en rampenbestrijding in Nederland doen ook uitspraken over effecten van het gevoerde beleid in de periode van de beleidsdoorlichting. Zo constateert de Commissie Hoekstra in haar rapport dat 'in het algemeen het ontwikkelen van de veiligheidsregio's een gunstig effect hebben gehad op de kwaliteit en effectiviteit van de rampenbestrijding. De invoering van de Wet veiligheidsregio's heeft gezorgd voor een vergroting van expertise, een versterking van operationele slagkracht en vergroting van de effectiviteit. De Commissie concludeert dat dankzij de wet verbeteringsprikkels zijn gecreëerd en is de mogelijkheid ontstaan om op een hoger dan gemeentelijk niveau te werken aan een goede voorbereiding op rampen en crises. Dat zijn grote verbeteringen'.[63]

Verder komt in het rapport van de Commissie naar voren dat 'hoewel nog geen van de veiligheidsregio's aan *alle* wettelijke minimumeisen voldoet, het niveau waarop de veiligheidsregio's functioneren de afgelopen jaren is gestegen. Zo is de samenwerking tussen de verschillende hulpverleningsdiensten sterk verbeterd, net als de samenwerking tussen veiligheidsregio's en andere crisispartners'[64]. De Commissie geeft aan dat 'zij onder de indruk was van het vele werk dat in de voorgaande jaren al was verricht en de professionaliteit en geestdrift waarmee door de regio's aan verbeteringen wordt gewerkt'[65].

De Commissie Hoekstra concludeert ook dat er ruimte voor verbetering is. 'De Wet veiligheidsregio's richt zich vooral op de klassieke rampenbestrijding. Op dit gebied heeft de wet flinke verbeteringen teweeggebracht. Het effect van de wet is minder goed te zien op andere gebieden waar verbetering nodig was: een betere

63 Eindrapportage Evaluatiecommissie Wet veiligheidsregio's en het stelsel van Rampenbestrijding en Crisisbeheersing, Evaluatiecommissie Hoekstra, d.d. 18 september 2013, p. 7, 19
64 Eindrapportage Evaluatiecommissie Wet veiligheidsregio's en het stelsel van Rampenbestrijding en Crisisbeheersing, Evaluatiecommissie Hoekstra, d.d. 18 september 2013, p. 7
65 Eindrapportage Evaluatiecommissie Wet veiligheidsregio's en het stelsel van Rampenbestrijding en Crisisbeheersing, Evaluatiecommissie Hoekstra d.d. 18 september 2013, p. 3

(aansturing van de) brandweerzorg en effectievere beheersing van crises waarmee de samenleving momenteel wordt geconfronteerd. Ook zijn de taken van de gemeente en de politie nog onvoldoende geïntegreerd in de rampenbestrijding. Multidisciplinaire samenwerking en de voorbereiding op crises laten nog altijd te wensen over; er is onder meer aandacht nodig voor bovenregionale samenwerking, regelmatig oefenen en de rol van de rijksoverheid.'[66]

Ook de Inspectie van Veiligheid en Justitie concludeert in haar rapport Staat van de rampenbestrijding 2016 dat de veiligheidsregio's in de afgelopen jaren een positieve ontwikkeling doormaakten. 'Was in de Staat van de rampenbestrijding 2013 het beeld dat de veiligheidsregio's nog volop bezig waren met de inrichting van de organisatie, uit de Staat 2016 komt naar voren dat de veiligheidsregio's in de afgelopen jaren een positieve ontwikkeling hebben doorgemaakt en in toenemende mate taakvolwassen zijn geworden.'[67]
'De voorbereiding op rampen en incidenten in de plannen is doorgaans goed geregeld en de samenwerking met de (vitale) partners gaat steeds beter. De gemeenten hebben belangrijke stappen gezet, niet alleen als verantwoordelijke voor de veiligheidsregio, maar ook op weg als partner in crisisbeheersing[68]. De daadwerkelijke taakuitvoering bij de aanpak van incidenten en oefeningen is echter op meerdere punten nog voor verbetering vatbaar. Ook kwaliteitszorg is in de veiligheidsregio's nog volop in ontwikkeling. Het evalueren van oefeningen en incidenten is de afgelopen jaren duidelijk verbeterd. Het zicht op de vakbekwaamheid van de multidisciplinaire crisisfunctionarissen daarentegen is in de meeste veiligheidsregio's nog beperkt'.

Zoals te zien is in bijlage 6[69] zijn door de NCTV ook diverse beleidsinstrumenten ingezet voor het vergroten van de weerbaarheid van de vitale infrastructuur en zijn deze beleidsinstrumenten grotendeels dan wel volledig gerealiseerd. Zo heeft onder andere een herijking van wat voor Nederland vitaal is plaatsgevonden, wordt de stand van zaken van de weerbaarheid van vitale processen periodiek in kaart gebracht, zijn de vitale processen geborgd in de uitwerking van beleid en wet en (Europese) regelgeving, en is door de NCTV de internationale tabletop oefening VITEX georganiseerd waarin 22 Europese lidstaten hebben samengewerkt aan hoe te handelen als een vitale infrastructuur uitvalt.

Er zijn echter geen evaluaties beschikbaar die uitspraken doen over in hoeverre deze beleidsinstrumenten hebben bijgedragen aan het vergroten van de weerbaarheid van de vitale infrastructuur.

4.2.4 *Uitspraken over doelmatigheid van het beleid ten aanzien van nationale veiligheid en crisisbeheersing niet mogelijk*

Op basis van de beschikbare evaluaties is het niet mogelijk uitspraken te doen over de doelmatigheid van de afzonderlijke beleidsinstrumenten of het gevoerde beleid in bredere zin. De beschikbare evaluaties doen daarover geen uitspraken.

4.3 Doeltreffendheid en doelmatigheid beleid cybersecurity

In deze paragraaf gaan wij eerst in op de evaluaties die zijn uitgevoerd op dit taakdomein. Daarna beschrijven we de implementatie van de instrumenten. Vervolgens zetten wij, op basis van de beschikbare evaluatie-onderzoeken, uiteen in hoeverre het plausibel is dat er een relatie bestaat tussen de doelstellingen en de ingezette beleidsinstrumenten. Daarbij gaan wij ook in op de rolinvulling van de NCTV. Tot slot zullen wij inzicht geven in wat bekend is over de doelmatigheid van het gevoerde beleid.

66 Eindrapportage Evaluatiecommissie Wet veiligheidsregio's en het stelsel van Rampenbestrijding en Crisisbeheersing, Evaluatiecommissie Hoekstra d.d. 18 september 2013, p. 7
67 Staat van de rampenbestrijding 2016 Landelijk beeld, Inspectie Veiligheid en Justitie, oktober 2016, p. 36
68 Staat van de rampenbestrijding 2016 Landelijk beeld, Inspectie Veiligheid en Justitie, oktober 2016, p. 3
69 Bijlage 2: Overzicht beleidsinstrumenten crisisbeheersing en nationale veiligheid, instrument 30,33,34

4.3.1 *Beperkt aantal evaluaties uitgevoerd op het terrein cybersecurity*

In de afgelopen jaren zijn een beperkt aantal onderzoeken verschenen op het taakgebied van Cybersecurity. Dit is ook te zien in bijlage 7 waarin een matrix is opgenomen om inzicht te geven in onder andere de uitgevoerde evaluaties van de verschillende beleidsinstrumenten. Twee evaluaties hebben plaatsgevonden door de Inspectie van het ministerie van VenJ. De eerste evaluatie was naar de DigiNotar-crisis (2011) en tweede evaluatie naar het gebruik van beveiligingsadviezen van het NCSC (2015). Verder zijn in 2017 nog twee rapporten verschenen: het rapport 'Een nooit gelopen race – Over cyberdreigingen en versterking van weerbaarheid' uitgebracht door het Rathenau Instituut en is een rapport gepubliceerd door het Potomac Institute for Policy Studies over Cyber Readiness van Nederland. Dit rapport kan worden gezien als een nulmeting waarmee inzicht wordt gegeven in hoeverre Nederland is voorbereid op cyberincidenten[70]. Ondanks dat het rapport over de situatie in 2016 gaat is het onderzoek wel relevant. De huidige score op de Cyber Readiness Index is deels ook beïnvloed door de inspanningen die de afgelopen jaren zijn geleverd in het kader van de Nationale Cyber Security Strategie.

4.3.2 *Merendeel van de beleidsinstrumenten cybersecurity geïmplementeerd*

Zoals in bijlage 7 is te zien heeft de NCTV het merendeel van de instrumenten gerealiseerd. De matrix bevat niet alle instrumenten zoals opgenomen in de cybersecurity strategie. De reden is dat ook onderdelen van het uit te voeren beleid zijn belegd bij andere (interdepartementale) partners. Dit sluit ook aan op de coördinerende rol van de NCTV.

4.3.3 *Relatie tussen beleidsinstrumenten cybersecurity en de gewenste effecten niet geëvalueerd*

Kijkend naar de werkbaarheid geeft het in 2017 uitgevoerde onderzoek naar Cyber Readiness een beeld[71]. Hierin is gesteld dat Nederland deels operationeel is op het merendeel van zeven essentiële elementen van de Cyber Readiness Index (CRI), te weten: 'national strategy, incident response, e-crime and law enforcement, information sharing, investment in R&D, diplomacy and trade, and defense and crisis response'. Hoewel deze constatering niet direct iets zegt of het beleid beschreven in deze beleidsdoorlichting ook is toegepast in de praktijk, bevat het beleid zoals verwoord in deze doorlichting wel raakvlakken met de zeven essentiële elementen van CRI. Zo zijn ingezette beleidsinstrumenten bijvoorbeeld gericht op onder andere het verkrijgen van gezamenlijk integraal beeld van actuele dreigingen en kwetsbaarheden, stimuleren van onderzoek op het gebied van cybersecurity en het versterken van de responscapaciteit[72].

Een relatie tussen het gevoerde beleid en de gewenste effecten komen niet duidelijk naar voren in uitgevoerde evaluaties. Wel geeft het onderzoek naar Cyber Readiness inzicht in de mate waarop Nederland is voorbereid op cyberrisico's. Zoals in de vorige paragraaf aangegeven, is Nederland deels operationeel op het merendeel van de essentiële elementen van CRI[71]. Deze bevinding kan niet direct worden toegeschreven aan het gevoerde beleid en de inspanningen van de NCTV, maar geeft wel aan dat het gehele cyberstelsel waar ook de beleidsinstrumenten van de NCTV onderdeel van uitmaken, een bepaald volwassenheidsniveau ontwikkeld heeft. Hoewel belangrijke stappen zijn gezet, laat het onderzoek ook zien dat Nederland zich nog verder kan ontwikkelen. Het

70 Landen kunnen een evaluatie laten uitvoeren om aan de hand van de ontwikkelde methodiek inzicht te verkrijgen in de operationele 'cyber readiness'; Nederland is 1 van de 9 landen (in totaal 125 landen die methodiek hanteren) die evaluatieonderzoek heeft laten uitvoeren.

71 Potomac Institute for Policy Studies, The Netherlands Cyber readiness at a glance, Cyber Readiness Index 2.0, all rights reserved

72 Zie bijlage 3: overzicht beleidsinstrumenten cybersecurity 2012-2015

recente onderzoek van het Rathenau instituut stelt zelfs dat de weerbaarheid het gehele cyberstelsel in Nederland onvoldoende op orde is[73].

Het onderzoek van de inspectie VenJ naar het gebruik van de beveiligingsadviezen van het NCSC geeft enig inzicht in de rol van de NCTV. Daaruit komt naar voren dat betrokken partijen de kennis en expertise van het NCSC als onderdeel van de NCTV waarderen. Dit betreft niet alleen de beveiligingsadviezen, maar ook de andere producten die het NCSC levert (bijvoorbeeld factsheets, white papers en sectorale overlegvormen)[74].

4.3.4 *Uitspraken over doelmatigheid beleid cybersecurity niet mogelijk*

Net als voor de andere taakvelden is een uitspraak over doelmatigheid niet mogelijk. In het rapport over Cyber Readiness is opgenomen dat Nederland minder dan 0,01 procent van zijn Bruto Binnenlands Product uitgeeft aan cybersecurity. Daarbij is vermeld dat dit relatief gezien beduidend minder is dan andere ontwikkelde landen, zoals de Verenigde Staten, Verenigd Koninkrijk, Australie, Duitsland en Frankrijk[1]. Een kanttekening hierbij is wel dat uitgaven aan cybersecurity in Nederland mogelijk hoger zijn, maar niet altijd als zodanig zichtbaar dan wel benoemd zijn.
Een ander kengetal dat interessant is voor doelmatigheid betreft de schade die digitale dreigingen de maatschappij toebrengen. Zoals in 2014 reeds door het Kabinet[75] is aangegeven is de exacte schade moeilijke te becijferen, maar er verschijnen met regelmaat onderzoeken. Zoals recent TNO die in hun onderzoek zeer forse schadekosten berekenen voor cybercrime; ten minste €10 miljard, ofwel 1,5 tot 2% van het BBP. Uitgaande hiervan zijn de kosten daarmee vele malen hoger dan wat Nederland uitgeeft aan cybersecurity. Echter is het niet mogelijk om te bepalen wat de invloed is van het gevoerde beleid ten aanzien van het gevoerde beleid om de digitale weerbaarheid te verhogen ten aanzien van de de eventuele kosten van een gebrek daaraan. Wel geeft de impact van digitale dreigingen aan dat coördinatie op dit onderwerp relevant is, zodat Nederland daar beter weerbaar tegen is en adequaat kan gehandeld wordt bij een incident of crisis.

73 Geert Munnichs, Matthijs Kouw & Linda Kool, Een nooit gelopen race - Over cyberdreigingen en versterking van weerbaarheid. Den Haag, Rathenau Instituut 2017, p.44
74 Rapport Inspectie Veiligheid en Justitie, Gebruik van beveiligingsadviezen van het Nationaal Cyber Security Centrum, mei 2015.
75 Vragen van het lid Recourt (PvdA) aan de Minister van Veiligheid en Justitie over het bericht dat cybercrime Nederland jaarlijks 8,8 miljard euro kost (ingezonden 13 juni 2014). Antwoord van Minister Opstelten (Veiligheid en Justitie) (ontvangen 14 augustus 2014). Zie ook Aanhangsel Handelingen, vergaderjaar 2013–2014, nr. 2457.

5 Samenvattend beeld en aanbevelingen

Op basis van de bevindingen van deze beleidsdoorlichting presenteren wij in dit hoofdstuk een samenvattend beeld met bijbehorende aanbevelingen.

5.1 Merendeel van de ingezette beleidsinstrumenten is gerealiseerd

De NCTV heeft in de periode 2011-2015 veel werk verzet. Het gevoerde beleid op het gebied van contraterrorisme, nationale veiligheid en crisisbeheersing en cybersecurity is veelomvattend geweest. De NCTV heeft veel beleidsinstrumenten ingezet om het beleid op deze taakvelden over deze periode vorm te geven. Uit onze analyse blijkt dat het merendeel van de beoogde beleidsinstrumenten ook volledig of (groten)deels is gerealiseerd.

5.2 Veel evaluaties zijn beschikbaar met indicaties over plausibiliteit beleid, inclusief aandachtspunten voor verbetering

In alle drie de taakdomeinen zijn evaluaties uitgevoerd. Wel verschilt per taakdomein in hoeverre de uitgevoerde evaluaties inzicht geven in de plausibiliteit en effectiviteit van het gevoerde beleid.
Zo komt uit de evaluatie van de CT-strategie naar voren dat uitspraken over de doeltreffendheid van beleid niet mogelijk is, maar het wel plausibel is dat het ingezette beleid op het gebied van contraterrorisme gerechtvaardigd is.

Uit de evaluaties op het gebied van crisisbeheersing blijkt dat, hoewel verbetering mogelijk is, de kwaliteit en doeltreffendheid van de crisisbeheersing en rampenbestrijding in Nederland in de afgelopen jaren is verbeterd. De uitgevoerde evaluaties doen maar beperkt uitspraken over de relatie tussen de ingezette beleidsinstrumenten en de gerealiseerde effecten. Wel hebben de diverse uitgevoerde evaluaties geleid tot aandachtspunten en/of aanbevelingen. Deze aandachtspunten en aanbevelingen zijn op hun beurt in de periode 2011-2015 veelal vertaald in nieuwe beleidsinstrumenten of aanpassing van bestaande instrumenten.

Op het gebied van cybersecurity zijn maar beperkt evaluaties aanwezig.
Door het achterblijven hiervan zijn nu nog maar zeer beperkt uitspraken over de plausibiliteit en effecten op dit beleidsterrein mogelijk. Echter hebben enkele evaluaties die zijn uitgevoerd wel geleid tot aandachtspunten en/of aanbevelingen die vervolgens door de NCTV zijn opgepakt.

5.3 Uitspraken over effectiviteit en doelmatigheid van specifieke beleidsinstrumenten echter beperkt mogelijk

Hoewel met name ten aanzien van de taakvelden contraterrorisme en nationale veiligheid en crisisbeheersing over de periode 2011-2015 de nodige evaluaties zijn uitgevoerd, zijn deze onderzoeken veelal algemeen van aard en/of evalueren de ingezette beleidsinstrumenten in gezamenlijkheid. De doeltreffendheid en doelmatigheid van de afzonderlijke beleidsinstrumenten kan op basis van het beschikbare onderzoek veelal niet worden aangetoond. In sommige gevallen is evaluatie van (afzonderlijke) instrumenten echter ook niet mogelijk. Zo zijn de effecten van het contraterrorismebeleid niet rechtstreeks te evalueren, omdat de ogenschijnlijke effecten van het beleid ook door andere oorzaken tot stand kunnen zijn gekomen.

Daarnaast ontbreekt het aan onderzoek naar wat de NCTV vanuit haar coördinerende rol wil bereiken[76]. Hoewel beperkt, doen enkele evaluaties wel uitspraken over de rolinvulling van de NCTV. Zo blijkt uit bijvoorbeeld de evaluatie van de CT-strategie dat de NCTV wordt gewaardeerd en gerespecteerd als coördinator van de samenwerking[77]. Ook het onderzoek van de inspectie VenJ naar het gebruik van de beveiligingsadviezen van het NCSC geeft enig inzicht in de rol van de NCTV. Daaruit blijkt dat de betrokken partijen de kennis en expertise van het NCSC, als onderdeel van de NCTV, waarderen[78]. De uitgevoerde evaluaties doen echter geen uitspraken over wat de NCTV wil bereiken bij haar partners, maar zijn meer gericht op de maatschappelijke impact van instrumenten die door de publieke en private partners in gezamenlijkheid zijn ingezet.

Ten aanzien van de doelmatigheid van de afzonderlijke beleidsinstrumenten of het gevoerde beleid in bredere zin geldt voor alle drie de taakdomeinen dat het op basis van de beschikbare evaluaties niet mogelijk is hier uitspraken over te doen.
Het overgrote deel van de ingezette beleidsinstrumenten is niet direct te koppelen aan gelabelde uitgaven. Het betreft instrumenten waarbij de realisatie ervan vooral afhankelijk is van de inzet van medewerkers van de NCTV. Op het niveau van beleidsinstrumenten is nu niet inzichtelijk hoeveel tijd medewerkers aan instrumenten hebben besteed. Aparte kostprijzen voor het merendeel van de ingezette beleidsinstrumenten kunnen dan ook niet worden berekend.

5.4 Aanbevelingen

Op basis van onze bevindingen zijn wij van mening dat er meer mogelijk is op het gebied van het inzichtelijk maken van (effecten van) van het beleid van de NCTV dan op dit moment gebeurt. Wij achten het daarom van belang dat meer en/ of beter gericht materiaal beschikbaar komt om goede (effect)evaluaties mogelijk te maken met als doel beter inzicht te krijgen in de kwaliteit van het gevoerde en voorgenomen beleid en lessen te kunnen trekken over de doelmatigheid en doeltreffendheid van het beleid.

Wij adviseren de NCTV daarom eerst explicieter uit te werken wat de NCTV vanuit haar rol bij ketenpartners wil bereiken. Dit betekent dat de NCTV vanuit de verschillende ketenbrede strategieën per taakdomein, zoals bijvoorbeeld de CT-strategie, een vertaling zal moeten maken naar wat de NCTV vanuit haar rollen bij haar partners wil realiseren. Definieer vanuit de beleidsdoelstellingen de gewenste resultaten[79] waarbij de kernvraag is hoe de beleidsinterventie geacht wordt te werken. Met een goed beargumenteerde en onderbouwde beleidstheorie zal de NCTV beter in staat zijn haar eigen beleid te laten evalueren en zal een onderzoek ook specifieker inzicht kunnen geven in het functioneren en het effect van het beleid van de NCTV. Een dergelijk inzicht is van belang om als organisatie (beter) te kunnen leren en te verbeteren, maar ook om beter te kunnen verantwoorden over inspanningen die zijn geleverd.

Daarnaast adviseren wij om vervolgens, in aansluiting op meer concreet geformuleerd NCTV beleid, te inventariseren welke en hoe ingezette beleidsinstrumenten kunnen worden geëvalueerd op hun doeltreffendheid en

76 Zoals toegelicht in de inleiding van dit rapport is er voor deze beleidsdoorlichting een alternatieve onderzoeksvraag geformuleerd voor wat betreft de doeltreffendheid van het gevoerde beleid Door de begeleidingscommissie van deze beleidsdoorlichting is gekozen dit te richten op dat wat de minister van VenJ, werkende via de NCTV, vanuit zijn coördinerende functie bij de publieke en private partners wil bereiken. Reden hiervoor is dat de causaliteit tussen ingezette beleidsinstrumenten en de doeltreffendheid lastig is vast te stellen, omdat nog vele andere factoren van invloed kunnen zijn geweest op het uiteindelijke effect

77 Evaluatie CT strategie 2011 -2015: Gericht, gedragen en geborgd interventievermogen?, USBO Advies, 8 april 2016, p. 103,123,132

78 Rapport Inspectie Veiligheid en Justitie, Gebruik van veiligheidsadviezen van het Nationaal Cyber Security Centrum, mei 2015.

79 SMART geformuleerd: Specifiek, Meetbaar, Acceptabel, Realistisch en Tijdgebonden

doelmatigheid. Bij nieuwe beleidsinitiatieven adviseren wij steeds de mogelijkheid te onderzoeken of eerst een experiment kan worden uitgevoerd en daarbij een zodanige vorm te zoeken dat effectevaluaties mogelijk zijn. Uiteraard moet wel recht gedaan worden aan de complexiteit van het beleid op de verschillende taakgebieden, waarbij veelal geen sprake is van een ondubbelzinnige één-op-één relatie tussen de inzet van een beleidsinstrument en het beoogde doel.

6 Verantwoording onderzoek

Deze beleidsdoorlichting is uitgevoerd door onderzoekers van de ADR die zijn aan te merken als onafhankelijke deskundigen zoals bedoeld in de RPE. Bij het onderzoek is de ADR ondersteund door een begeleidingscommissie die beschikbare informatie en aanvullende inzichten heeft aangedragen. De begeleidingscommissie bestond uit medewerkers van de NCTV van het ministerie van JenV, medewerker directie Financieel Economische Zaken (DFEZ) van het ministerie van JenV, de Inspectie der Rijksfinanciën (IRF) en het Wetenschappelijk Onderzoek- en Documentatie Centrum van het ministerie van JenV (WODC).

6.1 Object van onderzoek, werkzaamheden en afbakening

Het object van onderzoek is het beleid dat ten grondslag ligt aan artikel 36.2 van de begroting van het ministerie van JenV, over de periode 2011 -2015. Het betreft hier het hele werkveld van de NCTV.

De ADR heeft de volgende uitgangspunten en werkwijze bij deze beleidsdoorlichting gehanteerd:

- De synthese benadering zoals benoemd in de RPE: er is bij de analyse uitsluitend gebruik gemaakt van reeds elders beschikbare informatie en onderzoeksmateriaal. Er is door de ADR geen aanvullend eigenstandig onderzoek verricht.
- De begeleidingscommissie heeft, vanuit haar diverse achtergronden en inzichten, zorg gedragen voor de aanlevering van de relevante informatie over de gehanteerde beleidstheorie en de beschikbare informatie en onderzoeken over de implementatie en effectiviteit van het beleid.
- Om vast te kunnen stellen of de beleidsdoelstellingen zijn gerealiseerd zijn ze op grond van de gehanteerde beleidstheorie zoveel mogelijk geconcretiseerd in SMART-doelstellingen[80] en daaraan gekoppelde instrumenten.
- Bij de analyse van de beschikbare informatie en het onderzoeksmateriaal is de volgende 'getrapte' aanpak gekozen om een uitspraak te kunnen doen over de doeltreffendheid en doelmatigheid van het beleid:
    - Bepalen van de mate waarin het doel is bereikt: kan op basis van de (SMART) geformuleerde doelstellingen en beschikbare informatie een uitspraak over de mate van doelbereiking gedaan worden?
    - Bepalen van de instrumentrealisatie: zijn de beoogde instrumenten ook daadwerkelijk ingezet en hoeveel geld is hiermee gemoeid?
    - Bepalen van de mate van de effectiviteit van het beleid(instrument): in welke mate blijkt uit effectonderzoeken dat het beleid(instrument) aantoonbaar aan de doelbereiking heeft bijgedragen?
    - En bij ontbreken van effectonderzoek: zijn er andere indicaties beschikbaar over de plausibiliteit dat het beleid heeft bijgedragen aan het realiseren van de doelen?
    - Bepalen van de mate van doelmatigheid: staat het ingezette budget in een redelijke verhouding tot de gerealiseerde effectiviteit?

80 SMART: specifiek, meetbaar, acceptabel, realistisch, tijdgebonden.

- Op basis van de voorgaande analyse beschrijft dit rapport het samenvattende beeld van de ADR-onderzoekers over de doeltreffendheid en doelmatigheid van het gevoerde beleid. Dit beeld is onafhankelijk van de begeleidingscommissie geformuleerd. De begeleidingscommissie heeft tijdens diverse stadia van het onderzoek gereflecteerd op de synthese die door de ADR is uitgevoerd, en waarnodig aanvullende inzichten en onderzoekmateriaal aangeleverd, die in de beoordeling door de ADR zijn meegenomen in het eindrapport.

De ADR heeft het onderzoek uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing en de kwaliteitseisen zoals vastgelegd in het Handboek Auditing Rijksoverheid (HARo).
In dit rapport wordt geen zekerheid verschaft, omdat er conform de standaarden geen zogeheten assurance-opdracht is uitgevoerd.

6.2 Afwijkingen initiële opdracht

In de opdrachtformulering van deze beleidsdoorlichting[81] is onderscheid gemaakt in vier taakdomeinen van de NCTV, te weten: terrorismebestrijding, crisisbeheersing, rampenbestrijding en brandweerzorg, cybersecurity en bewaking en beveiliging (inclusief burgerluchtvaart). Tijdens het uitvoeren van deze beleidsdoorlichting is gebleken dat het taakdomein bewaking en beveiliging zeer nauw gerelateerd is aan terrorismebestrijding. Daarom is er voor gekozen bewaking en beveiliging onderdeel te laten uitmaken van het dit taakdomein.

In de opdrachtformulering is nog de volgende aanvullende specifieke onderzoeksvraag opgenomen: Is het instrument van de decentralisatie-uitkering (aan gemeenten) of een lumpsum bijdrage (aan veiligheidsregio's) een effectief middel om centraal vastgesteld beleid decentraal te laten uitvoeren?

Voor zover het beschikbare onderzoeksmateriaal hier antwoord op geeft, is hier antwoord opgegeven bij het specifieke beleidsinstrument BDUR, zoals opgenomen in bijlage 3 bij dit rapport.

6.3 Beleidsreactie

De opdrachtgever, voorzitter van de begeleidingscommissie mw. Patricia Zorko (plv. NCTV en directeur Cybersecurity), is eigenaar van dit rapport.

De minister van JenV beschrijft in een separate beleidsreactie zijn reactie op de bevindingen van deze beleidsdoorlichting.

Naast het onderhavige onderzoekrapport van de ADR, dat is gericht op de effectiviteit en doelmatigheid van het beleid, is er door de NCTV en de directie FEZ van het ministerie van JenV een onderzoek uitgevoerd naar besparingsmogelijkheden. Dit geeft uitvoering aan de RPE-bepaling om beleidsdoorlichtingen te voorzien van een 20% besparingsvariant. De resultaten van dit onderzoek zijn opgenomen in de beleidsreactie bij dit rapport.

81 Opdrachtbevestiging Beleidsdoorlichting Nationale Veiligheid (art. 36.2), 3 november 2016

7 Ondertekening

Den Haag, 22 november 2017

drs. C. Spaaij RO CIA

Auditmanager
Auditdienst Rijk (ADR)

Bijlagen

Bijlage 1: Beleidsboom NCTV

Veilig en stabiel Nederland: voorkomen en beperken van maatschappelijke ontwrichting door het beschermen van vitale belangen, door dreigingen weg te nemen en de weerbaarheid te verhogen.

Contra Terrorisme: voorkomen van aanslagen, verminderen van de vrees voor aanslagen en beperken van eventuele gevolgen van een aanslag

- **Verstoren van dreigingen en verijdelen aanslagen door beperken van toegang tot middelen en tegengaan reisbewegingen**
  - **Ontwikkelen, ondersteunen en beschikbaar stellen instrumenten voor partners**
    - *Aanjagen van en bijdragen aan wijzigingen in wet -en regelgeving*
    - *Ontwikkelen van, adviseren over én toepassen van maatregelen en interventies*
    - *Versterken informatie-uitwisseling voor detectie en tegengaan reisbewegingen*
  - **Coördineren en faciliteren van lokale, nationale en internationale samenwerkingsverbanden**
    - *Opzetten (samenwerkings)structuur en verbeteren (operationele) informatie uitwisseling*
    - *Intensivering van de internationale samenwerking en aanpak jihadgangers*
- **Voorkomen aanwas door ondermijning aanbod propaganda en verhogen kwetsbare groepen**
  - **Coördineren en faciliteren van het netwerk aan partijen waarbinnen activiteiten ter voorkoming aanwas moet plaatsvinden**
    - *Opzetten structuur en verbetering informatie-uitwisseling*
    - *Versterken van het netwerk, lokaal en landelijk, gericht op ingrijpen bij radicalisering en deradicalisering*
- **Beschermen van personen, objecten en vitale processen tegen terroristische aanslagen**
  - **Verder professionaliseren van het Steisel Bewaken en Beveiligen**
  - **Intensivering aanpak solistische dreigers**
  - **Toekomstbestendig maken van de beveiligingscontroles op de luchthavens**

Nationale veiligheid en crisisbeheersing: voorkomen en beperken van maatschappelijke ontwrichting door crisis

- **Verbeteren van het functioneren van het steisel crisisbeheersing door coördinatie en vereenvoudigen van besluitvorming**
  - **Versterken nationale crisisorganisatie**
  - **Versterken presterend vermogen veiligheidsregio's en Caribisch Nederland**
  - **Versterken samenwerking**
  - **Versterken informatievoorziening en crisiscommunicatie**
  - **Behoud historisch erfgoed**
- **Vergroten weerbaarheid vitale belangen**
  - **Versterken weerbaarheid ten behoeve van de nationale veiligheid**
  - **Versterken economische veiligheid**
  - **Verhogen weerbaarheid Rijk tegen spionage**

Cybersecurity: veiligheid en vertrouwen in een open en vrije digitale samenleving

- **Versterken integrale aanpak cybersecurity door publieke en private partijen**
  - **Duidelijke verdeling van taken, verantwoordelijkheden en bevoegdheden**
  - **Bouwen aan coalities voor vrijheid, veiligheid en vrede in het digitale domein**
- **Nederland zorgt voor adequate en actuele dreiging- en risicoanaalyses**
  - **Gezamenlijk integraal beeld van de actuele dreigingen en kwetsbaarheden van ICT**
  - **Versterken van onderzoeks- en analysecapaciteit**
- **Versterken van de weerbaarheid tegen ICT-verstoringen en Cyberaanvallen**
  - **Vergroten en ontwikkelen cybersecurity experts**
  - **Stimuleren onderzoek Cybersecurity**
  - **Vergroten kennis over en veiligheidsbewustzijn van ICT-producten en diensten bij de gebruikers (burgers en bedrijven)**
  - **Bewerkstelligen dat publieke en private leveranciers voldoen aan minimum eisen op het gebied van continuiteits - dienstverlening en spionage**
- **Versterken responscapaciteit om ICT-verstoringen en cyberaanvallen te kunnen pareren**
  - **Duidelijke crisis structuur bij cyberincidenten**
  - **Informeren van de burgers en bedrijfsleven bij cyberincidenten**
  - **Stimuleren kennis(deling) en oefening**

Bijlage 2: Beleidsboom Contraterrorisme

Taakveld Contraterrorisme
2011 - 2015

Contra Terrorisme: voorkomen van aanslagen, verminderen van de vrees voor aanslagen en beperken van eventuele gevolgen van een aanslag

Verstoren van dreigingen en verijdelen aanslagen door beperken van toegang tot middelen en tegengaan reisbewegingen

Ontwikkelen, ondersteunen en beschikbaar stellen instrumenten voor partners

Aanjagen van en bijdragen aan wijzigingen in wet -en regelgeving

- Wijziging van de Rijkswet op het Nederlanderschap ter verruiming van de mogelijkheden voor het ontnemen van het Nederlanderschap bij terroristische misdrijven (na strafrechtelijke veroordeling).
- Wijziging van de Rijkswet op het Nederlanderschap in verband met het intrekken van het Nederlanderschap in het belang van de nationale veiligheid (zonder tussenkomst rechter).
- Tijdelijke wet bestuurlijke maatregelen terrorismebestrijding.
- Wijziging van de Paspoortwet (Min BZK). Met deze wijziging wordt het mogelijk dat de Nederlandse identiteitskaart en paspoort van een persoon van rechtswege vervallen na het opleggen van een uitreisverbod
- Wijziging van de sociale zekerheidswetgeving, de Wet structuur uitvoeringsorganisatie werk en inkomen, de Wet Studiefinanciering 2000, de Wet studiefinanciering BES, de Wet tegemoetkoming onderwijsbijdrage en schoolkosten en de Algemene wet inkomensafhankelijke regelingen in verband met opname van een grondslag voor beëindiging van uitkeringen, studiefinanciering en tegemoetkoming bij deelname aan een terroristische organisatie
- Wet gericht op de invoering van een langdurige gedragsbeïnvloedende en vrijheid beperkende maatregel voor ter beschikking gestelden en zeden- en geweldsdelinquenten.
- Maatregel Inrichting Stelselmatige Daders (ISD) - onderzoeken of deze toepasbaar is voor extremisme/ terrorisme (Bezien wordt of de ISD-maatregel ook van toepassing kan worden verklaard op terugkeerders die worden veroordeeld voor enig misdrijf).

Ontwikkelen van, adviseren over én toepassen van maatregelen en interventies

- NCTV maakt afspraken met DGSenB/DJI en OM dat alle verdachten en veroordeelden voor een terroristisch misdrijf conform regelgeving direct geplaatst worden op een Terrorisme Afdeling (TA).
- De NCTV draagt bij aan het vormgeven van de kaders voor de strafrechtelijke aanpak in samenwerking met het OM en de Nationale Politie. Aanvullend versterkt de NCTV het tactische en operationele netwerk door samenwerkingsverbanden en informatie-uitwisseling te intensiveren, op te richten en te stimuleren.
- NCTV onderzoekt samen met partners hoe onderkende uitreizigers met een of meerdere nationaliteiten die zich aansluiten bij een terroristische strijdgroepering te melden bij de autoriteiten van die landen, voor zover dit past binnen de bestaande praktijk en niet in strijd is met nationale en internationale wet- en regelgeving
- NCTV ondersteunt en adviseert het lokaal bestuur in geval van vermoedelijke uitreis de directe omgeving van de uitreiziger te waarschuwen .
- NCTV maakt afspraken met de Raad van de Kinderbescherming dat in het geval van vermoedelijke uitreis waarbij een minderjarige betrokken is, kinderbeschermingsmaatregelen worden getroffen.
- NCTV maakt afspraken met IND dat onderkende uitreizigers met een niet EU nationaliteit ongewenst vreemdeling worden verklaard (voor het Schengengebied).
- NCTV, FIN, AIVD, CTI, OM en BZ zetten gezamenlijk in op plaatsing van alle onderkende uitreizigers die zich aansluiten bij een terroristische strijdgroepering op de nationale terrorismelijst (bevriezingslijst) (Sanctieregelingterrorisme 2007-II).
- De minister van Veiligheid en Justitie (namens deze de NCTV) verzoekt om weigering of vervallen verklaring van het paspoort van betrokkene. Daartoe worden de personalia - op aangeven van het casusoverleg - van personen waarvan het gegrond vermoeden bestaat dat zij willen uitreizen naar een terroristisch strijdgebied opgenomen in het Register Paspoortsignaleringen (RPS) en in het Nationaal Opsporingsregister (OPS).
- NCTV maakt procesafspraken met uitvoeringsorganisatie hoe onderkende uitreizigers cf. regels direct uit te schrijven uit de Basisregistratie Personen (BRP) en evt. uitkeringen, financiële toelagen en studiefinanciering te beëindigd.
- De NCTV maakt het kwaadwillenden moeilijker om aan aanslagmiddelen te komen. Hiervoor zet de NCTV de volgende instrumenten in wetgeving, informatiecampagne, informatiedeling en samenwerking (EU).
- Het project Terrorismefinanciering: een initiatief vanuit het FEC (Financieel Expertise Centrum) en de landelijk officier tegengaan Terrorismefinanciering van het Landelijk Parket (tevens projectleider) dat zich richt, in samenwerking met andere relevante organisaties, op het bestrijden van terrorismefinanciering.
- NCTV maakt duidingen van visumplichtige extremistische predikers die naar Nederland willen reizen en die mogelijk een bedreiging voor de openbare orde of nationale veiligheid kunnen zijn ten behoeve van de IND met het doel het visum te weigeren of in te trekken.
- NCTV traint samen met Buitenlandse Zaken en AIVD medewerkers op de Nederlandse posten in het buitenland ten behoeve van detectie mogelijk terroristen in proces consulaire bijstand.
- NCTV onderzoekt de juridische kaders voor uitwisselen informatie over personen in het casusoverleg en stelt een landelijk beschikbaar modelconvenant op samen met partners tbv casus overleggen jihadisme op lokaal niveau.

Versterken informatie-uitwisseling voor detectie en tegengaan reisbewegingen

- Wijziging van de Paspoortwet (Min BZK) Met deze wijziging wordt het mogelijk dat de Nederlandse identiteitskaart en paspoort van een persoon van rechtswege vervallen na het opleggen van een uitreisverbod .
- Identificeren van gaten in de huidige Europese (en internationale) informatie uitwisseling. Daartoe heeft de NCTV ingezet op een Europees plan om te komen tot verbetering van de Europese informatie-uitwisseling.
- Onderkende uitreizigers worden geplaatst in de internationale en Europese signaleringssystemen.
- Versterking detectie-en signaleringssystemen en (inter)nationale informatie-uitwisseling. Verhoogd gebruik en stijging in deling van informatie over jihadgangers met Europese en internationale systemen.
- Realisatie technische voorziening reisgegevens Travel Information Portal (TRIP) voor de ontsluiting en verwerking van bestaande stromen van passagiersgegevens op basis van bestaande wetgeving.
- Ingezet is op de totstandkoming van de EU PNR-richtlijn met hoogwaardige bescherming van persoonsgegevens van passagiers.
- Oprichting structureel multidisciplinair platform nationale diensten die zich bezighouden met informatie uitwisseling en reisbewegingen.
- Ten behoeve van een versterkte coördinatie op de uitvoering heeft de NCTV de CT-Infobox verzocht een integraal en actueel overzicht van de genomen maatregelen op persoonsniveau bij te houden.

Coördineren en faciliteren van lokale, nationale en internationale samenwerkingsverbanden

Opzetten (samenwerkings)structuur en verbeteren (operationele) informatie uitwisseling

- Verwerking van inlichtingenproducten en vervaardiging van analyseproducten waaronder het Dreigingsbeeld Terrorisme Nederland (DTN).
- Het monitoren en analyseren op trendniveau van dreigingen om anderen in staat te stellen te kunnen handelen (onder meer door uitbrengen Dreigingsbeeld Terrorisme Nederland (DTN) en diverse monitoring - en analyseproducten voor partners.
- De NCTV stelt adviseurs beschikbaar voor de betrokken gemeenten. De adviseurs ondersteunen gemeenten bij kennis en kunde over dreigingsniveau en het fenomeen jihadisme en de aanpak ervan.
- Intensivering van de samenwerking in de vreemdelingenketen door awareness bijeenkomsten te organiseren samen met de IND, COA en DT&V en de Vreemdelingenketen en het CT-netwerk op onderdelen te verbinden (bijvoorbeeld in I&R-straat).
- Het verlenen van consulaire bijstand in aangrenzende landen van personen die uit eigen beweging terug keren naar Nederland, omdat zij uit jihadistische beweging of terroristische organisatie willen stappen.

Intensivering van de internationale samenwerking en aanpak jihadgangers

- Om de internationale samenwerking en aanpak te versterken worden internationale afspraken gemaakt over het delen van informatie over concrete activiteiten. Hierbij vervult de NCTV de rol van trekker of deelnemer aan internationale gremia en werkgroepen.

Voorkomen aanwas door ondermijning aanbod propaganda en verhogen kwetsbare groepen

Coördineren en faciliteren van het netwerk aan partijen waarbinnen activiteiten ter voorkoming aanwas moet plaatsvinden

Opzetten structuur en verbetering informatie-uitwisseling

- Versterking van de vroegsignalering en monitoring van radicalisering, in het bijzonder gericht op wijken met de grootste kwetsbaarheid. Hiertoe heeft de NCTV ingezet op aanvullende ondersteuning voor scholen, actualiseren van de handreiking aanpak van radicalisering en terrorismebestrijding op lokaal niveau, opstellen van een handreiking terrorismegevolg-bestrijding, bundeling initiatieven rondom verbetering van risicotaxaties. delen van de woordvoerlingslijnen integrale aanpak radicalisering met gemeenten.
- Oprichting van een Nationaal Meldpunt radicalisering voor alle vormen van extremisme en terrorisme.
- Zorgen dat betrokken burgers radicaliserende, haatzaaiende jihadistische content op internet en social media kunnen melden en dat producenten en verspreiders van online jihadistische propaganda - en de digitale platforms die zij misbruiken - worden geïdentificeerd. Daarnaast wordt deze informatie actief gedeeld met de handelingsbevoegde instanties en relevante dienstverleners.

Versterken van het netwerk, lokaal en landelijk, gericht op ingrijpen bij radicalisering en deradicalisering

- Deskundigheidsbevordering in de uitvoering door o.a. gerichte voorlichting en het ontwikkelen van specialistische trainingen en vakopleiding, de ondersteuning van onderwijsinstellingen en het oprichten van een expertcentrum dat de informatiepositie van Rijk en gemeenten over maatschappelijke spanningen en radicalisering versterkt.
- Oprichting van een EXIT-faciliteit in Nederland, die personen die uit het jihadistische beweging of terroristische organisatie willen stappen onder strenge voorwaarden begeleidt
- Oprichten ondersteuningsfaciliteit waarmee familie/ vrienden van geradicaliseerde individuen en uitreizigers worden ondersteund
- Samenwerking met de islamitische gemeenschap door periodiek overleg met imams. Nederlandse imams en moskeebestuurders zijn medestanders in de strijd tegen de extremisten, die hun geloof kapen en hun kinderen misleiden en misbruiken.
- De ondersteuning bij het versterken van bestaande netwerken van lokale en landelijke sleutelfiguren. Sleutelfiguren die het alternatieve geluid uitdragen en stelling nemen tegen jihadisme worden ondersteund en getraind (mediatraining). Daarnaast worden sleutelfiguren die worden bedreigd, gesteund en waar nodig opgenomen in het stelsel Bewaken en Beveiligen.
- Het versterken van netwerken rond jongeren en hun opvoeders. Daarbij wordt een laagdrempelig aanbod van professionele opvoedondersteuning gestimuleerd.
- Het stimuleren van het maatschappelijke debat over de grenzen van de rechtstaat. Om de verspreiding van extremisme geen kans te geven, worden onderliggende waarden van de rechtsstaat gedeeld en uitgedragen.
- Het mobiliseren van maatschappelijke tegengeluiden en versterken van de weerbaarheid tegen radicalisering en spanningen. Het gaat hier onder andere om de ondersteuning van kleinschalige initiatieven.

Beschermen van personen, objecten en vitale processen tegen terroristische aanslagen

Verder professionaliseren van het Stelsel Bewaken en Beveiligen

- Evaluatie van het stelsel B&B: onderzoek naar de werking van de kritische (werk)processen die binnen en tussen de verschillende partners plaatsvinden en die direct van invloed zijn op de effectiviteit van het stelsel.
- Opstellen werkwijze Nationale Evenementen: Met de werkwijze wordt beoogd Nationale Evenementen veilig en ongestoord te laten verlopen, zonder afbreuk te doen aan het karakter van het evenement.

Intensivering aanpak solistische dreigers

- Project Solistische Dreigers: in 2010 is project 'solistische dreigers' gestart. Het project kent een drietal deeltrajecten: de pilot Dreigingsmanagement (PDM) waarmee is ingezet op een gestructureerde aanpak van verwarde en gefixeerde bedreigers. Daarnaast is onder jongeren de aandacht vergroot voor het feit dat bedreigen strafbaar is, om op die manier het aantal zogenaamde 'straattaalcreigers' te verminderen. Tot slot is er een aantal onderzoeken gestart met als doel de kennis over het fenomeen van solistische dreigers te vergroten, waaronder ook de ongekende dreigers.

Toekomstbestendig maken van de beveiligingscontroles op de luchthavens

- De kern van de activiteiten zijn er daarom gericht op de ontwikkeling van een Proof of Concept van een beveiligings-infrastructuur, die risk based security mogelijk maakt. Daarom is met Schiphol en fabrikanten gewerkt aan beveiligingsapparatuur die een op risico gebaseerde screening mogelijk maakt. Er zijn verschillende projecten gestart en begeleid die tot doel hebben om het beveiligingsproces,passagiersvriendelijker ,efficiënter en daarmee effectiever te maken.
- Creëren van (inter)nationaal draagvlak: Om draagvlak te creëren voor bovenstaande projecten zijn op regelmatige basis op initiatief van de NCTV presentaties gehouden voor o.a. partner organisaties, Europese Commissie, IATA en lidstaten tijdens overleggen, seminars, congressen en bezoeken. Dit draagvlak is nodig omdat voor een aantal pilots de regelgeving moest worden aangepast om nieuwe technologieën te kunnen toepassen.

Bijlage 3: Beleidsboom Nationale Veiligheid en crisisbeheersing

Taakveld Nationale veiligheid en crisisbeheersing
2011 -2015

Voorkomen en beperken van maatschappelijke ontwrichting door crisis

Verbeteren van het functioneren van het stelsel crisisbeheersing door coördinatie en vereenvoudigen van besluitvorming

Versterken nationale crisisorganisatie

- ***Vergroten efficiency en effectiviteit van de crisisbesluitvorming***
- ***Vergroten van het inzicht in risico's en capaciteiten***
  Met onder andere de Strategie Nationale Veiligheid onderzoeken welke dreigingen de nationale veiligheid in gevaar kunnen brengen en wat men daaraan kan doen.
- ***(Laten) ontwikkelen specifieke nationale crisisplannen***
  Mede op basis van de risico's in het NVP (voorheen de NRB) zijn er specifieke crisisplannen ontwikkeld
- ***Rijksbreed systeem van opleiden, trainen, oefenen, evalueren en leren.*** Onderdeel van een kwalitatief goede nationale crisisorganisatie zijn professioneel toegeruste crisisfunctionarissen en een sterk en flexibel (rijksbreed) crisisnetwerk. Hiertoe heeft de minister de Nationale Academie voor Crisisbeheersing (NAC) in het leven geroepen
- ***Realiseren voorzieningen om continuïteit van de rijkscrisisfunctie te waarborgen***
- ***Onderhoud Nationaal Crisiscentrum (NCC)***
- ***Onderhoud opgeschaald Landelijk Operationeel Coördinatiecentrum (LOCC)***

Versterken presterend vermogen veiligheidsregio's en Caribisch Nederland

- ***Evalueren van de Wet veiligheidsregio's***
  Een evaluatieonderzoek naar de Wet veiligheidsregio's om te bezien in hoeverre de wet in de praktijk aan de verwachtingen voldoet wat betreft het functioneren van het stelsel
- ***Verbeteren van de regelgeving voor veiligheidsregio's***
  Mede op basis van de uitkomsten van de evaluatie op de Wet Veiligheidsregio's de regelgeving aanpassen en actualiseren.
- ***Verbeteren van de ondersteuning van veiligheidsregio's***
  Oprichting Instituut Fysieke Veiligheid (IFV).
- ***Brede Doeluitkering (BDUR) aan de veiligheidsregio's en de herijking en actualisatie daarvan***
- ***Versterken brandweer*** door:
  a) de regionalisering.
  b) onderzoek naar opkomsttijden en variabele voertuigbezetting.
  c) verbetering van de brandweerstatistiek (door onderzoek).
  d) convenant ter verbetering van het brandweeronderwijs.
- ***Versterken Geneeskundige Hulpverleningsorganisatie (GHOR) in de Regio***
  a) Vastleggen bekwaamheidseisen GHOR-functionarissen in Bpv
  b) Afspraken over de rol van het Rode Kruis bij rampen en crisis en over de Grootschalige Geneeskundige Bijstand
- ***Versterken crisisbeheersing Caribisch Nederland***
  Door invoering en bevorderen van de implementatie van wet- en regelgeving crisisbeheersing en brandweerzorg Caribisch Nederland.

Versterken samenwerking

- ***Versterking van de aansluiting Rijk - regio***
  Versterking van de bovenregionale samenwerking en de samenwerking tussen regio's
  - Het realiseren van een opschalingstructuur waarin helder is opgenomen op welk moment de Rijksoverheid een taak heeft en de wettelijke verankering daarvan
  - Instellen c.q. versterken van Crisis Expert Teams
  - Het bevorderen dat de Nationale Risicobeoordeling en de risicoprofielen van de veiligheidsregio's beter op elkaar worden afgestemd.
- ***Bevorderen samenwerking door gezamenlijke vaststelling en uitvoering prioriteiten en doelstellingen***
- ***Versterking van de civiel-militaire samenwerking (VCMS)*** door
  a) Onderzoek naar kansrijke mogelijkheden
  b) Ontwikkelen catalogus
  c) Instellen taskforce OTOTEL
- ***Versterken themagerichte aanpak***
  - Het ontwikkelen van producten voor grootschalige evacuaties in het project Grootschalige Evacuatie
  - Het versterken van de organisatorische voorbereiding op de 'nafase' met specifieke aandacht voor de opvang en zorg voor getroffenen en herstel en wederopbouw
  - Het versterken van de CBRN-respons door de multidisciplinaire samenwerking bij CBRN te vergroten en het versterken van (generieke) CBRN capaciteiten in het kader van het EU Actieplan
- ***Versterking samenwerking Reddingsbrigade Nederland en de veiligheidsregio's***
- ***Bevorderen van de internationale samenwerking*** door onder andere te participeren in Europese activiteiten en bij te dragen aan EU mechanisme, NATO en bilateraal

Versterken informatievoorziening en crisiscommunicatie

- ***Streven naar uniformiteit***
  Om de uniformiteit in de informatievoorziening en crisiscommunicatie te bevorderen, heeft de minister VenJ overleg met de besturen van de veiligheidsregio's
- ***Beter alarmeren en informeren*** door de implementatie van alarmmiddel NL-Alert en het verhogen van het bereik ervan
- ***Verbeteren van de risico- en crisiscommunicatie***
  - Verder ontwikkelen van communicatiemiddelen: als 0800-1351 en www.crisis.nl
  - De oprichting van een Nationaal Kernteam Crisiscommunicatie (NKC)
  - Het inzetbaar maken van een bovenregionaal expertteam crisiscommunicatie voor ondersteuning van de veiligheidsregio's.
- ***Versterken van de operationele en bestuurlijke informatievoorziening bij rampen en crises*** door het invoeren van netcentrisch werken met een Landelijk Crisismanagement Systeem (LCMS)
- ***Verbeteren van de noodcommunicatie*** door zorg te dragen voor een functionerend noodcommunicatiesysteem als geen gebruik gemaakt kan worden van de reguliere communicatiemiddelen.

Behoud historisch erfgoed

- ***Bevorderen oprichting Nederlands Veiligheids Instituut (NVI)***

Vergroten weerbaarheid vitale belangen

Versterken weerbaarheid ten behoeve van de nationale veiligheid

- ***Herijken interdepartementale strategie en beleid met betrekking tot de bescherming van vitale infrastructuur.***
- ***Ontwikkelen in publiek-private samenwerking van roadmaps***
- ***Stroomlijnen van de overheidsinzet*** door het zoveel mogelijk samenbrengen van specifieke initiatieven en instrumenten (bijvoorbeeld ATb systeem, crisisafspraken)
- ***Signalering van mogelijke nieuwe vitale processen.***
- ***Aanbieders van vitale producten en diensten aan laten sluiten op de nationale crisisbesluitvorming*** inclusief de deelname aan opleiden, trainen en oefenen.

Versterken economische veiligheid

- ***Ex ante analyses van vitale sectoren***
  Beoordelen van het huidige overheidsinstrumentarium (de weerstand) voor het beschermen van de nationale veiligheid bij buitenlandse investeringen in als vitaal aan te merken sectoren
- ***Risicoverkenning op aanbesteding en inhuur***
  Op basis van een risicoverkenning wordt uitvoering gegeven aan maatregelen gericht op risico's voor de nationale veiligheid die samenhangen met aanbesteding en inhuur.
- ***Verkenning van het bredere thema economische veiligheid***
  door onder andere een verkenning meerwaarde generieke investeringstoets en een verkenning (probleemschets en handelingskader) digitale economische spionage

Verhogen weerbaarheid Rijk tegen spionage

- ***Zelfanalyse Spionage***
  Het uitvoeren van een zelfevaluatie van de Rijksoverheid naar gevoeligheid kernbelangen voor spionage en de implementatie van de aanbevelingen hieruit
- ***Monitoring voortgang implementatie aanbevelingen zelfanalyse***
  Onderzoek naar de mate waarin aanbevelingen uit de evaluatie zijn doorgevoerd.

Bijlage 4: Beleidsboom Cybersecurity

Taakveld Cybersecurity 2011-2015

Veiligheid en vertrouwen in een open en vrije digitale samenleving

Versterken integrale aanpak cybersecurity door publieke en private partijen

Duidelijke verdeling van taken, verantwoordelijkheden en bevoegdheden

Oprichten en versterken van NCSC
Wens van het kabinet was dat publieke en private partijen, op basis van hun eigen taken en binnen de wettelijke mogelijkheden, informatie, kennis en expertise in een op te richten Nationaal Cyber Security Centrum bij elkaar brengen

Oprichten Cyber Security Raad
Oprichten van een Cyber Security Raad, waarin op strategisch niveau vertegenwoordigers van alle relevante partijen zitting hebben en waarin afspraken worden gemaakt over uitvoering en uitwerking van deze strategie.

Bouwen aan coalities voor vrijheid, veiligheid en vrede in het digitale domein

Versterkt participeren in multistakeholder evenementen (Cyberspace conferenties en het IGF)
Of het nu gaat om standaarden in ICT, fundamentele rechten, de bestrijding van cybercrime of het bevorderen van de internationale rechtsorde in cyberspace, een internationale beleidsagenda is belangrijk onderdeel van een geïntegreerd nationaal cybersecuritybeleid.

Nederland zorgt voor adequate en actuele dreiging- en risicoanaalyses

Gezamenlijk integraal beeld van de actuele dreigingen en kwetsbaarheden van ICT

Risico's in kaart brengen van legacy systemen in vitale processen en diensten
Legacy systemen zijn systemen die zijn gebouwd met technologie die niet of nauwelijks meer wordt ondersteund door externe leveranciers en/of de eigen organisatie

Coördineren, faciliteren, samenvoegen en delen dreigings- en risicoanalyses
Naast het in kaart brengen van risico's is het vergaren van inzichten binnen het cyberdomein vanuit andere partijen een belangrijke taak. Daarom heeft de NCSC ook een coördinerende en faciliterende rol om informatie te verkrijgen voor een integraal dreigingsbeeld

Versterken van onderzoeks- en analysecapaciteit

NCSC uitbreiden met meer analisten en inventariseren van samenwerkingsmogelijkheden
Om de onderzoeks- en analysecapaciteit te verwerken, heeft NCSC ingezet op de inzet van meer analisten. Ook wil NCSC samenwerkingsmogelijkheden met inlichtingendiensten inventariseren.

Oprichten van een nationaal detectie- en responsnetwerk voor de Rijksoverheid en overige vitale sectoren
In samenwerking met haar partners richt het NCSC een nationaal detectie- en responsnetwerk in voor de Rijksoverheid en overige vitale sectoren.

Versterken van de weerbaarheid tegen ICT-verstoringen en Cyberaanvallen

Vergroten en ontwikkelen cybersecurity experts

Ontwikkelplan gericht op kwalificering en certificering
Voor de beroepsgroepen en het onderwijsveld wordt een plan ontwikkeld voor het uitbreiden van het aandeel van ICT-veiligheid in de daarvoor geschikte opleidingen

Oprichten PPS Taskforce Cybersecurity
In de tweede Cybersecurity strategie is als actie opgenomen om een PPS taskforce Cybersecurity in te stellen, die zich richt op advisering van het cybersecurity onderwijsaanbod

Stimuleren onderzoek Cybersecurity

Afstemmen onderzoeksprogramma's via de research cyber security agenda
Het kabinet zal onderzoeksprogramma's van in ieder geval de overheid en waar mogelijk van wetenschappelijke onderzoekscentra en het bedrijfsleven beter op elkaar afstemmen in de Nationale Cyber Security Raad.

Ondersteunen bij aanboren onderzoeksgelden
De NCTV levert een bijdrage vanuit een coördinerende taak om te faciliteren bij het verkrijgen van financiële middelen voor onderzoeken

Lanceren van cybersecurityplatform voor nieuwe en gevestigde bedrijven, studenten en onderzoekers.

Vergroten kennis over en veiligheidsbewustzijn van ICT-producten en diensten bij de gebruikers (burgers en bedrijven)

Beter beschikbaar maken van informatie over veiligheid van ICT-producten en diensten bij de gebruiker.
Vanuit het NCSC wordt actief bijgedragen aan de bewustwording van publiek, overheid en het bedrijfsleven via publicaties, de website en het delen van concrete expertise met belanghebbende partijen.

Publicatie kennisdocumenten en beveiligingsadviezen
Het NCSC publiceert kennisdocumenten die informatie en inzicht bieden over cyber aanval-technieken, preventie, kwetsbaarheden en dreigingen en daarnaast ook specifieke tools voor het bieden van concrete handelingsperspectieven

Introductie Alert Online
Alert Online is een jaarlijkse campagne om mensen en organisaties bewust te maken van hun internet- en mobiel gebruik en de risico's die dit met zich meebrengt

Lancering Veiliginternetten.nl
De website van Veilig Internetten (www.veiliginternetten.nl) is het actuele kanaal met informatie over veilig internetten voor burgers en het MKB

Bewerkstelligen dat publieke en private leveranciers voldoen aan minimum eisen op het gebied van continuïteitsdienstverlening en spionage

Stimuleren minimale ICT beveiligingsstandaarden op basis van good practices
De overheid gaat samen met de vitale organisaties het gebruik van de gangbare minimale ICT beveiligingsstandaarden op basis van good practices stimuleren.

Beschikbaar stellen handleiding Kwetsbaarhedenanalyse Spionage
Voor bedrijven is er een handleiding Kwetsbaarhedenanalyse Spionage beschikbaar waarmee zij hun weerbaarheid tegen spionage kunnen vergroten

Inzetten voor internationale afspraken over veilige hard- en software en zorgen dat Nederland actief deelneemt in het Internet Governance Forum

Haalbaarheidsonderzoek gescheiden netwerk vitaal
Er wordt een verkenning uitgevoerd in hoeverre het realiseren van een gescheiden ICT-netwerk voor (publieke en private) vitale processen op technisch en organisatorisch vlak mogelijk en wenselijk is.

Versterken responscapaciteit om ICT-verstoringen en cyberaanvallen te kunnen pareren

Duidelijke crisis structuur bij cyberincidenten

Opstellen Nationaal Crisisplan ICT
De NCTV levert in 2011 het Nationaal Crisisplan ICT op (NCP-ICT). Onderdeel hiervan is een oefenplan, dat zowel nationale als internationale oefeningen op elkaar afstemt.

ICT Response Board onderbrengen bij NCSC
De ICT Response Board (IRB), een publiek-private samenwerking die de crisisbesluitvormings-organisaties advies geeft over maatregelen om grootschalige ICT-verstoring tegen te gaan of te bestrijden

Versterken internationale samenwerking CERT-organisaties
Internationaal zet NCSC in op de versterking van de samenwerking bij de operationele respons tussen de CERT-organisaties in Europa

Inventariseren accreditatie bedrijven als digitale brandweer
Het gaat daarbij om cybersecurity-dienstverleners die andere partijen kunnen bijstaan bij digitale incidenten.

Informeren van de burgers en bedrijfsleven bij cyberincidenten

Uitbreiding van het Alerteringsysteem Terrorisme-bestrijding (ATb) met cyber component en deze beoefenen

Informatie verspreiden via Veiliginternetten.nl

Stimuleren kennis(deling) en oefening

De NCSC levert een bijdrage aan een trainingsprogramma voor respons op grootschalige ICT-incidenten.
Daarnaast ook organisatie en deelname aan grote en kleine oefeningen.

Bijlage 5 : Overzicht beleidsinstrumenten contraterrorisme 2012 -2015

Nr.	Doelstelling en instrumenten	Realisatie en werkbaarheid[82]	Specifiek uitgevoerde evaluatie(s) doeltreffendheid en doelmatigheid beleidsinstrument[83]
Verstoren van dreigingen en verijdelen aanslagen door beperken toegang tot middelen en tegengaan van reisbewegingen			
Ontwikkelen, ondersteunen en beschikbaar stellen van instrumenten voor partners			
Aanjagen van en bijdragen aan wijzigingen in wet- en regelgeving			
1.	Wijziging van de Rijkswet op het Nederlanderschap ter verruiming van de mogelijkheden voor het ontnemen van het Nederlanderschap bij terroristische misdrijven (na strafrechtelijke veroordeling).	De wet was in periode van evaluatie nog niet gerealiseerd. Wel zijn werkzaamheden uitgevoerd in verband met het consultatieproces. Het voorstel tot wijziging van de Rijkswet op het Nederlanderschap ter verruiming van de mogelijkheden voor het ontnemen van het Nederlanderschap bij terroristische misdrijven is op 31 maart 2016 in werking getreden[84].	*In de evaluatie van de CT strategie zijn de ingezette beleidsinstrumenten, zoals opgenomen in deze tabel, integraal geëvalueerd.* *Er zijn geen specifieke evaluaties van de verschillende instrumenten.*
2.	Wijziging van de Rijkswet op het Nederlanderschap in verband met het intrekken van het Nederlanderschap in het belang van de nationale veiligheid.	De wet was in periode van deze evaluatie nog niet gerealiseerd. Wel zijn werkzaamheden uitgevoerd in verband met het consultatieproces. De wet is op 1 maart 2017 in werking getreden[85].	
3.	Tijdelijke wet bestuurlijke maatregelen terrorismebestrijding. Deze wet	De wet was in periode van deze evaluatie nog niet gerealiseerd. Wel zijn werkzaamheden uitgevoerd in verband	In de wet is bepaald dat de wet na drie jaar wordt geëvalueerd. Het parlement wordt

82 De hieronder beschreven informatie over de realisatie en werkbaarheid van de verschillende instrumenten is - tenzij met een aparte voetnoot aangegeven – afkomstig uit de Voortgangsrapportages Actieprogramma Integrale Aanpak Jihadisme 1 t/m 6.
83 Hier worden alleen beschikbare evaluaties genoemd die uitspraken doen over de doeltreffendheid en/ of doelmatigheid van het specifieke instrument; als die er niet zijn blijft cel leeg.
84 Staatscourant, nr. 33997, 30 juni 2016.
85 Staatsblad van het Koninkrijk der Nederlanden, nr. 2017 67, 28 februari 2017.

	introduceert nieuwe bestuurlijke bevoegdheden in het kader van terrorismebestrijding, zijnde: contactverbod, gebiedsverbod, meldplicht, uitreisverbod en intrekken of weigeren van vergunningen, beschikkingen, besluiten en subsidies.	met het consultatieproces. Op 1 maart 2017 is de tijdelijke wet bestuurlijke maatregelen in werking getreden[86].	van de uitkomsten van deze evaluatie op de hoogte gesteld.
4.	Wijziging van de Paspoortwet (Min BZK). Ter ondersteuning van een uitreisverbod uit de Twbmt is ook de Paspoortwet gewijzigd. Hierin wordt geregeld dat paspoorten en de Nederlandse identiteitskaarten van rechtswege vervallen bij het opleggen van een uitreisverbod. Tevens wordt het mogelijk om in dit geval betrokkene een vervangend identiteitsbewijs te geven. Daarmee mag alleen binnen Schengen worden gereisd.	De wet was in periode van deze evaluatie nog niet gerealiseerd. Wel zijn werkzaamheden uitgevoerd in verband met het consultatieproces. Op 1 maart 2017 is de tijdelijke wet bestuurlijke maatregelen in werking getreden[87].	
5.	Wijziging van de sociale zekerheids wetgeving, de Wet structuur uitvoerings-organisatie werk en inkomen, de Wet Studiefinanciering 2000, de Wet studiefinanciering BES, de Wet tegemoetkoming onderwijsbijdrage en schoolkosten en de Algemene wet inkomensafhankelijke regelingen in verband met opname van een grondslag voor beëindiging van uitkeringen,	De wet is als hamerstuk aangenomen door de Eerste Kamer[88]. De inwerkingtreding wordt voorzien op 1 oktober 2017. Sinds november 2013 zijn circa 95 (peildatum 2 maart 2016) sociale uitkeringen stopgezet van onderkende Nederlandse of aan Nederland te relateren personen die met jihadistische intenties naar Syrië/Irak zijn gereisd. Dit gebeurt mede naar aanleiding van een uitschrijving uit het BRP of door bemiddeling van de CT-infobox. Het wetsvoorstel tot het stopzetten van uitkeringen, toeslagen en studiefinanciering wordt naar verwachting in de zomer aan de Raad van State aangeboden.	

86 Staatsblad van het Koninkrijk der Nederlanden, nr. 2017 65, 27 februari 2017. & nr. 2017 51, 22 februari 2017.
87 Staatsblad van het Koninkrijk der Nederlanden, nr. 2017 65, 27 februari 2017. & nr. 2017 58, 22 februari 2017.
88 Staatsblad van het Koninkrijk der Nederlanden, nr. 2017 78, 9 maart 2017.

	studiefinanciering en tegemoetkoming bij deelname aan een terroristische organisatie. Deze wet voorziet in een uniforme beëindiginggrond voor het stopzetten van uitkeringen/financiële toelagen e.d. op gronden van een bedreiging nationale veiligheid (Min SZW).		
6.	Wet gericht op de invoering van een langdurige gedragsbeïnvloedende en vrijheid beperkende maatregel voor ter beschikking gestelden en zeden- en geweldsdelinquenten.	Het wetsvoorstel uit maatregel 3c is op 24 november 2015 door de Eerste Kamer aangenomen. Hiermee wordt het mogelijk om de toezichttermijnen op onder andere voormalige tbs-ers en geweldsdelinquenten te verlengen. Met deze regeling wordt het mogelijk om, indien nodig, levenslang toezicht te houden op zeden- en geweldsdelinquenten. Op 1 januari 2017 is de wet in werking getreden[89].	
7.	Maatregel Inrichting Stelselmatige Daders (ISD) – onderzoeken of deze toepasbaar is voor extremisme/ terrorisme (Bezien wordt of de ISD-maatregel ook van toepassing kan worden verklaard op terugkeerders die worden veroordeel voor enig misdrijf).	In 2014 communiceerde de NCTV naar de TK: Op strafrechtelijk gebied onderzoek ik (red.: Minister VenJ) of het mogelijk is om naar analogie van het programma-aanbod van de 'Inrichting Stelselmatige Daders (ISD-maatregel)' maatregelen te ontwikkelen die zien op gedragsverandering bij terugkeerders[90]. De NCTV heeft tijdens de beleidsdoorlichting aangegeven dat deze maatregel niet geschikt bleek voor categorale toepassing in de aanpak van jihadisme. Afhankelijk van de casus zijn situaties denkbaar dat er toch aanknopingspunten zijn voor toepassing van de ISD-maatregel (casus op maat). In de gevallen dat dit mogelijk effectief kan zijn, kan de ISD-maatregel volgens de NCTV dus toegepast worden.	

89 Staatsblad van het Koningkrijg der Nederlanden, nr. 2016 493,14 december 2016.& nr. 2015 460, 4 december 2015.
90 Kamerstuk 29754 nr. 272. 24 november 2014.

Ontwikkelen van, adviseren over én toepassen van maatregelen en interventies			
8.	NCTV maakt afspraken met DGSenB/DJI en OM dat alle verdachten en veroordeelden voor een terroristisch misdrijf conform regelgeving direct geplaatst worden op een Terroristen Afdeling (TA).	Verdachten en veroordeelden voor een terroristisch misdrijf worden conform huidige regelgeving direct geplaatst op TA. De capaciteit heeft tot op heden aan de vraag kunnen voldoen en uitbreiding is indien nodig snel te realiseren. Ook is in de voortgangsrapportages opgenomen dat nog onderzoek wordt gedaan of het regime op deze afdelingen meer op maat kan worden vormgegeven om terugkeer in de maatschappij van deze gedetineerden beter te kunnen begeleiden. In een kamerbrief is het volgende opgenomen: de uitkomsten van dit onderzoek hebben mij (red.: Staatssecretaris VenJ) opnieuw bevestigd dat met de huidige inrichting van de TA en de concentratie van TA-gedetineerden op een speciale afdeling het beoogde doel wordt bereikt. Daarnaast is in de brief aangegeven dat het noodzakelijk is om meer maatwerk mogelijk te maken dan thans het geval is. Een essentiële voorwaarde is dat voor per individu een accurate beoordeling plaatsvindt van het verspreidings- en veiligheidsrisico[91]. In de vierde voortgangsrapportage is opgenomen dat een eerste versie van het beoordelings-instrument voor een dergelijke beoordeling beschikbaar is.	
9.	De NCTV draagt bij aan het vormgeven van de kaders voor de strafrechtelijke aanpak in samenwerking met het OM en de Nationale Politie. Aanvullend versterkt de NCTV het tactische en operationele netwerk door samenwerkingsverbanden en informatie-uitwisseling te intensiveren, op te richten en te stimuleren.	In de voortgangsrapportages worden de ontwikkelingen van de strafrechtelijke aanpak beschreven. Zo is in diverse voortgangsrapportages door het OM aangegeven hoe de strafrechtelijke aanpak uitwerking heeft en is inzage gegeven in het aantal strafrechtelijke onderzoeken naar terroristische misdrijven.	

91 Kamerbrief, 3 juli 2015, Toezeggingen terroristenafdelingen.

10.	NCTV onderzoekt samen met partners hoe onderkende uitreizigers met een of meerdere nationaliteiten die zich aansluiten bij een terroristische strijdgroepering te melden bij de autoriteiten van die landen, voor zover dit past binnen de bestaande praktijk en niet in strijd is met nationale en internationale wet- en regelgeving.	In samenwerking met de partners in de CT-keten en in samenhang met aanpalende maatregelen, is uitgewerkt hoe en waar de bestaande informatie-uitwisselingspraktijk van politie- en inlichtingendiensten met counterparts in derde landen kunnen worden aangevuld dan wel versterkt, in het bijzonder ten aanzien van het doormelden van de paspoortsignaleringen naar landen van de tweede nationaliteit. Hierbij is zoveel als mogelijk gebruik gemaakt van de reeds bestaande instrumenten en kanalen. Het OM en de politie werken bij de aanpak van terroristische misdrijven nauw samen met internationale partners. In dat kader zijn er namen van uitreizigers gedeeld met onder meer de EU-landen, Turkije en de Verenigde Staten.	
11.	NCTV ondersteunt en adviseert het lokaal bestuur in geval van vermoedelijke uitreis de directe omgeving van de uitreiziger te waarschuwen (onder meer onderdeel van de handreiking lokaal).	Personen die geradicaliseerd zijn en die in beeld zijn, worden besproken in een multidisciplinair casusoverleg in het lokale domein. De betrokken partijen bepalen daar de meest effectieve aanpak. Het informeren van de omgeving door de lokale overheid kan een onderdeel van de aanpak zijn. Deze maatregel is gerelateerd aan maatregel 30 van het Actieprogramma Integrale Aanpak Jihadisme, ondersteuning lokale aanpak. Sinds het begin van de uitvoering van het Actieprogramma heeft de lokale overheid enkele malen de omgeving geïnformeerd over een op hande zijnde uitreis. In een aantal gevallen heeft dit bijgedragen aan het voorkomen van uitreis.	
12.	NCTV maakt afspraken met de Raad van de Kinderbescherming dat in het geval van vermoedelijke uitreis waarbij een minderjarige betrokken is, kinderbeschermingsmaatregelen worden getroffen.	Wanneer minderjarigen die door hun ouders zijn meegenomen naar ISIS strijdgebieden of wanneer kinderen in ISIS strijdgebied worden geboren uit Nederlandse ouders naar Nederland terugkeren volgt altijd een melding bij de Raad voor de Kinderbescherming. De Raad voor de Kinderbescherming bekijkt of reeds sprake is van hulpverlening aan de minderjarige en besluit indien nodig tot	

		het instellen van een raadsonderzoek. Tegelijkertijd wordt door zorg- en veiligheidspartners in een multidisciplinair casusoverleg een behandelplan opgesteld dat de veilige ontwikkeling van het kind moet waarborgen en eventuele veiligheidsrisico's moet tegengaan. In de periode februari 2013 tot 2 februari 2016 zijn 65 aan jihadisme gerelateerde unieke kindzaken door de Raad voor de Kinderbescherming in onderzoek genomen. Van die 65 minderjarigen waren er 28 individuele potentiële vertrekkers en 37 kinderen in gezinsverband (peildatum 2 maart 2016).	
13.	NCTV maakt afspraken met IND dat onderkende uitreizigers met een niet EU nationaliteit ongewenst vreemdeling worden verklaard (voor het Schengengebied).	Deze maatregel wordt toegepast op vreemdelingen die een Nederlandse verblijfsstatus hebben en die op basis van een ambtsbericht van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) of Militaire Inlichtingen- en Veiligheidsdienst (MIVD) in verband kunnen worden gebracht met jihadisme of een (potentiële) uitreis in dit kader en waarbij de AIVD of MIVD tevens heeft geconcludeerd dat zij een gevaar zijn voor de nationale veiligheid. Sinds maart 2013 is de IND in circa 15 gevallen (peildatum 9 maart 2016) overgegaan tot het treffen van vreemdelingrechtelijke maatregelen op onderkende uitreizigers met een niet-EU nationaliteit. Het gaat daarbij om verblijfsbeëindiging, het opleggen van een inreisverbod of ongewenst verklaring.	
14.	NCTV, FIN, AIVD, CTI, OM en BZ zetten gezamenlijk in op plaatsing van alle onderkende uitreizigers die zich aansluiten bij een terroristische strijdgroepering op de nationale terrorismelijst (bevriezingslijst) (Sanctieregelingterrorisme 2007-II).	Sinds december 2013 heeft de Minister van BZ in overeenstemming met de Ministers van Financiën en VenJ 29 personen toegevoegd aan de nationale terrorismelijst (peildatum 14 maart 2016).	

15.	De minister van Veiligheid en Justitie (namens deze de NCTV) verzoekt om weigering of vervallen verklaring van het paspoort van betrokkene. Daartoe worden de personalia – op aangeven van het casusoverleg – van personen waarvan het gegrond vermoeden bestaat dat zij willen uitreizen naar een terroristisch strijdgebied opgenomen in het Register Paspoortsignaleringen (RPS) en in het Nationaal Opsporingsregister (OPS). Doel van de signalering in RPS en OPS is het enerzijds innemen en (door de burgemeester) vervallen verklaren van uitgegeven paspoorten en het anderzijds voorkomen nieuwe reisdocumenten worden uitgegeven.	Sinds december 2013 zijn ongeveer 235 (peildatum 1 maart 2016) verzoeken gedaan door de Minister van Veiligheid en Justitie ter weigering of vervallen verklaring van het paspoort. Er wordt doorlopend gekeken naar de noodzaak van het voortduren van de paspoortmaatregel. Wanneer het gegronde vermoeden niet langer bestaat, wordt de signalering opgegeven. Dit is in ongeveer 25 gevallen gebeurd.	
16.	NCTV maakt procesafspraken met uitvoeringsorganisatie hoe onderkende uitreizigers cf. regels direct uit te schrijven uit de Basisregistratie Personen (BRP) en evt. uitkeringen, financiële toelagen en studiefinanciering te beëindigd.	De personalia van onderkende uitreizigers wordt, indien mogelijk, gedeeld met de gemeente waarin zij staan ingeschreven. De betreffende gemeente draagt zorg voor uitschrijving uit het BRP bij onderkende uitreis, zodat eventuele financiële toelagen en studiefinanciering worden stop gezet. Sinds november 2013 zijn circa 95 (peildatum 2 maart 2016) sociale uitkeringen stopgezet van onderkende Nederlandse of aan Nederland te relateren personen die met jihadistische intenties naar Syrië/Irak zijn gereisd. Dit gebeurt mede naar aanleiding van een uitschrijving uit het BRP of door bemiddeling van de CT-infobox.	

17.	De NCTV maakt het kwaadwillenden moeilijker om aan aanslagmiddelen te komen. Hiervoor zet de NCTV de volgende instrumenten in: • Wetgeving: De beschikbaarheid van grondstoffen voor zelfgemaakte explosieven is door de EU in 2013 met verordening 98/2013 beperkt. Tevens moeten bedrijven verdachte transacties, verdwijningen en diefstal melden bij de overheid. • Informatiecampagne: Om relevante sectoren en eindgebruikers bewust te maken van de risico's van grondstoffen voor explosieven wordt de informatiecampagne over de wetgeving geïntensiveerd en verbreed. Tevens is er aandacht voor het verhogen van de kennis- en informatiepositie over aanslagmiddelen bij diverse partners. • Informatiedeling: De informatiedeling, opsporing en inlichtingenverwerving inzake (pogingen tot) verwerving van aanslagmiddelen worden geïntensiveerd, met name wat betreft de verkrijgbaarheid van vuurwapens in het criminele circuit en de vermenging van dit circuit met jihadistische netwerken. • Samenwerking (EU): In EU-verband wordt gesproken over aanpassing van de Europese vuurwapenrichtlijn ten	Wetgeving: De NCTV heeft de Europese verordening vertaald in Nederlandse wetgeving – de Wet Precursoren voor explosieven. De Wet Precursoren voor Explosieven is sinds 1 juni 2016 van kracht[92]. NCTV is de verantwoordelijke autoriteit, Inspectie Leefomgeving en Transport is verantwoordelijk voor de vergunningverlening en toezicht en de Nationale Politie (Centrex) is verantwoordelijk voor de uitvoer van het Meldpunt Verdachte Transacties. Informatiecampagne: Sinds augustus 2014 worden partners, ondernemers en particulieren geïnformeerd over de consequenties van de wet en de wijze waarop deze impact heeft op hun handelen. Om relevante sectoren en eindgebruikers bewust te maken van de risico's van grondstoffen voor explosieven is eind 2015 een tweede informatiecampagne gestart en is een E-learning tool opgeleverd. Informatiedeling: Als vervolg op het Landelijke Platform Vuurwapens is besloten tot de oprichting van een nieuw netwerk tussen de operationele diensten van de politie, KMar, douane en OM. Ook het ministerie van Veiligheid en Justitie zal hierbij aansluiten. Dit zwaardere netwerk versterkt de informatie uitwisseling tussen de operationele diensten en de internationale samenwerking om zo slagvaardiger de verspreiding en het gebruik van illegale wapens tegen te gaan. Ook is in JBZ-verband besloten de grenscontroles binnen het bestaande wetgevingskader te intensiveren en tot een betere uitwisseling van inlichtingen te komen. Samenwerking (EU): Na incidenten met vuurwapens, is binnen de EU in 2015 de aanpak van vuurwapens als prioriteit	

92 De Europese Verordening voor Precursoren voor Explosieven (http://eur-lex.europa.eu/legal-content/NL/ALL/?uri=celex:32013R0098)

	behoeve van strengere Europese standaarden. Op het gebied van nieuwe modus operandi wordt proactief samengewerkt met andere landen en de EU.	benoemd. Mede op aandringen van Nederland, heeft de Europese Commissie een verordening omtrent de deactivatie van vuurwapens aangenomen eind 2015. In EU-verband wordt gesproken over aanpassing van de Europese vuurwapenrichtlijn ten behoeve van strengere Europese standaarden. Tevens heeft de Europese Commissie eind 2015 een actieplan opgesteld voor de bestrijding van de illegale handel in en het gebruik van vuurwapens en explosieven. Ten slotte hebben politie- en justitievertegenwoordigers uit 25 EU-landen, de Verenigde Staten, Australië en Noorwegen, Eurojust en Europol recent afgesproken om anonieme, illegale marktplaatsen op het internet aan te pakken.	

18.	De NCTV en het Ministerie van Financiën hebben een gezamenlijke beleidsverantwoordelijkheid op het thema Terrorismefinanciering. Het project Terrorismefinanciering is een initiatief vanuit het FEC (Financieel Expertise Centrum) en de landelijk officier tegengaan Terrorismefinanciering van het Landelijk Parket (tevens projectleider) dat zich richt, in samenwerking met andere relevante organisaties, op het bestrijden van terrorismefinanciering.	Het FEC is in samenwerking met andere relevante organisaties per 1 februari 2015 een project gestart dat zich richt op informatie-uitwisseling op het gebied van terrorismefinanciering. Dit project heeft als doel om financiële netwerken in kaart te brengen van uitreizigers en andere relevante personen om op die wijze inzicht te verkrijgen in terroristische netwerken, groeperingen of (rechts)personen, terrorismefinanciering en zogenoemde facilitatoren. Op basis van dat verkregen inzicht kunnen passende preventieve en repressieve maatregelen genomen worden.	
19.	NCTV maakt duidingen van visumplichtige extremistische predikers die naar Nederland willen reizen en die mogelijk een bedreiging voor de openbare orde of nationale veiligheid kunnen zijn ten behoeve van de IND met het doel het visum te weigeren of in te trekken.	De NCTV houdt op basis van open bronnen actief een alerteringslijst bij van sprekers en/of referenten die extra aandacht vragen in de beoordeling. De NCTV kijkt doorlopend naar extremistische sprekers en ook specifiek naar personen of organisaties die betrokken zijn bij het fundamentalistische lezingencircuit, om vroegtijdig en proactief de komst van extremistische sprekers te kunnen onderkennen.	

		Sinds februari 2015 is van acht personen de visumaanvraag afgewezen of is het reeds verleende visum, afgegeven door Nederland of een Schengen lidstaat, ingetrokken wegens aanzetten tot haat en/of geweld (peildatum 16 maart 2016). Tevens worden gemeenten meer en meer actief in het proactief aangaan van een dialoog om de komst van extremistische sprekers te voorkomen. Deze tweeledige aanpak wordt voortgezet.	
20.	NCTV traint samen met Buitenlandse Zaken en AIVD medewerkers op de Nederlandse posten in het buitenland ten behoeve van detectie mogelijk terroristen in proces consulaire bijstand.	De NCTV geeft aan dat 2015 in het teken stond om te verkennen hoe de Nederlandse posten in het buitenland ten behoeve van detectie mogelijk terroristen in proces consulaire bijstand te versterken en de awareness te vergroten. Dit heeft geleid tot realisatie in 2016 van de volgende twee instrumenten. Ten eerste zijn de diplomatieke vertegenwoordigingen in de relevante regio's via trainingen bewust gemaakt alert te zijn op personen die terugkeren vanuit jihadistisch strijdgebied en hoe te handelen in deze situaties. Ten tweede heeft de NCTV in afstemming met OM, NP, BZ, AIVD, IND, KMAR een werkwijze opgesteld met daarin de te ondernemen stappen en te informeren partners indien een persoon waar vermoedens van radicalisering en/of terrorisme zijn zich meldt op de post[93].	
21.	NCTV onderzoekt de juridische kaders voor uitwisselen informatie over personen in het casusoverleg en stelt een landelijk beschikbaar modelconvenant op samen met partners tbv casus overleggen jihadisme op lokaal niveau.	Tijdens de periode van de evaluatie is geen landelijk modelconvenant gerealiseerd. Het modelconvenant en bijbehorend machtigingsbesluit voor de politie in op 20 juli 2017 gepubliceerd in de Staatscourant en is daarmee inmiddels beschikbaar geworden voor de lokale casusoverleggen[94].	

93NCTV, Nota Werkwijze jihadisten die zich melden/worden gemeld op de post, 25 november 2016
94 Staatscourant, Nr. 41324, 20 juli 2017.

Versterken informatie-uitwisseling voor detectie en tegengaan van reisbewegingen			
22.	Wijziging van de Paspoortwet (Min BZK). Met deze wijziging is het mogelijk dat de Nederlandse identiteitskaart en paspoort van een persoon van rechtswege vervallen na het opleggen van een uitreisverbod uit de Twbmt, alsmede het regelen van een vervangend identiteitsdocument in geval van een opgelegd uitreisverbod om te kunnen blijven voldoen aan de Wet op de identificatieplicht.	Zie realisatie opgenomen onder instrument D.	
23.	Identificeren van gaten in de huidige Europese (en internationale) informatie uitwisseling. Daartoe heeft de NCTV naar aanleiding van de uitkomsten van een samen met Europese partners uitgevoerde studie in 2014 en 2015 ingezet op een Europees plan om te komen tot verbetering van de Europese informatie-uitwisseling.	In de geannoteerde agenda van de JBZ-raad is het volgende opgenomen: Nederland onderschrijft voorts het belang van een goed werkend, wettelijk gekaderd nationaal systeem van informatie-uitwisseling tussen inlichtingen- en opsporingsdiensten en acht het voorstelbaar dat verdere systematisering van SIS II uitwisseling hieraan bij kan dragen[95]. In Nederland zijn deze acties vertaald in het Actieprogramma Integrale Aanpak Jihadisme[96]. Ter voorbereiding op het Nederlands voorzitterschap van de EU heeft de NCTV voor de prioriteit terrorisme bestrijding, het initiatief genomen tot het opstellen van verdere specifieke acties om de aanpak van informatie uitwisseling en detectie van reisbewegingen te versterken. Dit Europese initiatief heeft geresulteerd in 2016 in een bijdrage aan de Roadmap[97].	

95 Brief regering, kenmerk: 32317-339, 30 september 2015, Bijlage 2: Geannoteerde agenda JBZ-Raad.
96 NCTV, Actieprogramma Integrale Aanpak Jihadisme, augustus 2014
97 St9368/2016/REV1 Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area 6 juni 2016

		De Roadmap is gericht op verbetering van informatie-uitwisseling door concrete knelpunten - in een specifiek tijdbestek - weg te nemen tussen lidstaten op het gebied van rechtshandhaving, terrorismebestrijding, management en migratie.	
24.	Onderkende uitreizigers worden geplaatst in de internationale en Europese signaleringssystemen.	Nederland hanteerde reeds criteria voor het opvoeren van signaleringen van personen gerelateerd aan terrorisme. In de Roadmap[98] is getracht meer harmonie aan te brengen in de criteria die de Europese lidstaten gebruiken en deze consistent te gebruiken voor het opvoeren van signaleringen in verschillende systemen en deling van de informatie met Europol. Dit moet resulteren in een aanpassing van een aantal regelingen, waardoor het uitgangspunt nu voor de lidstaten gelijk is.	
25.	Versterking detectie-en signaleringssystemen en (inter)nationale informatie-uitwisseling. Verhoogd gebruik en stijging in deling van informatie over jihadgangers met Europese en internationale systemen.	Ter voorbereiding op het Nederlands voorzitterschap van de EU heeft de NCTV voor de prioriteit terrorisme bestrijding, het initiatief genomen tot het opstellen van verdere specifieke acties om de aanpak van informatie uitwisseling en detectie van reisbewegingen te versterken. Dit Europese initiatief heeft geresulteerd in 2016 in een hoofdstuk toegewijd aan het onderwerp in de Roadmap[99].	
26.	Realisatie technische voorziening reisgegevens Travel Information Portal (TRIP) voor de ontsluiting en verwerking van bestaande stromen van passagiersgegevens op basis van bestaande wetgeving.	De technische voorziening reisgegevens TRIP was nog in ontwikkeling gedurende de periode van deze doorlichting. De technische voorziening reisgegevens is in 2016 in gebruik genomen[100].	

98 St9368/2016/REV1 Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area 6 juni 2016
99 St9368/2016/REV1 Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area 6 juni 2016
100 Staatscourant, Nr. 11932, 9 maart 2016

27.	Ingezet is op de totstandkoming van de EU PNR-richtlijn met hoogwaardige bescherming van persoonsgegevens van passagiers.	De richtlijn is na de periode van deze beleidsevaluatie gepubliceerd. Op 4 mei 2016 is de richtlijn (EU) 2016/681 van het Europees parlement en de Raad van 27 april 2016 over het gebruik van reisgegevens (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit gepubliceerd in het Publicatieblad van de Europese Unie[101].	
28.	Oprichting structureel multidisciplinair platform nationale diensten die zich bezighouden met informatie uitwisseling en reisbewegingen.	De NCTV heeft in het kader van de versterking van de detectie van reisbewegingen een platform ingericht waarbij de diensten die alleen hun eigen, zelfstandige verantwoordelijkheid hebben structureel bijeen te brengen. In het platform 'reisbewegingen en informatie uitwisseling' wordt onder voorzitterschap van de NCTV de nationale praktijk van informatie uitwisseling, en de detectie en signalering van personen reisbewegingen(op operationeel en strategisch niveau) besproken. De werkgroep komt periodiek bijeen en richt zich op verbetering van processen in de nationale praktijk en levert input voor de Europese samenwerking[102].	
29.	Ten behoeve van een versterkte coördinatie op de uitvoering heeft de NCTV de CT-Infobox verzocht een integraal en actueel overzicht van de genomen maatregelen op persoonsniveau bij te houden.	Ten tijde van de periode van de beleidsdoorlichting werkt de CT-Infobox aan een centraal overzicht van de genomen maatregelen op persoonsniveau. Dit betreft de in de CT-Infobox aangemelde personen.	

101 Publicatieblad van de Europese unie L119/132 NL 4 mei 2016
102 Brief NCTV, kenmerk: 779815, onderwerp: Voortgang Actieprogramma Integrale Aanpak Jihadisme, 11 juli 2016.

Coördineren en faciliteren van lokale, nationale en internationale samenwerkingsverbanden			
Opzetten (samenwerkings)structuur en verbeteren (operationele) informatie uitwisseling			
30.	Verwerking van inlichtingenproducten en vervaardiging van analyseproducten waaronder het Dreigingsbeeld Terrorisme Nederland (DTN).	In de onderzoeksperiode van deze doorlichting heeft de NCTV DTN 24 tot en met 40 uitgebracht[103].	
31.	Het monitoren en analyseren op trendniveau van dreigingen om anderen in staat te stellen te kunnen handelen (onder meer door uitbrengen Dreigingsbeeld Terrorisme Nederland (DTN) en diverse monitoring – en analyseproducten voor partners.	Dit betreft een van de kerntaken van de NCTV. Op de website van de NCTV zijn diverse producten te vinden die de NCTV heeft gepubliceerd, zoals trendanalyses. Voor intern gebruik stelt de NCTV dagelijks een Duidingsoverzicht Nationale Veiligheid op. Deze informatie is voornamelijk bedoeld voor tactische en strategische afstemming NCTV intern. Ook stelt de NCTV situatieschetsen en duiding op bij incidenten en maatschappelijke ontwikkelingen die de Nationale veiligheid kunnen raken. Tot slot verstuurt de NCTV een attendering op voor ketenpartners, het zogeheten weekbericht internetmonitoring. Het weekbericht bestaat uit online waargenomen trends en ontwikkelingen over terrorisme en extremisme die zijn gebaseerd op open bronnen[104].	
32.	De NCTV stelt adviseurs beschikbaar voor de betrokken gemeenten. De adviseurs ondersteunen gemeenten bij kennis en kunde over dreigingsniveau en het fenomeen jihadisme en de aanpak ervan. Zij stimuleren vroegsignalering, adviseren over interventiemogelijkheden, versterken relevante netwerken en ondersteunen (beleidsmatig) bij het opzetten van een	De NCTV heeft meerdere adviseurs beschikbaar gesteld voor de meest betrokken gemeenten. Daarnaast hebben zij zich ook gericht op gemeenten die nog geen structuren hebben opgezet om casuïstiek te behandelen of signalen naar boven te krijgen. Dit laatste omdat de meest betrokken gemeenten steeds weerbaarder zijn geworden. Overige gemeenten werden bediend via de inzet voor de regio beschikbare adviseur van de NCTV.	In de evaluatie van de CT-strategie is opgenomen dat de inzet van de NCTV wordt gewaardeerd wanneer zij gemeenten, politie of andere organisaties ondersteunt met extra expertise.

103 Publicatie NCTV, Barometer van de dreiging: Tien jaar Dreigingsbeeld Terrorisme Nederland 2005-2015, december 2015.
104 De NCTV heeft de ADR inzicht gegeven in de verschillende beschikbare analyseproducten, zoals benoemd bij de realisatie.

	lokale of regionale (bestuurlijke) aanpak. Daarnaast vindt geregeld afstemmingsoverleg plaats met de burgemeesters van de meest betrokken gemeenten over de lokale aanpak. Tevens sluit het Rijk en de betrokken gemeenten een pact ter preventie van radicalisering en beheersing van maatschappelijke spanningen.	De adviseurs van de NCTV ondersteunen gemeenten concreet met kennis en kunde over dreiging en fenomeen, helpen gemeenten hier gericht beleid/aanpak op te formuleren (operationeel/tactisch/strategisch), versterken de regierol van gemeenten door samenwerkingsverbanden samen met gemeenten in te richten en barrières in informatie-uitwisseling weg te nemen. Tot slot zijn de adviseurs van de NCTV beschikbaar om mee te denken over interventiemogelijkheden op individueel en netwerk niveau en adviseren zij in de breedte van de aanpak (van preventie tot repressie) over handelingsperspectief[105]. Gemeenten en andere lokale partijen in de risicogebieden worden ondersteund bij het ontwikkelen en versterken van hun aanpak. Tot en met 2015 zijn 28 gemeentes zijn ondersteund via leerkringen (De Expertise-unit Sociale Stabiliteit is betrokken bij de uitvoering van deze leerkringen). In aanvulling daarop worden gemeenten ondersteund door het Rijk in het opbouwen van strategische netwerken met sleutelfiguren, professionals en gemeentemedewerkers. In 2013, 2014 en 2015 zijn de burgermeesters van de meest betrokken gemeenten zo'n 15 keer bijeengekomen in aanwezigheid van de betrokken bewindspersonen NCTV en AIVD om ontwikkelingen en dreigingen en de aanpak af te stemmen en door te spreken[106]. Het pact is uiteindelijk niet gerealiseerd. NCTV heeft ervoor gekozen de voorgestane bestuurlijke afspraken uitwerking te geven met de gelden voor versterking van de veiligheidsketen voor het lokaal domein op 27 februari 2015 beschikbaar zijn gekomen.	

105 Algemeen voorlichtingsdocument NCTV, De Rol en aanpak van de NCTV ten aanzien van het lokaal bestuur op het gebied van gewelddadig extremisme, datum onbekend.
106 Agenda's Periodiek bestuurlijk overleg integrale aanpak jihadgangers (deel in bijzijn TK-leden) over de periode 2013 tot en met 2015,

33.	In verband met berichten over vermenging van terroristen in de vluchtelingenstroom zet de NCTV sinds het najaar van 2015 aanvullend in op intensivering van de samenwerking in de vreemdelingenketen door awareness bijeenkomsten te organiseren samen met de IND, COA en DT&V en de Vreemdelingenketen en het CT-netwerk op onderdelen te verbinden (bijvoorbeeld in I&R-straat).	In een kamerbrief is het volgende opgenomen. In Nederland is en wordt geïnvesteerd in het bevorderen van het veiligheidsbewustzijn bij medewerkers van de vreemdelingenketen (waaronder COA, DT&V, IND). Zo ontvangen de medewerkers op de vele nieuwe locaties van het Centraal Orgaan opvang asielzoekers (COA) die momenteel worden opengesteld een training met speciale aandacht voor veiligheidsonderwerpen. Daarin wordt onder meer aandacht geschonken aan veiligheidsbewustzijn in het kader van nationale veiligheid. Ook het Rijksopleidingsinstituut tegengaan Radicalisering (ROR), dat vanaf september 2015 operationeel is, zal opleidingen verzorgen voor professionals in onder andere de (brede) Veiligheids- Terrorismebestrijdings- en Vreemdelingenketen[107]. Binnen de uitvoerende organisaties van de vreemdelingenketen is een meldstructuur ingericht voor dergelijke signalen waar de registratie- en screeningprocedures deel van uitmaken, maar ook via de medewerkers op de werkvloer en uit de vluchtelingenpopulatie zelf worden signalen ontvangen.	
34.	Het verlenen van consulaire bijstand in aangrenzende landen van personen die uit eigen beweging terug keren naar Nederland, omdat zij uit jihadistische beweging of terroristische organisatie willen stappen.	In de voortgangsrapportages is opgenomen dat de NCTV samen met de AIVD en BZ werkt aan het vergroten van de awareness op het postennetwerk in de omgang met mogelijke terugkerende jihadisten. In het bijzonder is daarbij aandacht voor het aanscherpen van procedures rondom reisdocumentatie, consulaire bijstand en uitzettingen naar Nederland. De Nederlandse ambassades in de relevante regio's hierover zijn geïnformeerd en via trainingen bewust gemaakt.	

107 Brief NCTV aan Tweede Kamer, 9 november 2015, kenmerk: 699865, Onderwerp: beleidsimplicaties Dreigingsbeeld Terrorisme Nederland 40.

Intensivering van de internationale samenwerking en aanpak jihadgangers			
35.	Om de internationale samenwerking en aanpak te versterken worden internationale afspraken gemaakt over het delen van informatie over concrete activiteiten. Hierbij vervult de NCTV de rol van trekker of deelnemer aan internationale gremia en werkgroepen. Zoals vervulling van het co-leadership van de workstream Foreign Terrorist Fighters (samen met Marokko) in het verband van het Global CounterTerrorism Forum (GCTF) en het co-leadership van de Foreign Terrorist Fighters Working Group (samen met Turkije) in het Global Coalition Countering ISIL (GCCI) verband.	Als co-voorzitters van de GCTF FTF werkgroep hebben Nederland en Marokko het initiatief genomen om aanvullende richtsnoeren te ontwikkelen voor effectieve aanpak van terugkerende uitreizigers. Thema's die centraal staan zijn informatie-uitwisseling, detectie, strafrechtelijke aanpak en rehabilitatie en re-integratie. In maart en mei vonden hierover expertbijeenkomsten plaats. Deze richtsnoeren zijn onderdeel van een breder GCTF initiatief gericht op het voorkomen en aanpakken van radicalisering. Dit omvat ook thema's als jeugdrecht, de rol van families in (voorkomen van) radicalisering, en (online) tegengeluid. In EU en multilateraal kader is de samenwerking verder geïntensiveerd. In EU verband is Nederland zeer actief als voorzitter van de Raad van Ministers (JZB-raad). Tevens agendeert het specifieke prioriteiten in de EU Kopgroep Jihadisme die periodiek onder Belgische voorzitterschap bijeenkomt en voorzitter is van de EU-werkgroep over de externe dimensie van terrorismebestrijding (COTER).	
Het voorkomen van aanwas door ondermijning aanbod propaganda en verhogen weerbaarheid kwetsbare groepen			
Coördineren en faciliteren van het netwerk aan partijen waarbinnen activiteiten ter voorkoming van aanwas moeten plaatsvinden			
Opzetten structuur en verbetering informatie-uitwisseling			
36.	Versterking van de vroegsignalering en monitoring van radicalisering, in het bijzonder gericht op wijken met de grootste kwetsbaarheid.	• Binnen de 18 geprioriteerde gemeenten is de aanvullende ondersteuning voor de scholen in de vorm van een complementaire aanpak ontwikkeld. Deze aanpak bestaat uit een aanbod van trainingen en advies, ontwikkeld en uitgevoerd door NCTV, OCW, SZW, de	De evaluatie van de Complementaire Onderwijs Aanpak (COA), die voortvloeit uit het Actieprogramma Aanpak Jihadisme, is reeds afgerond. De evaluatie geeft inzicht in de mate waarin de aanpak heeft

	Hiertoe heeft de NCTV ingezet op de volgende instrumenten: • Aanvullende ondersteuning voor scholen. • Actualiseren van de handreiking aanpak van radicalisering en terrorismebestrijding op lokaal niveau. • Opstellen van een handreiking terrorismegevolgbestrijding. • Bundeling initiatieven rondom verbetering van risicotaxaties. • Delen van de woordvoerlingslijnen integrale aanpak radicalisering met gemeenten.	Stichting School en Veiligheid en de Expertise-unit Sociale Stabiliteit. Daarnaast wordt er een aanbod ontwikkeld om met leerlingen het gesprek aan te gaan over deze thema's. In het kader van de aanvullende ondersteuning zijn er inmiddels circa 108 adviesgesprekken gehouden met scholen en gemeenten en zijn reeds meer dan 101 trainingen gegeven.[108] • De NCTV heeft geactualiseerde handreiking gepubliceerd in november 2014 met daarin informatie over de rol van de gemeenten bij het signaleren en tegengaan van radicaliseren[109]. • De NCTV heeft de handreiking Terrorismegevolgbestrijding voor (eind) beslissers in de crisisbeheersing en hun adviseurs op strategisch niveau gepubliceerd in november 2015[110]. • NCTV heeft in januari 2015 woordvoeringslijnen integrale aanpak radicalisering met alle gemeenten gedeeld, verschillende bijeenkomsten rondom communicatie radicalisering met meest betrokken gemeenten (o.a. maart 2015) georganiseerd[111].	bijgedragen aan het tegengaan van radicalisering en in de mate waarin de aanpak voor verbetering vatbaar is. De aanbevelingen worden meegenomen in een vervolgaanpak.
37.	Oprichting van een Nationaal Meldpunt radicalisering voor alle vormen van extremisme en terrorisme.	Burgers en professionals kunnen bij Meld Misdaad Anoniem terecht met anonieme meldingen inzake alle vormen van extremisme. De medewerkers van Misdaad Anoniem zijn door de NCTV getraind op het onderwerp. In de periode januari 2015 tot en met mei 2016 zijn 199 meldingen met betrekking tot terrorisme en extremisme ontvangen.	

108 8e Voortgangsrapportage actieprogramma jihadisme d.d. 6 april 2017
109 Handreiking aanpak van radicalisering en terrorismebestrijding op lokaal niveau, november 2014
110 Handreiking terrorismegevolgbestrijding,Publicatienummer: 88037, november 2015. & Nieuwsbrief Nationaal Crisiscentrum, 30 november 2015.
111 Mogelijke woordvoeringslijnen radicalisering en terrorismebestrijding, 20 januari 2015.

38.	Zorgen dat betrokken burgers radicaliserende, haatzaaiende jihadistische content op internet en social media kunnen melden en dat producenten en verspreiders van online jihadistische propaganda – en de digitale platforms die zij misbruiken – worden geïdentificeerd. Daarnaast wordt deze informatie actief gedeeld met de handelingsbevoegde instanties en relevante dienstverleners. De NCTV zet samen met de Nationale Politie ingezet op de oprichting van een specialistische unit die zich richt op verwijdering van jihadistische content van openbare (sociale media) accounts en websites. Ook heeft de NCTV afspraken gemaakt met private partijen over omgang met online extremistische content.	Door tussenkomst van de NCTV zijn in 2014 twee websites met extremistische content offline gehaald[112]. In verschillende Eenheden van de Nationale Politie is in 2014 en 2015 binnen OSINT verband haatzaaiende content aangetroffen. In een aantal gevallen is deze content verwijderd en in een aantal gevallen is een strafrechtelijk onderzoek gestart. Binnen de NP is op een specialistische unit opgericht die zich vanaf 2015 richt op verwijdering van jihadistische content van openbare (sociale media) accounts en websites. Deze Nederlandse Internet Referral Unit (NL IRU), voert haar kerntaak uit via NTA (Notice and take action). Ook kan content onder gezag van het OM middels de inzet van het strafrecht via een NTD- procedure worden verwijderd. Afstemming en samenwerking op dit thema tussen de NP en Europol vindt doorlopend plaats. Verschillende bedrijven accepteren niet dat op hun platform terrorisme wordt bevorderd en hun gebruikersvoorwaarden maken helder dat dit soort gedrag , of gewelddadige bedreigingen niet is toegestaan. Zo heeft bijvoorbeeld Twitter sinds de zomer van 2015 alleen al meer dan 125.000 accounts voor bedreigend of het bevorderen van terroristische daden, voornamelijk met betrekking op ISIS, opgeschort.	

Versterken van het netwerk, lokaal en landelijk, gericht op ingrijpen bij radicalisering			
39.	Deskundigheidsbevordering in de uitvoering door o.a. gerichte voorlichting en het ontwikkelen van specialistische trainingen en vakopleiding, de ondersteuning van onderwijsinstellingen en het oprichten van	Zie ook de realisatie bij II over de versterking van de vroegsignalering en monitoring van radicalisering. *Kennisbank terrorisme app*: Lancering door de NCTV in december 2014 van de kennisbank Terrorisme app waarmee	

112 Website www.nctv.nl, Mail aan registar webiste de ware regelie, & Nieuwsbericht NOS, 11 februari 2014, NCTV wil jihadzender uit de lucht

	een expertcentrum dat de informatiepositie van Rijk en gemeenten over maatschappelijke spanningen en radicalisering versterkt. De NCTV zet hiertoe in op en was medeopdrachtgever van taken op het gebied van radicalisering: • Lancering van de kennisbank terrorisme app Deskundigheidsbevorderings-bijeenkomsten voor de leden van het Landelijk Platform Lokale Professionals. • Oprichting van het Rijksopleidingsinstituut Radicalisering (ROR). • Oprichting van de Expertise-unit Sociale Stabiliteit waarbij NCTV is mede-opdrachtgever van de ESS voor taken op gebied van radicalisering.	eerste lijnsprofessionals vanaf hun mobiele telefoon toegang krijgen tot informatie over terroristische organisaties[113]. *Deskundigheidsbevorderingsbijeenkomsten*: Organisatie door de NCTV van jaarlijkse deskundigheidsbevorderingsbijeenkomsten voor de leden van het Landelijk Platform Lokale Professionals. Tijdens deze bijeenkomsten worden kennis en good practices gedeeld en is ruimte om te netwerken[114.] *Oprichting Rijksopleidingsinstituut Radicalisering*: De ROR is per oktober 2015 opgericht. Het ROR is een samenwerking tussen de NCTV en het opleidingsinstituut DJI. Het ROR bedient o.a. de vreemdelingenketen, jeugdzorg-, welzijns-, veiligheids- en justitiële sector maar ook andere instanties binnen de (semi) publieke sector. In juli 2016 zijn diverse trainingen al aangevraagd en gepland. *Expertise-unit Sociale Stabiliteit*: Begin 2015 is de Expertise-unit Sociale Stabiliteit opgericht onder het ministerie van SZW. De ESS biedt gemeenten, eerstelijns professionals en diverse groepen in de samenleving praktijkkennis aan over maatschappelijke spanningen, waaronder radicalisering. In de eerste helft van 2016 heeft ESS 25 gemeenten geadviseerd. De training en workshop Omgaan Met Extreme Idealen, over de radicalisering vanuit een pedagogisch perspectief is in 2016 aan circa 500 professionals gegeven.	
40.	Oprichting van een EXIT-faciliteit in Nederland, die personen die uit het jihadistische beweging of terroristische	Per oktober 2015 is de Exit faciliteit 'Exits' ingericht. Exits biedt trajecten aan voor geradicaliseerde personen die openstaan voor een alternatief om te re-integreren in de	

113 https://play.google.com/store/apps/details?id=com.metro.kennisbank
114 Www.nctv.nl, Landelijk Platform Lokale Professionals.

	organisatie willen stappen onder strenge voorwaarden begeleidt	samenleving buiten het jihadistische netwerk. De Exit-faciliteit is als onafhankelijke organisatie ondergebracht bij de Stichting Fier Fryslân, die hiervoor subsidie ontvangt. Bij de Exit-faciliteit lopen in juli 2016 verschillende trajecten.	
41.	Oprichting van een ondersteuningsfaciliteit waarmee familie of vrienden van geradicaliseerde individuen en uitreizigers worden ondersteund.	Het Familiesteunpunt Radicalisering is operationeel sinds oktober 2015. Het Steunpunt richt zich op families van radicaliserende en geradicaliseerde personen en biedt kennis en instrumenten voor de omgang met geradicaliseerde familieleden. Het Familiesteunpunt is ondergebracht bij Stichting Fier Fryslân die hiervoor subsidie ontvangt. In maart 2016 werden ongeveer 15 families ondersteund door het steunpunt[115].	
42.	Samenwerking met de islamitische gemeenschap door periodiek overleg met imams. Nederlandse imams en moskeebestuurders zijn medestanders in de strijd tegen de extremisten, die hun geloof kapen en hun kinderen misleiden en misbruiken. De rol van de NCTV is meedenken in het kader van de integrale aanpak.	Het samenwerkingsverband Marokkaanse Nederlanders, Contact Orgaan Moslims en Overheid en Inspraak Orgaan Turken hebben vanuit het Rijk subsidie (SZW) ontvangen om interventieprogramma's uit te voeren. De programma's hebben tot doel radicalisering binnen de gemeenschappen tegen te gaan en te voorkomen. In juli 2016 zijn 99 (van de 190) trainers en vertrouwenspersonen getraind en hebben 19 (van de 100) voorlichtingsbijeenkomsten en debatten plaats gevonden.	
43.	De ondersteuning bij het versterken van bestaande netwerken van lokale en landelijke sleutelfiguren. Sleutelfiguren die het alternatieve geluid uitdragen en stelling nemen tegen jihadisme worden ondersteund en getraind (mediatraining). Daarnaast worden sleutelfiguren die worden	Gemeenten worden ondersteund door het Rijk in het opbouwen van strategische netwerken met sleutelfiguren, professionals en gemeentemedewerkers. De opbouw van strategische netwerken polarisatie en radicalisering in gemeenten was gedurende de periode van de beleidsdoorlichting nog in volle gang. Voorgenoemde netwerken bestaan uit 15 tot 30 personen, waaronder	

115 Www.familiesteunpunt.nl, en vijfde voortgangsrapportage Actieprogramma Integrale Aanpak Jihadisme.

	bedreigd, gesteund en waar nodig opgenomen in het stelsel Bewaken en Beveiligen.	sleutelfiguren, jongerenwerkers, moskeebestuurders, schooldirecteuren, politie en gemeentemedewerkers. Bevordering van deskundigheid en uitwisseling van kennis en inzichten staan voorop.	
44.	Het versterken van netwerken rond jongeren en hun opvoeders. Daarbij wordt een laagdrempelig aanbod van professionele opvoedondersteuning gestimuleerd.	In het kader van opvoedondersteuning is het plan Weerbaar Opvoeden opgesteld. Met een aantal gemeenten werd aan proefprojecten gewerkt om samenwerking tot stand te brengen tussen professionals, migrantenorganisaties en vrijwilligers. Metparticipatief onderzoek wordt verzekerd dat de resultaten in bruikbare producten worden omgezet voor gemeenten en professionals. In december 2015 vond de startbijeenkomst voor deze proefprojecten plaats.	
45.	Het stimuleren van het maatschappelijke debat over de grenzen van de rechtstaat. Om de verspreiding van extremisme geen kans te geven, worden onderliggende waarden van de rechtsstaat gedeeld en uitgedragen.	Voor het stimuleren van het maatschappelijke debat over de grenzen van de rechtstaat zijn in 2015 via het project Meten met twee maten meer dan 300 studenten het debat met elkaar aangegaan over het Nederlands buitenlands beleid.	
46.	Het mobiliseren van maatschappelijke tegengeluiden en versterken van de weerbaarheid tegen radicalisering en spanningen. Het gaat hier onder andere om de ondersteuning van kleinschalige initiatieven. Bijvoorbeeld lokale voorlichtingsbijeenkomsten in betrokken gemeenschappen over ronseling en online gevaren voor jongeren en initiatieven gericht op het intensiveren van de dialoog binnen de gemeenschappen over radicalisering en normoverschrijdend gedrag.	Voor het mobiliseren van maatschappelijke tegengeluiden en het versterken van de weerbaarheid tegen radicalisering en spanningen is in 2015 geïnvesteerd in 30 lokale voorlichtingsbijeenkomsten in betrokken gemeenschappen voor ouders over ronselen en online gevaren voor jongeren en het herkennen van radicalisering. Hiermee zijn in 2015 en 2016 1200 ouders en jongeren bereikt. Ook is in februari 2015 is een internationale expertbijeenkomst over tegengeluid georganiseerd. Vanuit het Kennisplatform Integratie en Samenleving is de This is Me Campagne in 2015 in 4 gemeenten gestart met als doel moslimjongeren weerbaarder te maken bij gevoelens van discriminatie en uitsluiting. Vanuit het Rijk is ondersteuning verleend aan de	

	De NCTV coördineert hier de interdepartementale samenwerking (met SZW en BZ); coördineert de strategievorming en voert regie in de uitvoering.	theatervoorstelling Jihad, de voorstelling. Tot en met juli 2016 hebben 5500 leerlingen het toneelstuk bijgewoond en zijn hierover na afloop in gesprek gegaan.	

Beschermen van personen, objecten en vitale processen tegen terroristische aanslagen			
Verder professionaliseren van het stelsel Bewaken en Beveiligen			
47.	Evaluatie van het stelsel B&B: onderzoek naar de werking van de kritische (werk)processen die binnen en tussen de verschillende partners plaatsvinden en die direct van invloed zijn op de effectiviteit van het stelsel.	In 2014 heeft de Inspectie VenJ evaluatie uitgevoerd naar stelsel bewaken en beveiligen[116]. Mede naar aanleiding van deze evaluatie is een Stuurgroep BenB ingesteld onder voorzitterschap van de D-DB3, met daarin verschillende uitvoeringspartners (OM, Politie, AIVD, MIVD en KMar).[117] Op basis van het Evaluatierapport is een overzicht opgesteld met een opsomming van de actiepunten die in het Evaluatierapport worden benoemd[118]. Een belangrijk deel van de verbeterpunten is verwerkt in de nieuwe Circulaire bewaken en beveiligen van personen, objecten en diensten. De Circulaire is aangepast in nauw overleg met alle uitvoeringspartners (in de Stuurgroep en een ambtelijke voorbereidingsgroep). Medio 2015 heeft de Minister VenJ de nieuwe Circulaire geaccordeerd[119].	Het rapport "Het Stelsel bewaken en beveiligen anno 2013; een onderzoek van de Inspectie Veiligheid en Justitie naar de organisatie en werking op decentraal niveau en in het rijksdomein' (Gerubriceerd SG, oplevering in 2014). Hoewel geen evaluaties beschikbaar zijn waaruit concreet blijkt dat het stelsel naar aanleiding van de evaluatie 'professioneler' is geworden, is het plausibel dat door de ondernomen acties het stelsel is verbeterd.
48.	Opstellen werkwijze Nationale Evenementen: Met de werkwijze wordt beoogd Nationale Evenementen veilig en ongestoord te laten verlopen, zonder afbreuk te doen aan het karakter van het evenement. Doel is alle partners, die in de voorbereiding en uitvoering betrokken zijn	Werkwijze bewaken en beveiligen Nationale Evenementen is in maart 2011 goedgekeurd door de toenmalige raad van korpschefs NCTV.[120] In 2011 en 2012 heeft een aantal evaluaties van Nationale Evenementen plaatsgevonden. Dit zijn onder andere evaluaties uitgevoerd door de Auditdienst Rijk[121] en verschillende interne evaluaties van de organiserende regiokorpsen. In 2013 heeft de ADR in	Het proces van bewaken en beveiligen van resp. Koninginnedag 2011, Koninginnedag 2012 en Prinsjesdag 2012 zijn positief geëvalueerd. Uit het evaluatieonderzoek bewaken en beveiligen NE blijkt dat de werkwijze een

116 Rapport Evaluatie stelsel Bewaken en Beveiligen, 2014, Inspectie VenJ - Staatsgeheim
117 Brief Uitnodiging Stuurgroep Stelsel Bewaken en Beveiligen, d.d. 10 oktober 2014
118 AGENDAPUNT 2: concept overzicht ter bespreking en aanvulling in de Stuurgroep Stelsel BenB van 17 oktober 2014: Inventarisatie van mogelijke verbeteringen ten aanzien van de kwaliteit , effectiviteit en toekomstbestendigheid van het Stelsel Bewaken en Beveiligen; AGENDAPUNT 4: concept-overzicht verbeterpunten Stelsel BenB,Stuurgroep BenB 19 november 2014; AGENDAPUNT 3: concept-overzicht verbeterpunten Stelsel BenB Stuurgroep BenB 26 augustus 2015
119 Nota nieuwe circulaire Bewaken en Beveiligen, d.d. 16 juni 2015
120 Aanbiedingsbrief behorend bij Werkwijze bewaken en beveiligen Nationale Evenementen, 18 maart 2011
121 Evaluatie bewaken en beveiligen Koninginnedag 2011 en 2012 en evaluatie bewaken en beveiligen Prinsjesdag 2012

	bij bewakings- en beveiligingsaspecten, te informeren en te voorzien van een duidelijke handreiking.	opdracht van de NCTV breed evaluatieonderzoek uitgevoerd om inzicht te krijgen hoe het proces van bewaken en beveiligen van Nationale Evenementen verder kan worden verbeterd[122]. Hieruit blijkt dat de handreiking in de praktijk ook is gebruikt.	waardevol is en dat het heeft geleid tot meer structuur in de voorbereiding van Nationale Evenementen[123].
Intensivering aanpak solistische dreigers			
49.	Project Solistische Dreigers: in 2010 is project 'solistische dreigers' gestart. Het project kent een drietal deeltrajecten: de pilot Dreigingsmanagement (PDM) waarmee is ingezet op een gestructureerde aanpak van verwarde en gefixeerde bedreigers. Ten tweede is onder jongeren de aandacht vergroot voor het feit dat bedreigen strafbaar is, om op die manier het aantal zogenaamde 'straattaaldreigers' te verminderen. Tot slot is er een aantal onderzoeken gestart met als doel de kennis over het fenomeen van solistische dreigers te vergroten, waaronder ook de ongekende dreigers.		
49a	Aanpak verwarde bedreigers: In een pilot 'Dreigingsmanagement' ontwikkelen van een gestructureerde aanpak van verwarde bedreigers, gericht op identificatie, risico-inschatting en zorgtoedeling.	Op 1 januari 2011 is bij het toenmalige Korps Landelijke Politiediensten de zogenaamde Pilot Dreigingsmanagement (PDM) van start gegaan[124]. In 2012 is een ex ante evaluatie op de pilot dreigingsmanagement uitgevoerd door een onderzoeksteam van de capaciteitsgroep Strafrecht en Criminologie van de faculteit der rechtsgeleerdheid van de Universiteit Maastricht[125]. Een planevaluatie is uitgevoerd met als doel: de assumpties en doelstellingen die aan de pilot ten grondslag liggen bloot te leggen en te analyseren, mogelijke knelpunten die zich bij de uitvoering van de PDM voor kunnen doen vast te stellen en indicatoren op te stellen ten behoeve van een toekomstige procesevaluatie. In 2013 is de wijze waarop de PDM is geïmplementeerd en uitgevoerd geëvalueerd[126.]	Uit de proces evaluatie blijkt dat op basis van het beperkt aantal casussen nog geen wetenschappelijke uitspraken over effectiviteit konden worden gedaan. Weliswaar kon worden vastgesteld dat op basis van herhaalde risicotaxaties door PDM op 1 januari 2013 bij 9 van de 13 dreigers de risico's op de verschillende onderscheiden domeinen waren gedaald ten tijde van de persoonsgerichte aanpak van de pilot – en dat als gevolg daarvan in vier gevallen de intensieve monitoring was beëindigd. Maar het was niet met zekerheid vast te stellen in welke mate de waargenomen daling aan de pilot kon worden toegeschreven.

122 Evaluatieonderzoek bewaken en beveiligen Nationale Evenementen, ADR, d.d. 24 oktober 2013
123 Evaluatieonderzoek bewaken en beveiligen Nationale Evenementen, ADR, d.d. 24 oktober 2013
124 Kamerbrief Afronding project solistische dreigers en vervolg, d.d. 5 september 2013
125 Pilot Dreigingsmanagement: een ex ante evaluatie, d.d. april 2012
126 Pilot Dreigingsmanagement: De implementatie en wijze van uitvoering onder de loep, Universiteit van Maastricht i.s.m. onderzoeksbureau Impact R&D, d.d. mei 2013

			In de kamerbrief van 5 september 2013 vult de minister hierop aan dat dit te allen tijde een lastig te meten aspect zal zijn. Er kan nooit met volle zekerheid worden gesteld dat een aanslag voorkomen is door een bepaalde aanpak. Wel geeft de minister aan te durven stellen dat het verminderen of hanteerbaar maken van de dreiging in een aantal gevallen is bewerkstelligd. Tevens is in de proces evaluatie aangegeven dat de pilot PDM leidt tot meer integrale, gestructureerde en multidisciplinaire samenwerking tussen politie en zorg. Dit wordt gezien als een groot winstpunt. Deze samenwerking leidt naar het oordeel van de meeste respondenten tot een kwalitatief betere en doelmatigere aanpak van solistische dreigers, wat volgens hen effectiever en ook goedkoper is dan uitsluitend de weg te bewandelen van strafrechtelijke sanctionering. Het onderzoek laat ook zien dat, wat betreft de gekende dreigers, het belang van dreigingsmanagement door diverse partijen wordt onderschreven.

49b	Verminderen van zogeheten 'straattaaldreigers' door bij jongeren onder de aandacht te brengen dat bedreigen strafbaar is. Hiervoor wordt aanpak ontwikkeld voor de zogenaamde 'straattaaldreigers'. Daarnaast worden er concrete communicatiemiddelen ontwikkeld voor organisaties die een rol kunnen vervullen in het terugdringen van bedreigingen of die zelf te maken hebben met bedreigingen.	Er is een aanpak ontwikkeld voor straattaaldreigers in samenwerking met HALT regio West Nederland (Haaglanden), het parket Den Haag en politie-eenheid Den Haag. Vervolgens is na overleg met de gemeente Den Haag besloten om het lespakket voor scholen zodanig aan te passen dat het onderwerp 'digitaal dreigen' (in deze context 'straattaaldreigen') er nadrukkelijk in naar voren komt. Hiermee is het een vast onderdeel geworden van het voorlichtingspakket dat HALT sinds 2011 op middelbare scholen in Den Haag, Hollands Midden en Rotterdam Rijnmond aanbiedt. De aangepaste lesmodule wordt sinds 2011 aan alle scholen in de regio aangeboden en de reacties vanuit de schoolleiding en de leerlingen zijn positief. Gelet op het belang voor zowel jongeren evenals het effect dat een bedreiging op een publiek persoon kan hebben, heeft HALT na afloop van de pilotfase besloten deze module landelijk in te voeren. Er is voorlichtingsmateriaal ontwikkelt dat informatie bevat over (de gevolgen van) digitaal bedreigen en is verspreid onder relevante partnerorganisaties.	Hoewel geen causale relatie met bovengenoemde initiatieven kan worden vastgesteld, kan geconstateerd worden dat ten opzichte van 2010 er in 2011 en 2012 minder politici in Den Haag bij de politie melding hebben gedaan van bedreiging. Onduidelijk is nog of deze trend zich voortzet in 2013. Het merendeel van deze bedreigingen wordt nog steeds gedaan door minderjarigen. Het terugdringen van de straattaaldreigers op het internet zorgt er daarnaast voor dat inlichtingen- en veiligheidsdiensten en de politie zich meer kunnen concentreren op de beoordeling en aanpak van andere dreigementen van eenlingen.[127]
49c	Vergroten kennis fenomeen over solistische dreigers: enkele onderzoeken zijn gestart om de kennis over het fenomeen van solistische dreigers te vergroten, waaronder de ongekende dreigers	NCTV heeft in dit kader: onderzoek laten uitvoeren door het Centrum voor Terrorisme en Contraterrorisme (CTC) waarin gekeken wordt naar systeemhaat in relatie tot complotdenken. De basisvraag bij dit onderzoek is of complottheorieën, verdachtmakingen en bedreigingen aan het adres van de overheid en diens vertegenwoordigers het vertrouwen in het bevoegd gezag op de langere termijn uithollen en daarmee wellicht een voedingsbodem vormen voor mogelijke acties door gewelddadige eenlingen. Een tweede onderzoek is een terreinverkenning in de	

127 Kamerbrief Afronding project 'Solistische Dreigers' en vervolg, d.d. 5 september 2013

		neurobiologie door onderzoekers van de Radboud Universiteit Nijmegen. Dit onderzoek richtte zich op de samenhang tussen neurobiologische reacties en stresssituaties, bijvoorbeeld een concrete bedreiging. Daarnaast zijn er in internationaal verband diverse initiatieven ontplooid om de kennis over (aanslagen van) potentieel gewelddadige eenlingen verder te vergroten. Voorbeelden hiervan zijn het internationaal kennisnetwerk tussen diverse landen op het gebied van dreigings-management en het gezamenlijk onderzoek naar daderkennis en dodingen in het publieke domein door eenlingen dat het NIFP en de Duitse en Zwitserse collega's hebben opgezet.	
Toekomstbestendig maken van de beveiligingscontroles op de luchthavens			
50.	Om nieuwe dreigingen het hoofd te kunnen bieden en tegelijk het beveiligingsproces effectiever, efficiënter en passagiersvriendelijker te laten verlopen, is het noodzakelijk dat voortdurend naar innovaties wordt gezocht. Door de toegenomen dreiging en de daaruit volgende stapeling van security maatregelen is de roep om meer in te zetten op het principe van "risk based security" steeds groter. Door minder aandacht te besteden aan de passagiers	*Pilot project Autoclear Screening* Op 17 december 2013 is de pilot is project autoclear Screening van start gegaan[128]. Gedurende de periode van deze beleidsdoorlichting bevond het project zich nog in de pilotfase. Op 14 november 2015 is specifieke regelgeving uitgebracht waarmee toepassing van autoclear software mogelijk is[129]. *Pilot 'Laptops and liquids in bags'* In november 2013 is de pilot 'Laptops and liquids in bags' gestart. Op 4 augustus 2015 is de laatste voortgangsrapportage uitgebracht. De input vanuit deze pilot	Uit de voortgangsrapportages komt naar voren dat ten tijde van de periode van de beleidsdoorlichting nog verdere doorontwikkeling van apparatuur en software nodig is om een efficiëntere en effectievere beveiligingscontrole te kunnen realiseren. Met ingang van juni 2015 is Schiphol gestart met de toepassing van CTI-TIP op hun centrale security checkpoints. Met ingang van het najaar 2017 wordt een start gemaakt met de uitrol van apparatuur

128 Brief NCTV, Onderwerp: Request for approval pilot project Auto-clear Screening, kenmerk: 310177, 4 oktober 2012.
129 EC-regulation L 299/141, paragraph 12.3 auto clear software (ACS), 14 november 2015.

	met een laag risicoprofiel blijft meer tijd en capaciteit over om te besteden aan de passagiers die een groter risico vormen. De kern van de activiteiten zijn er daarom gericht op de ontwikkeling van een Proof of Concept van een beveiligings-infrastructuur, die risk based security mogelijk maakt. Daarom is met Schiphol en fabrikanten gewerkt aan beveiligingsapparatuur die een op risico gebaseerde screening mogelijk maakt. Er zijn verschillende projecten gestart en begeleid die tot doel hebben om het beveiligingsproces,passagiersvriendelijker ,efficiënter en daarmee effectiever te maken. Deze pilots zijn hieronder nader toegelicht. *Pilot project Auto-clear Screening* Het doel van deze pilot is gericht op een efficiënter en effectiever screeningsproces van de handbagage. Dit middels de inzet van software die op basis van algoritmen handbagage scant en bins die bijna leeg zijn automatisch kan goedkeuren.	zal worden gebruikt voor verdere doorontwikkeling van de screening van handbagage[130]. Op 6 februari 2015 is regelgeving uitgebracht die gericht is op het beveiligingsonderzoek van handbagage met behulp van explosieven detectiesoftware waarbij het tevens toegestaan wordt om laptops en vloeistoffen in de tas te houden[131]. *Pilot ATIX Laptops in bags trail Schiphol* Op 2 juni 2014 is de pilot ATIX Laptops in bags trial Schiphol gestart. Gedurende deze pilot mochten passagiers de laptop in de handbagage laten. Vervolgens werd de handbagage met laptop gescreend door specifieke apparatuur en software. Uit de pilot is naar voren gekomen dat met de huidige techniek nog niet de gewenste resultaten worden behaald en leidt tot problemen in het operationele proces. Verdere ontwikkeling is daarom nog nodig[132]. *CTI TIP trial* De pilot is in juni 2015 van start gegaan. In de voortgangsrapportage van december 2015 is opgenomen dat de veronderstellingen van de toepassing van fictieve dreigingsvoorwerpen in handbagage in de tweede fase van de pilot worden getoetst. Dit is na de periode van deze beleidsdoorlichting[133]. Wel is op Europees niveau de regelgeving aangepast, zodat de implementatie van de pilot mogelijk is[134].	die handbagage controleert met behulp van explosievendetectiesoftware.

130 Brief NCTV, onderwerp: Concerning Final progress report Schiphol laptops and liquids in bags, kenmerk: 672229, 4 augustus 2015.
131 EC-regulation L 31/18, tot wijziging van verordening EU(185/2010) voor wat betreft beveiligingsonderzoeken van handbagage, 7 februari 2015
132 Brief NCTV, onderwerp: Concerning Final report Schiphol trial lLaptops in bags.kenmerk: 671761, 4 augustus 2015.
133 Brief NCTV, onderwerp: First Progress report CTI TIP trial, kenmerk: 719618, 23 december 2015.
134 EC-regulation L 299/134, paragraph 12.5 Threat Image Projection (TIP), 14 november 2015

	Pilot 'Laptops and liquids in bags' Met deze pilot wordt gezocht naar een meer gebalanceerde detectiemogelijkheid tegen de actuele hedendaagse dreigingen, waarbij passagiers hun laptops en vloeistoffen in de tas mogen houden. De pilot dient te bevestigen of de werkwijze bijdraagt aan een efficiëntere en effectievere aanpak en daarmee voordelig is voor de passagier en het beveiligingsniveau. *Pilot ATIX Laptops in bags trail Schiphol* Het doel van de pilot was net als bij bovenstaande pilot om ervaring op te doen met oplossingen waarbij laptops in de bagage konden blijven van passagiers gedurende de screening. *CTI TIP trial* Het doel van deze pilot is om onderzoek te doen naar de realistische toepassing van fictieve dreigingsvoorwerpen in handbagage. De verwachting is deze werkwijze leidt tot betere prestaties van screeners. Waar voorheen fictionele items werden toegevoegd aan bestaande bagage, kan met behulp van CTI een fictionele threat item worden toegevoegd aan fictionele bagage. Dit levert een		

	realistischer beeld en de screener zal minder snel door hebben dat het gaat om een test. Centraal screenen met behulp van RCBS heeft daarbij nog als voor dat de workload van de verschillende lanes optimaal kan worden gescreend, omdat pieken van verschillende lanes centraal kan worden opgevangen.		
51.	*Creëren van (inter)nationaal draagvlak* Om draagvlak te creëren voor bovenstaande projecten zijn op regelmatige basis op initiatief van de NCTV presentaties gehouden voor o.a. partner organisaties, Europese Commissie, IATA en lidstaten tijdens overleggen, seminars, congressen en bezoeken. Dit draagvlak is nodig omdat voor een aantal pilots de regelgeving moest worden aangepast om nieuwe technologieën te kunnen toepassen.	Uit de beschrijvingen bij de verschillende pilots blijkt dat regelgeving op EU niveau is aangepast. Dit is niet alleen de verdienste van de NCTV, maar de NCTV heeft hier wel aan bijgedragen. De bijdrage van de NCTV aan de pilot houdt op zodra de nieuwe toepassingen in regelgeving zijn opgenomen. De NCTV heeft bij diverse symposia, bijeenkomsten en overleggen presentaties gehouden over ontwikkelingen in het kader van deze projecten. Er is op internationaal niveau (IATA) circa 2 maal per jaar een stuurgroepbijeenkomst gehouden om af te stemmen over de toepassing van de nieuwe concepten/pilots wereldwijd.	

Bijlage 6 : Overzicht beleidsinstrumenten nationale veiligheid en crisisbeheersing 2011-2015

Nr.	Doelstelling en instrumenten	Realisatie en werkbaarheid[135]	Specifiek uitgevoerde evaluatie(s) doeltreffendheid en doelmatigheid instrument[136]
Verbeteren van het functioneren van het stelsel crisisbeheersing door coördinatie en vereenvoudigen van besluitvorming			
Versterken nationale crisisorganisatie			
1.	*Vergroten efficiency en effectiviteit van de crisisbesluitvorming* a) Ontwikkelen gezamenlijke functies en kwaliteitseisen voor crisisfunctionarissen en deze verankeren in het stelsel van de crisisbeheersing.[137] b) De crisisorganisatie verder vereenvoudigen en flexibiliseren. Uitgangspunt daarbij is het verkleinen van de afstand tussen (strategische) besluitvorming en de operationele praktijk. De afspraken opnemen in het Nationaal Handboek Crisisbesluitvorming en in het Instellingsbesluit Ministeriële Commissie Crisisbeheersing 2013.[138]	a) Op 3 september 2013 heeft het IOCB een herijkte versie van het Rollenhuis Crisisbeheersing vastgesteld, waarin de rollen binnen de crisisbeheersingsorganisatie met bijhorende competenties, taken en functies zijn gedefinieerd. Deze wordt in de nationale crisisstructuur gebruikt. Deze uniformiteit bevordert de professionaliteit van de crisisorganisatie. De rollen worden tevens gebruikt bij het vormgeven, opleiden en trainen en oefenen van de crisisbeheersingsorganisatie.[139] b) Verschillende aanpassingen doorgevoerd om de nationale crisisorganisatie meer flexibel te laten functioneren om in crises maatwerk te kunnen bieden. De betreffende aanpassingen zijn uitgewerkt in het aangepaste Instellingsbesluit Ministeriële Commissie Crisisbeheersing 2016 (Stcrt. 2016, nr. 48258) en in het aangepaste Nationaal Handboek Crisisbesluitvorming (NHC).[140]	Onderdeel in: Evaluatie Wvr Rapport evaluatiecommissie Hoekstra Wet evaluatie veiligheidsregio's Staat van rampenbestrijding 2013

135 De hieronder beschreven informatie over de realisatie en werkbaarheid van de verschillende instrumenten is - tenzij met een aparte voetnoot aangegeven – afkomstig uit de Voortgangsrapportages Actieprogramma Integrale Aanpak Jihadisme 1 t/m 6.

136 Hier worden alleen beschikbare evaluaties genoemd die uitspraken doen over de doeltreffendheid en/ of doelmatigheid van het specifieke instrument; als die er niet zijn blijft cel leeg.

137 Opstelten (2013), Kamerbrief 29517, nr. 76.

138 Van der Steur (2015), Kamerbrief 30821, nr. 23.

139 Herijking rollenhuis crisisbeheersing Rijksoverheid d.d. 3 september 2013

140 Van der Steur (2016), Kamerbrief 30821, nr. 32. Dit kamerstuk is van 2016, maar is wel opgenomen in het overzicht dat gaat over de periode 2011-2015. Deze keuze is gemaakt omdat het stuk een opsomming geeft van werkzaamheden die (deels) zijn uitgevoerd in de relevante periode (2011-2015).

2.	*Vergroten van het inzicht in risico's en capaciteiten* De overheid wil voorkomen dat de maatschappij ontwricht raakt door een ramp of crisis. Daarom onderzoekt zij onder andere met de Strategie Nationale Veiligheid welke dreigingen de nationale veiligheid in gevaar kunnen brengen en wat men daaraan kan doen.[141] De NCTV vervult een coördinerende rol in de totstandkoming van de Strategie Nationale Veiligheid. Hiertoe stelt het Analistennetwerk Nationale Veiligheid een nationale risicobeoordeling (NRB) op en worden capaciteitenanalyses uitgevoerd om de weerbaarheid in kaart te brengen.	Tot 2014 werd de Nationale Risicobeoordeling (NRB) uitgebracht, waarin elk jaar een aantal typen rampen en dreigingen werd geanalyseerd in de vorm scenario's die werden beoordeeld met behulp van een vaste meetlat. Bij elkaar zijn sinds de aanvang van de Strategie Nationale Veiligheid (2007) ongeveer 50 scenario's ontwikkeld op een groot aantal thema's.[142] In 2014 heeft de Stuurgroep Nationale Veiligheid besloten de NRB door te ontwikkelen tot het Nationaal Veiligheidsprofiel. Het NVP wordt als onderdeel van de Strategie Nationale Veiligheid geproduceerd door het Analistennetwerk Nationale Veiligheid (ANV) in opdracht van de Stuurgroep Nationale Veiligheid (SNV) en bevat een All Hazard overzicht van de belangrijkste risico's voor de nationale veiligheid. De NVP wordt elke 4 jaar uitgebracht. De eerste NVP is uitgebracht in 2016[143]. Mede op basis van het NVP en met input vanuit capaciteitenanalyses kan worden bezien op welke manier de nationale veiligheid kan worden versterkt. Uit onderzoek van de Algemene Rekenkamer[144] blijkt dat de minister van VenJ eind 2013 geen integraal zicht had op de capaciteiten die bij de veiligheidsregio's en andere crisispartners daadwerkelijk aanwezig zijn. Het Ministerie van VenJ was wel bezig met een inventarisatie hiervan. De tot nu toe uitgevoerde analyses en de daarop door het kabinet genomen maatregelen richten zich vooral op het maken van plannen, onderzoek doen, evaluaties uitvoeren, enzovoort. De uitgevoerde analyses geven geen concreet antwoord op de vraag hoeveel mensen, middelen en methoden nodig zijn voor welke ambitie.	

141 URL: https://www.nctv.nl/organisatie/nationale_veiligheid/strategie_nationale_veiligheid/index.aspx (geraadpleegd: 7 augustus 2017)
142 Analistennetwerk Nationale Veiligheid (2016), Nationaal veiligheidsprofiel 2016.
143 Analistennetwerk Nationale Veiligheid (2016), Nationaal veiligheidsprofiel 2016.
144 Algemene Rekenkamer (2014), Rapport Zicht overheden op beschermen burgers en bedrijven, november 2014

3.	*(Laten) ontwikkelen specifieke nationale crisisplannen* Mede op basis van de risico's in de NRB zijn er specifieke crisisplannen ontwikkeld. Het doel van deze specifieke crisisplannen is om zo optimaal mogelijk te kunnen reageren op specifieke vormen van crisis.	In de afgelopen jaren zijn verschillende nationale crisisplannen ontwikkeld, zoals voor hoogwater en overstromingen, luchtvaartongevallen, ICT, elektriciteit etc. Dit is mede gebeurd op basis van de uitkomsten van de nationale risicobeoordelingen.[145]	
4.	*Rijksbreed systeem van opleiden, trainen, oefenen, evalueren en leren* Onderdeel van een kwalitatief goede nationale crisisorganisatie zijn professioneel toegeruste crisisfunctionarissen en een sterk en flexibel (rijksbreed) crisisnetwerk. Om te zorgen voor rolgerichte opleidingen en trainingen en blijvend te leren en structureel lessen te trekken uit incidenten, crises en oefeningen heeft de minister de Nationale Academie voor Crisisbeheersing (NAC) in het leven geroepen.[146]	De afgelopen periode heeft de NAC haar leerprogramma voor crisisprofessionals volledig uitgevoerd. De inhoudelijke thema's waren o.a. de troonswisseling en de Nucleair Security Summit 2014 (NSS). De geleerde lessen zijn meegenomen bij het versterken van de crisisorganisatie en bij het ontwikkelen van het nieuwe leerprogramma. Nieuwe focusgebieden in de leerprogramma's zijn o.a.: vitale infrastructuur, cybersecurity, nucleair en overstromingen.[147] Naast de Interdepartementale Basisopleiding Crisisbeheersing (IBC) zijn voor alle rollen in het Rollenhuis Crisisbeheersing Rijksoverheid[148] specifieke rolgerichte trainingen ontwikkeld, bestaande uit roltrainingen voor specifieke crisisrollen, teamtrainingen en masterclasses.	
5.	*Realiseren voorzieningen om continuïteit van de rijkscrisisfunctie te waarborgen* Het doel van de uitwijklocatie is het waarborgen van de continuïteit van de rijkscrisisfunctie, 24 uur per dag, 365 dagen per jaar.[149]	Op 9 juli 2013 is het Convenant Uitwijk Rijkscrisisfunctie getekend. [150]	

145 Nationaal Crisisplan ICT, Nationaal Crisisplan Luchtvaartongevallen Burgerluchtvaart,Voortgangsbrief Nationale Veiligheid, d.d. 15 september 2016 pag. 3- 4
146 Opstelten (2014), Kamerbrief 29517, nr. 85.
147 Opstelten (2014), Kamerbrief 29517, nr. 85.
148 Herijking rollenhuis crisisbeheersing Rijksoverheid d.d. 3 september 2013
149 Opstelten (2012), Kamerstuk 33400, VI, nr. 2
150 Ministeries van Defensie en Veiligheid & Justitie (2013), Convenant Uitwijk Rijkscrisisfunctie.

6.	*Onderhoud Nationaal Crisiscentrum (NCC)* Het NCC draagt zorg voor samenhang in besluitvorming bij een crisis of dreigende crisis ten behoeve van de veiligheid van burgers[151.] In 2012 besloot het kabinet om het crisiscommunicatieteam van het NCC te versterken om de veiligheidsregio's te faciliteren met advies en middelen.[152]	Naar aanleiding van het advies van de bestuurlijke werkgroep Bovenregionale Samenwerking (2012)[153] is een afsprakenkader met spelregels uitgewerkt voor de één-loket-functie en een factsheet voor de regio's met daarin beschreven hoe het NCC werkt. Ook is er een bijlage opgesteld met een uitgebreidere beschrijving van het NCC, haar producten en diensten.[154] Zoals toegezegd door het kabinet is ook het crisiscommunicatieteam van het NCC versterkt.[155]	
7.	*Onderhoud opgeschaald Landelijk Operationeel Coördinatiecentrum (LOCC)* De NCTV investeert onder andere in de aansluiting van het LOCC op de 112 centrale en Operations van de Nationale Politie. Mede op basis van de verstrekte informatie wordt het landelijk beeld gevormd dat uiteindelijke door het LOCC wordt ontsloten voor de veiligheidsregio's via het LCMS (landelijk crisismanagement systeem).	Het LOCC heeft afspraken met zowel de afdeling preparatie als met (de informatieorganisatie van) het Operations Center (waaronder ook de relevante informatie van 112 centrale) van de Nationale Politie / Landelijke Eenheid. Op dagelijkse basis wordt wederkerig operationele informatie uitgewisseld door de informatiemanagers van alle partijen. Dit gebeurt in persoon of telefonisch.[156] Daarnaast is het LOCC aangesloten op het LCMS[157]	Onderdeel in Evaluatie Wvr: In de interviews die gehouden zijn in het kader van deze evaluatie komt het verzoek om het verlenen van bijstand vanuit het landelijke niveau en van naburige regio's regelmatig aan de orde. Er wordt door geïnterviewden aangegeven dat het feitelijk verlenen van bijstand goed verloopt. Formeel moet bijstand worden aangevraagd en verleend via de minister van VenJ – die hiervoor het LOCC heeft ingesteld. Sommige geïnterviewden geven aan dat zij de weg via het LOCC omslachtig vinden in een crisissituatie. Vaak wordt bijstand dan ook verleend door de buurregio en wordt dit achteraf 'gelegaliseerd'.[158]

151 NCTV en Veiligheidsberaad (2013), Eenheid in verscheidenheid.
152 Opstelten (2012), Voortgangsbrief nationale veiligheid.
153 NCTV en Veiligheidsberaad (2013), Eenheid in verscheidenheid.
154 NCTV en Veiligheidsberaad (2013), Eenheid in verscheidenheid. Bijlage 3.
155 NCTV (2012), Nota aan de leden van de bestuursraad inzake versterking crisiscommunicatie.
156 LOCC (2017), Werkinstructie Informatie coördinator.
157 Staat Netcentrisch Werken 2015, TNO
158 Van Veldhuisen e.a. (2013), Evaluatie Wet veiligheidsregio's.

Versterken presterend vermogen veiligheidsregio's en Caribisch Nederland			
8.	*Evalueren van de Wet veiligheidsregio's* Een evaluatieonderzoek naar de Wet veiligheidsregio's om te bezien in hoeverre de wet in de praktijk aan de verwachtingen voldoet wat betreft het functioneren van het stelsel (de realisatie van de aannames over het bijdragen aan een efficiënte en kwalitatief hoogwaardige organisatie van de brandweerzorg, geneeskundige hulpverlening, rampenbestrijding en crisisbeheersing onder één regionale bestuurlijke regie) en hoe actoren dat ervaren.	Het evaluatieonderzoek naar de Wet veiligheidsregio's is uitgevoerd[159]. De periode na het onderzoek heeft vooral in het teken gestaan van (verbeter)acties op basis van de uitkomsten. De Tweede Kamer is periodiek over de voortgang geïnformeerd.[160]	Evaluatie Wvr: In het algemeen hebben het ontwikkelen van de veiligheidsregio's een gunstig effect gehad op de kwaliteit en effectiviteit van de rampenbestrijding. De invoering van de Wet veiligheidsregio's heeft gezorgd voor een vergroting van expertise, een versterking van operationele slagkracht en vergroting van de effectiviteit. De Commissie concludeert dat dankzij de wet verbeteringsprikkels zijn gecreëerd en is de mogelijkheid ontstaan om op een hoger dan gemeentelijk niveau te werken aan een goede voorbereiding op rampen en crises.
9.	*Verbeteren van de regelgeving voor veiligheidsregio's* Mede op basis van de uitkomsten van de evaluatie op de Wet Veiligheidsregio's de regelgeving aanpassen en actualiseren.	De aanpassingen van wet- en regelgeving op basis van de uitkomsten uit de evaluatie zijn per 1 januari 2016 in werking getreden.[161.]	Evaluatie Wvr
10.	*Verbeteren van de ondersteuning van veiligheidsregio's* Oprichting Instituut Fysieke Veiligheid (IFV).	Op 1 januari 2013 is het IFV opgericht.[162]	Evaluatie WvR: Van het IFV wordt verwacht dat het een leidende rol kan spelen in de doorontwikkeling van het domein. In hoeverre het IFV daarin slaagt, is op dit ogenblik niet te voorzien.

159 Van Veldhuisen e.a. (2013), Evaluatie Wet veiligheidsregio's.

160 Kamerbrief 29517-69

161 Staatsblad 2015-381

162 Staatsbladen 2012-443 en 2012-526

11.	*Brede Doeluitkering (BDUR) aan de veiligheidsregio's en de herijking en actualisatie daarvan* Mede door een bijdrage op basis van het Besluit Veiligheidsregio's worden de veiligheidsregio's in staat gesteld uitvoering te geven aan het beleid met betrekking tot brandweer, geneeskundige hulpverlening, rampenbestrijding en crisisbeheersing	De aangepaste regelgeving is per 1 januari in werking getreden.[163] In 2015 heeft Cebeon onderzoek uitgevoerd naar (de verdeling van) de BDUR[164]. Om tot een betere verdeling te komen is de verdeelformule op basis van het uitgevoerde onderzoek in het Besluit Veiligheidsregio's aangepast.	Rapport Evaluatie commissie Hoekstra en Evaluatie Wvr: Deze soms moeizame verdelingsdiscussies geven wel eens aanleiding tot de gedachte dat het hybride financieringsstelsel beter kan worden opgeheven. In plaats daarvan zou het rijk de veiligheidsregio's voor honderd procent rechtstreeks moeten financieren via een rijksbijdrage. De Evaluatiecommissie is geen voorstander van een verandering in de financiering. Een wijziging als hiervoor gesuggereerd zou weliswaar het einde van moeizame discussies betekenen maar tevens het einde van het begrotingsrecht van de gemeente. Daarmee ligt de bijl aan de wortel van het stelsel van verlengd lokaal bestuur. Uiteraard zal de gemeentelijke afdracht aan de veiligheidsregio toereikend moeten zijn voor het vereiste noodzakelijke niveau van veiligheid in de regio. Om de transparantie betreffende kosten en baten te vergroten, dient de besteding van de budgetten inzichtelijker te worden. De Evaluatiecommissie beveelt daarnaast aan de Brede doeluitkering rampenbestrijding (BDUR) om te vormen van een lumpsumuitkering naar een gerichte bijdrage aan de veiligheidsregio's, toegespitst op het realiseren van specifieke landelijke doelstellingen. Daarmee kan het

163 Staatsblad 2015-381
164 Rapport Cebeon, 2015.

			landelijk afgedragen budget bijdragen aan de verwezenlijking van landelijk gestelde doelen. Met behulp van deze financieringswijze ook de besteding van het beschikbaar gestelde budget inzichtelijker worden[165].
12.	*Versterken brandweer door:* a) de regionalisering. b) onderzoek naar opkomsttijden en variabele voertuigbezetting. c) verbetering van de brandweerstatistiek (door onderzoek). d) convenant ter verbetering van het brandweeronderwijs.	a) Per 1 januari 2014 is de brandweer (verplicht) geregionaliseerd. [166] b) Meerdere onderzoeken rond opkomsttijden en voertuigbezetting plaatsgevonden. [167] c) Vanaf 29 en 30 september 2015 publiceert het CBS de verbeterde brandweerstatistiek. [168] d) Convenant gesloten op 24 juli 2012. [169]	Evaluatie Wvr Convenant Versterking brandweeronderwijs in NL Eindrapportage inzake uitvoering convenant.[170]
13.	*Versterken Geneeskundige Hulpverleningsorganisatie in de Regio (GHOR)* a) Vastleggen van bekwaamheidseisen GHOR-functionarissen in Bpv b) Afspraken over de rol van het Rode Kruis bij rampen en crisis en over de Grootschalige Geneeskundige Bijstand.	a) Bekwaamheidseisen GHOR-personeel zijn vastgelegd. [171] b) Alle Veiligheidsregio's/GHOR-bureaus en het Rode Kruis hebben aparte convenanten afgesloten. Hierin is vastgelegd dat het Rode Kruis zorg draagt voor noodhulpteams (NHT) om lichtgewonde slachtoffers te verzorgen ter ontlasting van de ambulancezorg.[172]	Evaluatie Wvr

165 Eindrapportage Evaluatiecommissie Wet veiligheidsregio's en het stelsel van Rampenbestrijding en Crisisbeheersing, Evaluatiecommissie Hoekstra, 18 september 2013, p.31
166 Staatsbladen 2012- 443 en 2012-526 en TK 32 841 nr. 62.
167 o.a. rapport RemBrand. Kamerbrief 219517-105 + bijlage 626393; Tussenrapportage variabele voertuigbezetting, IOOV, okt 2011 (TK 29 517, nr. 53); Uitruk op maat, rapportage project variabele voertuigbezetting, NVBR, juli 2012; Ter plaatse, Inspectieonderzoek naar opkomsttijden en dekkingsplannen, juni 2012 (TK 29 517 nr. 60); brief TK ontwikkelingen variabele voertuigbezetting (TK 29 517 nr. 66); Inspectierapport Dekkingsplannen 2013, IVenJ, sept 2013 (TK 29 517 nr. 73); WODC onderzoek "Beoordelingskader effecten variabele voertuigbezetting', nov 2013 (TK 29 517 nr. 82).
168 brief 29517-123; WODC onderzoek Inventarisatie informatiebehoefte brandweerstatistiek, 2012 brieven aan TK 30 821 nr.62 en 26 956 nr.113
169 Staatscourant, Jaargang 2012,Nr. 15261
170 Stuurgroep Versterkingsplan Brandweeronderwijs (2015), Verantwoording project Vbo. Kenmerk: BA 150170.
171 Regeling personeel veiligheidsregio's.
172 Minister van Veiligheid en Justitie (2014 en 2016), Subsidie NRK 2015 en 2017. Kenmerk: 577020 en 2011678

14.	*Versterken crisisbeheersing Caribisch Nederland* Door invoering en bevorderen van de implementatie van wet- en regelgeving crisisbeheersing en brandweerzorg Caribisch Nederland. Dit door onder andere ondersteuning te bieden bij de planvorming.	De NCTV heeft in 2013 aangekondigd een bijdrage over te maken ter ondersteuning van de rampenbestrijdingsplannen op Bonaire, Sint Eustatius en Saba (BES). [173] Deze bijdrage is sindsdien jaarlijks aan de eilanden verstrekt. Er is in de beschreven periode veel in gang gezet in de voorbereiding op rampen en crises en er zijn diverse inspecties uitgevoerd. Zowel bestuurlijk als operationeel is er veel aandacht voor opleiden, trainen en oefenen.[174] Ook heeft in opdracht van VenJ ondersteuning van de planvorming voor de eilanden plaatsgevonden.	
Versterken samenwerking			
15.	*Versterking van de aansluiting Rijk – regio* Versterking van de bovenregionale samenwerking en de samenwerking tussen regio's door: a) Het realiseren van een opschalingstructuur waarin helder is opgenomen op welk moment de Rijksoverheid een taak heeft en de wettelijke verankering daarvan. b) Instellen c.q. versterken van Crisis Expert Teams. c) het bevorderen dat de Nationale Risicobeoordeling en de risicoprofielen van de veiligheidsregio's beter op elkaar worden afgestemd.	a) In het Nationaal Handboek Crisisbesluitvorming is GRIP RIJK (als aanduidingsterm) geïntroduceerd en de GRIP opschalingstructuur opgenomen. Inmiddels is de term GRIP Rijk overbodig geworden, omdat het NCC bij een crisis de betrokken partners, waaronder de veiligheidsregio's, direct informeert over de rol.[175] In het Besluit veiligheidsregio's is vastgelegd dat de veiligheidsregio's een uniforme opschalingsprocedure hanteren (Besluit veiligheidsregio's, artikel 2.3.1, eerste lid) b) De rol van vraagregisseur en Crisis Expert Team (CET) zijn uitgewerkt. Op regionaal niveau wijst de hoogst operationeel leidinggevende bij een incident een "single point of contact" aan. In de loop van een incident kan de rol van vraagregisseur van persoon wisselen. De vraagregisseur schakelt met de voorzitter van het CET bij een adviesvraag aan een CET. [176]	

173 Minister van Veiligheid en Justitie (2013), Ondersteuning rampenbestrijdingsplannen BES. Kenmerk: 458824
174 kamerbrief -34300 IV-55 met bijlage 727920 (Inspectiebrede rapportage crisisbeheersing Caribisch Nederland)
175 Kamerbrief 30821-32
176 VB vergadering 20 maart 2015 Oplegnotitie agendapunt 10 bovenregionale samenwerking; DB/VB op 23 september 2015; Vraagregisseur en BTC (Vraag 49 en 50) 2 juli 2014 verzamelbrief aan Kamer Tweede Kamer, vergaderjaar 2013–2014, 29 517, nr. 85; Voortgangsbrief NV 2015, TK 30821-23

		c) De NCTV heeft een financiële bijdrage aan het Instituut Fysieke Veiligheid IFV verleend om in opdracht van het Veiligheidsberaad een onderzoek naar de regionale risicoprofielen te verrichten. De aansluiting op het Nationaal Veiligheidsprofiel maakt hiervan onderdeel uit.[177]	
16.	*Bevorderen samenwerking door gezamenlijke vaststelling en uitvoering prioriteiten en doelstellingen* Bevorderen dat het Rijk, het Veiligheidsberaad, de veiligheidsregio's en vitale sectoren/partners werken aan gezamenlijk vastgestelde prioriteiten en doelstellingen.	Sinds 2010 zijn er meerdere convenanten opgesteld tussen veiligheidsregio's en vitale partners/sectoren[178]. In de jaren daarna is de behoefte aan een gezamenlijke agenda tussen het Veiligheidsberaad en het Rijk ontstaan. Dit resulteerde in 2014 in een Strategische Agenda[179]. In juni 2015 stemde het Veiligheidsberaad in met de uitvoering zes prioritaire thema's van de Strategische Agenda: Gezamenlijke prioriteiten Veiligheidsberaad en Ministerie van VenJ • Water en evacuatie • Continuïteit van de samenleving • Versterking risico- en crisisbeheersing bij stralingsincidenten Prioriteiten Veiligheidsberaad en veiligheidsregio's • Kwaliteit en vergelijkbaarheid • Versterking bevolkingszorg • Bovenregionale operationele besluitvorming Anno 2017 zijn er (m.u.v. versterking bevolkingszorg) eindrapportages verschenen t.a.v. de thema's.	

177 Minister van Veiligheid en Justitie (2016), Bijdrage verkenning regionale risicoprofielen. Kenmerk: 2014159.
178 Auteur onbekend, (jaartal onbekend), 'Bestuurlijke eindrapportage' Project continuïteit van de samenleving.
179 Veiligheidsberaad (2014), Strategische Agenda Versterking Veiligheidsregio's 2014-2016.

17.	*Versterking van de civiel-militaire samenwerking (VCMS) door* a) Onderzoek naar kansrijke mogelijkheden b) Ontwikkelen catalogus c) Instellen taskforce OTOTEL	a) De samenwerking tussen de veiligheidsregio's en Defensie maakt deel uit van de Strategische Agenda van het Veiligheidsberaad en is het tot prioriteit benoemd. Het Veiligheidsberaad heeft het initiatief genomen om een werkgroep VCMS op te richten in aanvulling op de bestaande VCMS structuur en met het accent op de veiligheidsregio's om de civiel militaire samenwerking verder te helpen versterken. Deze werkgroep richt zich onder andere op de aanbevelingen uit de recent afgeronde quickscan onder de gevleugelde titel ' wees niet te bescheiden in welke effecten u vraagt'. Dit verkennende onderzoek, op initiatief van het Veiligheidsberaad, gaat met name over de samenwerking tussen Defensie en de veiligheidsregio's. Tevens is Defensie vertegenwoordigd in de bestuurlijke adviescommissie crisisbeheersing van het Veiligheidsberaad. [180] b) De oorspronkelijke catalogus is in 2015 omgewerkt naar een interactieve catalogus. Daarin staan de gegarandeerde capaciteiten die Defensie levert. Ook fungeert het als naslagwerk voor de crisisbeheersing met relevante informatie over o.a. wetgeving, procedures, richtlijnen, regio-indelingen en diverse links naar bronnen van (partner)organisaties.[181] c) Er is een Taskforce OTOTEL ingesteld met als taak om concrete werkafspraken te maken over gezamenlijke inspanningen in een actieprogramma. Na afronding van het initiële actieprogramma is ambtelijk besloten om de Taskforce te handhaven als Platform OTOTEL.[182]	

180 Civiel –militaire samenwerking Eindmeting 2013 door Audit Functie Defensie & Inspectie Veiligheid en Justitie. Link: https://www.rijksoverheid.nl/documenten/rapporten/2014/04/15/civiel-militaire samenwerking-eindmeting-2013; Kamerbrief over de eindmeting: https://www.rijksoverheid.nl/documenten/kamerstukken/2014/04/15/eindmeting-icms-2013; Link naar quickscan: https://www.ifv.nl/kennisplein/Documents/rapport-vb-compleet-vcms-2014-maart.pdf

181 Link naar de catalogus: https://www.defensie.nl/onderwerpen/taken-in-nederland/downloads/brochures/2016/09/09/catalogus-nationale-operaties-pdf-versie

182 Kamerbrief 29715 -85

18.	*Versterken themagerichte aanpak door* a) Het ontwikkelen van producten voor grootschalige evacuaties in het project Grootschalige Evacuatie b) Het versterken van de organisatorische voorbereiding op de 'nafase' met specifieke aandacht voor de opvang en zorg voor getroffenen en herstel en wederopbouw c) Het versterken van de CBRN–respons door de multidisciplinaire samenwerking bij CBRN te vergroten en het versterken van (generieke) CBRN capaciteiten in het kader van het EU Actieplan.	a) In 2014 is het Kader grootschalige evacuatie opgeleverd. Dit Kader dient als vertrekpunt voor het op te stellen Nationaal Crisisplan Evacuatie. b) In het Nationaal Handboek Crisisbesluitvorming is reeds voor 2011 vastgelegd dat de minister van (nu VenJ) verantwoordelijk is voor de coördinatie en organisatie van de nafase. Ook zijn interdepartementaal de generieke thema's geïdentificeerd en toebedeeld. In de periode 2011-2015 zijn de genoemde thema's actueel gehouden en zijn uiteindelijk in de wijziging van het Nationaal Handboek Crisisbesluitvorming in 2016 aangepast. Er is/was geen reden om de in het Nationaal Handboek Crisisbesluitvorming beschreven procedure ten aanzien van de nafase aan te passen. c) *Ten aanzien van de voorbereiding***:** • Het Nationaal Trainingscentrum CBRN te Vught is in 2014 geopend[183]. Effectuering van VCMS afspraken DEF/BZK uit 2006. Sinds dat moment hebben er groot aantal trainingen en oefeningen plaatsgevonden door operationele partijen[184] • Het ministerie van Defensie heeft verder in het kader van de civiel militaire samenwerking een CBRN responseenheid ingericht, welke met advies, capaciteit en middelen de civiele partijen bij kan staan ingeval van CBRN incidenten https://www.dcbrnc.nl/cbrn-responseenheid . • Diverse protocollen zijn geactualiseerd, zoals o.a. het PVO 2015 per 1-1 2016 in werking (actualisatie van PVO 2006). Geactualiseerd in opdracht NCTV. Het PVO beschrijft hoe operationele teams vanuit verschillende organisaties samenwerken en moeten omgaan met verdachte objecten die gevaarlijke stoffen kunnen bevatten, zoals explosieven of chemicaliën.	

183 Voortgangsbrief Nationale veiligheid 2015 (12 mei 2015) https://www.rijksoverheid.nl/documenten/kamerstukken/2015/05/14/tk-voortgangsbrief-nationale-veiligheid
184 https://www.dcbrnc.nl/opleiding-en-training .

		• Oefeningen op zowel strategisch als operationeel niveau georganiseerd. Zowel binnen Nederland als internationaal. Voorbeelden hiervan zijn de @tomic oefeningen in 2012185/2014186 *Ten aanzien van het voorkomen van gebruik CBRN-E middelen:* • Realisatie van de op 1 juni 2016 in werking getreden Wet precursoren voor explosieven[187.] • Meldingen van verdachte transacties worden gedaan bij het Meldpunt Verdachte Transacties Chemicaliën (samenwerkingsverband nationale politie en FIOD).[188] • Informatiecampagnes richting bedrijven t.a.v. omgang met potentiële aanslagmiddelen (CBRN-E).[189] • Sinds augustus 2014 zijn tientallen detailhandelketens, groothandels, producenten en brancheorganisaties bezocht om hen te informeren over maatregelen ter preventie van terrorisme, de nieuwe regels en om afspraken te maken over de uitvoering daarvan[190.]	
19.	*Versterking samenwerking Reddingsbrigade Nederland en de veiligheidsregio's* Door afspraken te maken met de Reddingsbrigade NL over opbouw van Regionale Voorziening Reddingsbrigades; dit zijn samenwerkingsverbanden van de	De Regionale Voorziening Reddingsbrigade is gerealiseerd.[191]	

185 Atomic 2012 - An Exercise in Perspective
186 @tomic 2014 evaluation
187 Zevende voortgangsrapportage Integrale Aanpak Jihadisme plus beleidsbrief (14 nov 2016) https://www.rijksoverheid.nl/documenten/rapporten/2016/11/14/bijlage-1-zevende-voortgangsrapportage-integrale-aanpak-jihadisme
188 Vierde voortgangsrapportage Integrale Aanpak Jihadisme (9 nov 2015) https://www.nctv.nl/binaries/kamerbrief-vgr-4-actieprogramma-integrale-aanpak-jihadisme-def_tcm31-31640.pdf
189 https://www.nctv.nl/onderwerpen_a_z/Beveiliging-CBRN-stoffen/index.aspx https://www.nctv.nl/binaries/folder-cbrn-security-maart2014_tcm31-32677.pdf , https://www.nctv.nl/binaries/j-23977-nw-handleiding-screening-cbrn_tcm31-32681.pdf (product voorbeelden)
190 https://www.nctv.nl/binaries/bijlage-1-voortgangsrapportage-actieprogramma-intergrale-aanpak-jihadisme_tcm31-32365.pdf
191 Kamerbrief 29517-117 en 29517-123

	reddingsbrigades op de schaal van de veiligheidsregio's.		
20.	*Bevorderen van de internationale samenwerking* Door onder andere te participeren in Europese activiteiten en bij te dragen aan EU mechanisme, NATO en bilateraal	Nederland neemt deel actief deel aan EU fora PROCIV en CPC en het NAVO forum CEPC. In deze fora heeft NL de afgelopen periode aandacht gevraagd voor preventie, intensievere EU-NAVO samenwerking, hybride dreigingen, terrorismegevolgbestrijding en vitale infrastructuur. Met name hybride dreigingen heeft als onderwerp de afgelopen periode aan aandacht gewonnen in EU en NAVO verband, zo is oa met NL steun een nieuwe FoP hybride dreigingen opgezet binnen de EU.[192] Per 1 januari 2014 is het EU besluit 1313/2013 inzake de EU Civiele Bescherming Mechanisme van kracht. Het Mechanisme heeft als doel versterking van de efficiëntie, effectiviteit en coherentie van de EU rampenrespons. De EU-wetgeving (Besluit 1313/2013) richt zich slechts tot de internationale samenwerking (in en buiten de EU). In tegenstelling tot de voorgaande EU-regelgeving waar slechts de EU-samenwerking in de responsfase wordt behandeld, worden in de huidige EU-wetgeving alle fases van de veiligheidsketen behandeld. Het Mechanisme is gebaseerd op een structuur bestaande uit een Coördinatiecentrum voor respons in noodsituaties (ERCC), een Europese responscapaciteit voor noodsituaties in vorm van een vrijwillige pool van vooraf vastgestelde capaciteiten van de EU lidstaten en ervaren deskundigen, een door de Europese Commissie beheerd gemeenschappelijk noodcommunicatie- en informatiecentrum (CECIS) en contactpunten in de EU lidstaten.	

192 Agenda's, verslagen en producten van Civil Protection Committee, PROCIV

Versterken informatievoorziening en crisiscommunicatie			
21.	*Streven naar uniformiteit* Om de uniformiteit in de informatievoorziening en crisiscommunicatie te bevorderen, heeft de minister VenJ overleg met de besturen van de veiligheidsregio's. In deze overleggen gaat het over de wijze waarop kan worden geborgd dat alle veiligheidsregio's gebruik maken van dezelfde standaarden, zodat informatie zowel interregionaal als bovenregionaal kan worden uitgewisseld.	Een en ander heeft geleid tot het Programma Informatievoorziening Veiligheidsregio's 2015 - 2020.[193] Dit plan is goedgekeurd door het Veiligheidsberaad op 12 juni 2015. Onder dit programma worden zes projecten uitgevoerd, waaronder de projecten Basisvoorziening GEO, Landelijke Kernregistraties, landelijke ICT-omgeving en gemeenschappelijke applicaties, die rechtstreeks bijdragen aan het gebruik maken van standaarden voor informatie-uitwisseling. Gezien deze ontwikkeling is afdwingen via regelgeving niet noodzakelijk.	
22.	*Beter alarmeren en informeren door* a) de implementatie van alarmmiddel NL-Alert b) het verhogen van het bereik van NL-Alert. Dit door de verzending door de telecomoperators verplicht te stellen via de Telecomwet, door afspraken te maken met toestelleveranciers en door het voeren van publiekscampagnes rondom de landelijke controleberichten.	a) Op 8 november 2012 is NL-Alert ingevoerd als modern alarmmiddel voor levensbedreigende incidenten. [194] b) Via een aanwijzing zijn de telecomoperators verplicht NL-Alertberichten te verzenden. Met de toestelleveranciers zijn afspraken gemaakt dat zij nieuwe toestellen bij verkoop afleveren ingesteld voor de ontvangst van NL-Alertberichten. Halfjaarlijks wordt een landelijk controlebericht uitgezonden. In de drie weken daaraan voorafgaand wordt een landelijke publiekscampagne o.a. gericht op het bekendmaken van NL-Alert en het oproepen om toestellen voor de ontvangst van NL-Alert in te stellen. Bij het controlebericht van 7 december 2015 bleek uit een representatieve steekproef dat het NL-Alert bericht werd ontvangen door ongeveer 7,1 miljoen mensen (49% van de bevolking van 12 jaar en ouder). Verdere groei zal plaatsvinden: de meeste nieuwe toestellen die worden gekocht zijn bij koop al ingesteld om NL-Alerts te	

193 Veiligheidsberaad (2015), Programma Informatievoorziening Veiligheidsregio's 2015-2010.

194 Kamerbrief 29517 107

		ontvangen. Verder stellen steeds meer mensen hun telefoon in voor de ontvangst van NL-Alert. Bij aanvang was NL-Alert geschikt voor verzending op 2G en 3G. Eind 2015 konden de drie operators die op 4G uitzonden ook NL-Alerts uitzenden op 4G. NL-Alert wordt regelmatig ingezet, gemiddeld drie keer per maand. [195]	
23.	*Verbeteren van de risico- en crisiscommunicatie door* a) verder ontwikkelen van communicatiemiddelen: als 0800-1351 en www.crisis.nl b) de oprichting van een Nationaal Kernteam Crisiscommunicatie (NKC) c) het inzetbaar maken van een bovenregionaal expertteam crisiscommunicatie voor ondersteuning van de veiligheidsregio's.	a) Voor de verdere ontwikkeling van de betreffende communicatiemiddelen zijn er verschillende (prestatie)afspraken gemaakt, o.a. op het gebied van hosting, beheer en telefonische afhandeling in crisissituaties.[196] b) Het NKC is opgericht.[197] c) BTC is sinds februari 2014 actief.[198]	
24.	*Versterken van de operationele en bestuurlijke informatievoorziening bij rampen en crises* Door het invoeren van netcentrisch werken met een Landelijk Crisismanagement Systeem (LCMS)	LCMS is ingevoerd. Sinds de afronding van de implementatie van netcentrisch werken in 2012 hebben veiligheidsregio's en het NCC/LOCC zichzelf en het netcentrisch werken doorontwikkeld. Structuren en processen zijn versterkt, nieuwe onderwerpen zijn ontdekt en opgepakt. Hierbij valt te denken aan bijvoorbeeld netcentrische aanpak van evenementen en werken met een geografische plot. Alle regio's werken met LCMS en maken in ieder geval bij het opschalen een startbeeld aan. Iets meer dan de helft van de regio's houdt een continu	

195 Besluit aanwijzing aanbieders inzake alarmeringsdienst NL-Alert van 27 november 2015
196 O.a.: Ministerie van Veiligheid en Justitie, NCC (2011), Opdracht inzake hosting en beheer van website crisis.nl na 31 augustus 2011; Ministerie van Veiligheid en Justitie, NCC (2012), Verlengingsovereenkomst Callcenter afhandeling telefonische crisis.
197 NCTV (2012), Nota Bestuursraad inzake crisiscommunicatie.
198 https://www.ifv.nl/kennisplein/bovenregionaal-team-crisiscommunicatie

		risicobeeld bij. Er zijn nieuwe releases uitgebracht die hebben bijgedragen aan verbetering van de gebruiksvriendelijkheid.[199]	
25.	*Verbeteren van de noodcommunicatie* Door zorg te dragen voor een functionerend noodcommunicatiesysteem als geen gebruik gemaakt kan worden van de reguliere communicatiemiddelen. De NCTV stimuleert organisaties om aangesloten te zijn en brengt het belang ervan onder de aandacht, maar het is een eigen verantwoordelijkheid van de organisaties die een rol kunnen hebben in de crisisbeheersing om aangesloten te zijn op het noodcommunicatiesysteem.	NCV is sinds 1 mei 2011 operationeel en bruikbaar voor de gebruikers. De gebruikers van het Nationale Noodnet zijn herhaaldelijk schriftelijk attent gemaakt op de beschikbaarheid van de NCV en gestimuleerd om over te stappen naar deze dienst. Alle aansluitingen van het Nationaal Noodnet zijn overgezet op de NCV. Iedere gebruiker heeft een aparte aansluiting + toestel200. Bij de stroomstoring in Diemen van 27 maart 2015 bleek dat het gebruik van NCV niet bij iedere aangeslotene voldoende op het netvlies stond. Daar zijn (en worden anno 2017) maatregelen op genomen[201.]	
Behoud historisch erfgoed			
26.	*Bevorderen oprichting Nederlands Veiligheids Instituut (NVI)* Het NVI heeft een platformfunctie voor historisch erfgoed dat betrekking heeft op veiligheid en hulpverlening in Nederland. Daarnaast heeft het NVI als doel om burgers meer risicobewust en weerbaar te maken. Het gewenste effect is dat de burger daardoor medeproducent van veiligheid wordt.	Als (gedelegeerd) stelselverantwoordelijke op het gebied van crisisbeheersing heeft de NCTV in de betreffende periode subsidie verstrekt voor de oprichting van het NVI. [202]	

199 Staat van Netcentrisch werken 2015
200 Agentschap Telecom: '1-1-2 onder de loep - Een onderzoek naar de opbouw en organisatie van het alarmnummer en de storingen in 2012' (maart 2013).

201 Inspectie Veiligheid en Justitie en Agentschap Telecom: 'Stroomstoring Noord-Holland 27 maart 2015 - Lessen uit de crisisbeheersing en telecommunicatie' (juni 2016).
202 Minister van Veiligheid en Justitie (2014), Subsidie NVI 2015. Kenmerk: 692808.

Vergroten weerbaarheid van vitale belangen			
Versterken weerbaarheid ten behoeve van de nationale veiligheid			
27.	*Herijken interdepartementale strategie en beleid bescherming van vitale infrastructuur* In samenwerking met onder andere de stuurgroep nationale veiligheid wordt de strategie nationale veiligheid geëvalueerd en doorontwikkeld, onder andere door het onderwerp 'vitaal' meer integraal in de strategie op te nemen.	In de voortgangsbrief nationale veiligheid van 8 november 2013 is toegezegd om het beleid rondom de bescherming van vitale infrastructuur te herijken. Inmiddels is de beoordeling van wat vitaal is voor Nederland afgerond. Tijdens de herijking is een integrale beoordeling van de mate van vitaliteit uitgevoerd waarbij de gevolgen van uitval van vitale processen zijn gescoord op economische, fysieke en sociale impact. Hierbij zijn per sector de vitale processen benoemd. Daarbij is onderscheid gemaakt tussen twee categorieën vitaal om recht te doen aan de diversiteit binnen de vitale infrastructuur, om te kunnen prioriteren bij o.a. incidenten en om maatwerk in eventuele weerbaarheidsverhogende maatregelen mogelijk te maken. [203] Er is nog geen nieuwe strategie nationale veiligheid. Wel biedt de bestaande strategie voldoende haken om "vitaal" goed te borgen. Om de vijf vitale belangen van Nederland te beschermen is de continuïteit en integriteit van de 22 vitale diensten en processen in de vitale infrastructuur essentieel, ongeacht de natuurlijke of menselijke dreiging die daar tegen uitgaat. Om die reden wordt vanuit het perspectief van de bescherming van de vitale diensten en processen (de te beschermen belangen) gewerkt aan een integrale weerbaarheid van de vitale infrastructuur.	

203 Tweede Kamer, vergaderjaar 2014–2015, 30 821, nr. 23 p. 3; Voortgangsbrief Nationale Veiligheid, d.d. 12 mei 2015, Directie Weerbaarheidsverhoging NCTV.

28.	*In publiek- private samenwerking ontwikkelen van 'roadmaps'* De NCTV stimuleert gezamenlijke ontwikkeling van roadmaps voor de optimalisering van de weerbaarheid van als vitaal geïdentificeerde processen	Er is door de NCTV een format roadmaps ontwikkeld voor de roadmap. Dit is de basis voor de departementen met een vitaal proces. Tevens zijn er door verschillende departementen roadmaps ontwikkeld voor vitale processen.[204]	
29.	*Stroomlijnen van de overheidsinzet* Inzetten op het zoveel mogelijk samenbrengen van specifieke initiatieven en instrumenten, zoals het Alerteringssysteem Terrorismebestrijding (Atb) en het maken van crisisafspraken, zodat samenwerking met vitale organisaties tijdens incidenten, rampen en crisis wordt versterkt. Primair ligt het zorgdragen voor de continuïteit bij de vitale aanbieders, de overheid ondersteunt ze daarin en probeert in overleg met de vitale aanbieders de weerbaarheid tegen verschillende dreigingen, indien nodig, verder te vergroten. De vakdepartementen zijn degene die daarover met de vitale aanbieders in gesprek zijn en beleid voeren om te zorgen dat de vitale processen de nodige maatregelen treffen om weerbaar te zijn. Om op effectieve en efficiënte wijze te zorgen dat de weerbaarheid van de vitale aanbieders	In mei 2016 is door de NCTV de internationale tabletop oefening VITEX georganiseerd. In deze oefening hebben 22 Europese lidstaten samengewerkt aan hoe te handelen als een vitale infrastructuur uitvalt. In 2014 zijn de voorbereidingen hiervoor gestart, door aanvraag subsidie en indienen van projecten. Het beleid is vastgesteld in de voortgangsbrieven Nationale Veiligheid. De maatregelen tezamen vormen de weerbare vitale infrastructuur. De vitale processen zijn inmiddels ook geborgd in de uitwerking van aanpalend beleid en wet en (Europese) regelgeving. In de Wet Gegevensverwerking Cybersecurity (inwerking vanaf 1-1-2017) is de wet van toepassing verklaard op alle vitale aanbieders. Ook is bij de implementatie van de NIB-richtlijn de vitaliteitsbeoordeling aangepast om zo tot een eenduidige invulling te komen binnen de essentiële diensten vanuit de NIB-richtlijn en de vitale processen die in Nederland reeds vastgesteld waren. In de regeling naslag onder de WIV heeft de NCTV gezorgd dat er een basis is gelegd voor vitale aanbieders en de rijksoverheid om naslag te kunnen plegen binnen hun organisaties. Met het Deltaprogramma, en met name met het programma Vitaal en Kwetsbaar vindt een intensieve	

204 Format Raodmap, Lijst status gerealiseerde roadmaps (gerubriceerd)

	gewaarborgd is, is een interdepartementale- en intersectorale aanpak nodig. Om de samenwerking optimaal in te richten is goede coördinatie en regie nodig. De NCTV is degene die zorgt voor deze coördinatie. De vitale infrastructuur zal worden opgenomen binnen de crisisstructuren, krijgt deze bijzondere aandacht binnen de Nationale Academie voor Crisisbeheersing, wordt deze opgenomen in de Producten- en Diensten Catalogus van het Nationaal Cybersecurity Centrum en krijgt deze een plek binnen de gezamenlijke doelstelling Continuïteit van de Samenleving als onderdeel van de Strategische Agenda. Dit geldt eveneens voor het Alerteringssysteem Terrorismebestrijding (ATb), dat overigens van onverkorte toepassing blijft op de huidige daarbij aangesloten sectoren. maatregelen treffen om weerbaar te zijn. Tenslotte kan het zijn van vitaal als afbakening worden gebruikt in bepaalde trajecten. Dit gebeurt bijvoorbeeld al bij de op handen zijnde Netwerk en Informatiebeveiligingsrichtlijn (NIB-richtlijn) en de Wet Meldplicht en Gegevensverwerking Cybersecurity.[205]	afstemming plaats zodat optimaal gebruik kan worden gemaakt van elkaars producten. In de periode tot 2016 heeft de NCTV voor de herijking gewerkt met SPOCS – single point of contact. Deze NCTV medewerkers waren per proces aangewezen met als taak om als penvoeders met de verschillende departementen en vitale aanbieders bijvoorbeeld de vitalitetsbeoordelingen en roadmaps op te stellen.	

205 Tweede Kamer, vergaderjaar 2014–2015, 30 821, nr. 23 p. 5

	Ook is uit de herijking van de vitale infrastructuur gebleken dat er een behoefte is aan intersectorale informatie-uitwisseling en kennisborging o.a. over intersectorale afhankelijkheden tussen de vitale infrastructuur. Vanuit de coördinerende verantwoordelijkheid voor nationale veiligheid zal NCTV (namens de minister van VenJ) het intersectorale overleg faciliteren, waarbij nauw samengewerkt zal worden met vitale organisaties.		
30.	*Signalering van mogelijk nieuwe vitale processen* Er is een veelheid en diversiteit aan processen en objecten die vanuit verschillende invalshoeken (terrorisme, continuïteit, cyber en CBRN[206] security) aandacht krijgen ten behoeve van het verhogen van hun weerbaarheid. In dit kader is nadere definiëring van het begrip 'vitale infrastructuur' nodig, evenals het aanbrengen van focus in de inspanningen van de NCTV om de vitale infrastructuur te beschermen. Door het aanbrengen van focus kunnen instrumenten zo effectief mogelijk worden ingezet.	Door een vierjaarlijkse opmaak van de stand van zaken van de weerbaarheid van vitale processen in roadmaps en de vierjaarlijkse opmaak van een actieprogramma voor het (door)ontwikkelen van capaciteiten wordt periodiek inzichtelijk waar de focus op inspanningen om de vitale infrastructuur te beschermen nodig is. In geval van nieuw geïdentificeerde risico's kunnen de roadmaps en actieprogramma's worden geactualiseerd.[207]	

206 CBRN: chemische, biologische of radiologische/nucleaire stoffen
207 Tweede Kamer, vergaderjaar 2015–2016, 30 821, nr. 32, p. 5

31.	*Aansluiting van vitale aanbieders op de nationale crisisbesluitvorming* Aanbieders van vitale producten en diensten aan laten sluiten op de nationale crisisbesluitvorming inclusief de deelname aan opleiden, trainen en oefenen.	In het Instellingsbesluit Ministeriële Commissie Crisisbeheersing 2016 en het Nationaal Handboek Crisisbesluitvorming (NHC) is vastgelegd dat structuur en werkwijze van de nationale crisisorganisatie vanaf de initiële respons gefocust en ingericht zijn op een intensieve samenwerking en afstemming met betrokken publieke en private partners. Expliciet is vastgelegd dat vertegenwoordigers vitale sectoren vergaderingen van de ICCb én MCCb kunnen bijwonen; ditzelfde geldt voor het Interdepartementaal Afstemmingsoverleg en de ondersteunende multidisciplinaire staf. [208]) Genoemde afspraken zijn een formalisering van hetgeen in voorkomend geval al daadwerkelijk in de praktijk werd gebracht. In het OTO-aanbod wordt inmiddels steeds meer ruimte geboden voor deelname door (private) vitale partners. De Nationale Academie voor Crisisbeheersing (NAC) richtte zich in eerste instantie op de interdepartementale crisisbeheersingsorganisatie. Nu heeft de NAC haar doelgroepen uitgebreid naar ook de veiligheidsregio's, partners in de vitale infrastructuur en internationale partners. In een veilige leeromgeving kunnen deze partners worden betrokken bij de activiteiten van de NAC om te komen tot een kwalitatief betere crisisbeheersingsorganisatie. Zo organiseert zij opleidingen voor ongeveer 500 crisisprofessionals uit alle relevante publieke en private sectoren gericht op advisering, besluitvorming, communicatie en operatie binnen de nationale crisisbeheersingsorganisatie.[209]	

208 Instellingsbesluit MCCb 2016, Staatscourant 2016, 48258 en TK 2015-2016, 30 821, nr. 32 (Voortgangsbrief Nationale Veiligheid, 15 september 2016).
209 TK 2014-2015, 30821, nr. 23 (Voortgangsbrief Nationale Veiligheid, 12 mei 2015).

Versterken economische veiligheid			
32.	*Ex ante analyses van vitale sectoren* Beoordelen van het huidige overheidsinstrumentarium (de weerstand) voor het beschermen van de nationale veiligheid bij buitenlandse investeringen in als vitaal aan te merken sectoren	Aan de hand van ex-ante-analyses worden voor elke sector binnen de vitale infrastructuur eventuele risico's voor de nationale veiligheid bij buitenlandse investeringen en aanbestedingen van overheidsopdrachten in kaart gebracht teneinde te bepalen of het bestaande instrumentarium van de overheid voldoende waarborgen biedt. In de periode van de beleidsdoorlichting zijn drie analyses uitgevoerd: Waterkeren, Energie en Telecom. Ook voor andere sectoren met een vitaal proces worden ex-ante-analyses uitgevoerd: drinkwatervoorziening, chemie, nucleair, betalingsverkeer, vlucht- en vliegtuigafhandeling, scheepsvaartafwikkeling, inzet defensie en inzet politie.	
33.	*Risicoverkenning op aanbesteding en inhuur* Op basis van een risicoverkenning wordt uitvoering gegeven aan maatregelen gericht op risico's voor de nationale veiligheid die samenhangen met aanbesteding en inhuur.	In algemene zin is er bij aanbestedingen altijd sprake van een nieuwe of aanvullende afhankelijkheidsrelatie met een externe partij. Of deze afhankelijkheid een probleem vormt voor de nationale veiligheid, hangt sterk af van de sector c.q. het type product of dienst dat geleverd wordt, de opdrachtgever/afnemer en het bedrijf dat de opdracht (mogelijk) wordt gegund. In vervolg op een verkenning van de mogelijke risico's voor de nationale veiligheid bij aanbestedingen zijn meerdere voorlichtingsbijeenkomsten binnen de rijksinkoop gehouden. Verder wordt in samenwerking met inkopers, CBA, Pianoo en departementen (oa EZ, BZK O&O) gewerkt aan de ontwikkeling van instrumenten om mogelijke EV-risico's te identificeren en de rijksinkoper handelingsperspectief te bieden.	

		Daartoe wordt onder meer een handreiking ontwikkeld die opdrachtgevers en inkopers helpt bij het maken van een risico-inschatting en het treffen van beheersmaatregelen zoals het programma van eisen, de selectie van aanbieders en contractuele voorwaarden.	
34.	*Verkenning van het bredere thema economische veiligheid* Momenteel wordt gewerkt aan een verkenning meerwaarde generieke investeringstoets en een verkenning (probleemschets en handelingskader) digitale economische spionage. Ook is er een onderzoek door de Radboud Universiteit uitgevoerd naar een strategisch concept voor economische veiligheid.	In aanvulling op de sectorspecifieke benadering is een verkenning gaande naar de wenselijkheid en haalbaarheid van generieke wetgeving op het gebied van economische veiligheid. Daarbij worden ook buitenlandse ervaringen betrokken. Ook loopt er een verkenning naar de risico's van digitale economische spionage. De Radboud Universiteit heeft onlangs een onderzoek opgeleverd dat inzicht biedt hoe aandeelhouderschap in een Nederlandse vennootschap toegang kan bieden tot vertrouwelijke en invloed op beslissingen en op welke wijze dit gevolgen kan hebben voor de nationale veiligheid. Momenteel wordt ook een onderzoek naar een strategisch concept voor economische veiligheid uitgevoerd. Hierdoor is het mogelijk beter zicht te krijgen op de schaal en omvang van het vraagstuk economische veiligheid, kan het strategisch concept en de discussie daarover leiden tot directe en praktische versterking van het beleid en eventuele betere coördinatie en helpt een strategisch concept bij het formuleren van beleidsdoelen en -instrumenten op de middellange termijn.	

Verhogen weerbaarheid Rijk tegen spionage			
35.	*Zelfanalyse Spionage* Het uitvoeren van een zelfevaluatie van de Rijksoverheid naar gevoeligheid kernbelangen voor spionage en de implementatie van de aanbevelingen hieruit De departementen zijn in beginsel zelf verantwoordelijk voor het verhogen van hun weerbaarheid tegen spionage en de uitvoering van de noodzakelijke maatregelen waaronder de zelfevaluatie o.b.v. de Leidraad Te Beschemen Belangen (TBB).	Elk departement heeft met behulp van de Handleiding KWAS (2010) én de Leidraad Te Beschermen Belangen' (juni 2015) de eigen kernbelangen en kwetsbaarheden in kaart gebracht.[210] (De minister van BZK heeft vanuit zijn systeemverantwoordelijkheid voor de beveiliging binnen de Rijksdienst de implementatie van de KWAS (zelfanalyse en toetsing van de te beschermen belangen) verder opgepakt en rapporteert periodiek de stand van zaken binnen de SGO.)	
36.	*Monitoring voortgang implementatie aanbevelingen zelfanalyse* Onderzoek naar de mate waarin aanbevelingen uit de evaluatie zijn doorgevoerd.	De minister van Veiligheid en Justitie heeft de Inspectie Openbare Orde en Veiligheid in 2011 verzocht om in samenwerking met de rijksinspecties een specifiek onderzoek te verrichten naar de voortgang van weerbaarheidsverhoging tegen spionage binnen de rijksoverheid[211.] Opvolging van het onderzoek van de Inspectie is opgepakt door BZK. De ADR heeft onderzoek gedaan om inzichtelijk te maken in hoeverre bij de departementen de te beschermen belangen geïnventariseerd zijn en welke definitie van te beschermen belangen wordt gehanteerd.[212]	

210 TK, 2010-2011, 30 821, nr. 13
211 TK, Handelingen 2011-2012, nr. 88, item 2; Rapport Onderzoek KWAS, Inspectie ministerie VenJ
212 ADR Rapport,Opdracht te beschermen belangen (gerubriceerd)

Bijlage 7 : Overzicht beleidsinstrumenten cybersecurity 2011-2015

Nr	Doelstelling en instrumenten	Realisatie en werkbaarheid	Specifiek uitgevoerde evaluatie(s) doeltreffendheid en doelmatigheid instrument[213]
Versterken integrale aanpak cybersecurity door publieke en private partijen			
Duidelijke verdeling van taken, verantwoordelijkheden en bevoegdheden			
1.	*Oprichten van Cyber Security Raad* Oprichten van een Cyber Security Raad, waarin op strategisch niveau vertegenwoordigers van alle relevante partijen zitting hebben en waarin afspraken worden gemaakt over uitvoering en uitwerking van deze strategie. De Raad geeft gevraagd en ongevraagd advies aan het kabinet en heeft daarnaast als taak het toezien op de uitvoering van de Nationale Cyber Security Strategie.	Op 1 juli 2011 is de Cyber Security Raad ingesteld. Deze Raad, onder voorzitterschap van Eelco Blok (CEO KPN) en Erik Akerboom (Nationaal Coördinator Terrorismebestrijding en Veiligheid), met in totaal veertien leden uit wetenschap, bedrijfsleven en overheid, heeft als taak het kabinet te adviseren over de uitvoering en uitwerking van de Nationale Cyber Security Strategie[214].	
2.	*Oprichten en versterken Nationaal Cyber Security Centrum* Wens van het kabinet was dat publieke en private partijen, op basis van hun eigen taken en binnen de wettelijke mogelijkheden, informatie, kennis en expertise in een op te richten Nationaal Cyber Security Centrum bij elkaar brengen, zodat inzicht kan worden verkregen in ontwikkelingen, dreigingen en trends, en ondersteuning kan	In januari 2012 is het Nationaal Cyber Security Centrum (NCSC) van start gegaan als incident-respons organisatie en als platform voor samenwerking tussen publieke en private partijen op het gebied van cyber security. In het NCSC wordt kennis en expertise samengebracht van private partijen en overheidsorganisaties. Het NCSC werkt samen met de aangesloten partners aan de versterking van de digitale weerbaarheid van Nederland. Daarbij heeft iedere partij zijn eigen verantwoordelijkheid. Het NCSC heeft hierin, naast uiteraard de inbreng van eigen expertise, een	Er is een onderzoek uitgevoerd naar Cyber Readiness in 2017. Dit onderzoek maakt gebruik van de speciaal ontwikkelde CRI-methodologie. Ten tijde van het onderzoek zijn 125 landen onderzocht op basis van deze methodiek. In het rapport is opgenomen dat: "…the Netherlands is on a path to becoming cyber ready and is currently partially operational in most of the seven CRI

213 Hier worden alleen beschikbare evaluaties genoemd die uitspraken doen over de doeltreffendheid en/ of doelmatigheid van het specifieke instrument; als die er niet zijn blijft cel leeg.
214 Staatscourant, nr. 17780, 3 september 2012

	worden geboden bij incidentafhandeling en crisisbesluitvorming. Het kabinet zal het huidige GOVCERT.NL uitbreiden, versterken en inbrengen in dit Centrum. De positie van het NCSC wordt verstevigd door een versterkte structuur te bieden voor vertrouwde informatiedeling en -analyse en door in te zetten op een rol als kennisautoriteit. Het NCSC geeft vanuit deze expertrol gevraagd en ongevraagd advies aan aangesloten private en publieke partijen. Ten slotte verbreedt het NCSC zich op basis van de eigen detectiecapaciteit en de triagerol bij crises ook naar een Nationaal Cyber Security Operations Center (CSOC), naast zijn rol van Computer Emergency Respons Team (CERT).	ondersteunende rol. Naast zijn kennisfunctie treedt het NCSC ook zelf op of biedt ondersteuning bij crises of incidenten die kunnen leiden tot maatschappelijke ontwrichting [215]. De in 2014 ingezette personele versterking van het NCSC heeft in 2015 verder vorm gekregen. Het 24/7 beschikbare Nationaal Cyber Security Operations Center (NCSOC) functioneert als meldpunt, signaleert nieuwe dreigingen en voorziet haar netwerk van contacten van opvolgbare informatie[216]. Op 11 juli 2017 is de eerste kamer akkoord gegaan met de Wet gegevensverwerking en meldplicht cybersecurity (Wgmc)[217]. De Wgmc vormt een belangrijke basis voor deze publiek-private samenwerking. Zo biedt de wet een kader voor de wijze waarop het NCSC met vertrouwelijke informatie moet omgaan. Daarnaast worden nu ook de wettelijke grondslag van de taken en bevoegdheden van het NCSC vastgelegd.	essential elements"[218]. De Wgmc zal op 1 oktober 2017 in werking treden. In de wet is opgenomen dat de wet geëvalueerd moet worden na drie jaar en daarmee dus ook de taken en bevoegdheden van het NCSC zoals vastgelegd in deze wet.
Bouwen aan coalities voor vrijheid, veiligheid en vrede in het digitale domein			
3.	*Versterkt participeren in multistakeholder evenementen* Of het nu gaat om standaarden in ICT, fundamentele rechten, de bestrijding van cybercrime of het bevorderen van de internationale rechtsorde in cyberspace, een internationale beleidsagenda is belangrijk onderdeel van een geïntegreerd nationaal cybersecuritybeleid.	Het internationale karakter van cybersecurity kwam nadrukkelijk naar voren bij de GCCS 2015 waarvan Nederland gastheer was. Deze internationale top met vertegenwoordigers op ministerieel niveau, van internationale organisaties en leiders uit de private sector benadrukte het belang van internationale samenwerking tussen alle stakeholders en kennisuitwisseling in het digitale domein.	

215 Brief NCTV, kenmerk: 275614, Voortgang Nationale Cyber Security Strategie, 6 juli 2012.
216 Kamerbrief, vergaderjaar 2015–2016, 26 643, nr. 369, 14 oktober 2015.
217 Staatsblad van het Koninkrijk der Nederlanden, nr 2017 316, 3 augustus 2017.
218 Potomac Institute for Policy Studies, The Netherlands Cyber readiness at a glance, Cyber Readiness Index 2.0, all rights reserved

	De internationale visie van de Nationale Cyber Security Strategie 2 gaat uit van een geïntegreerde aanpak van veiligheid, waarin naast het belang van defence en development, in de vorm van capaciteitsopbouw, ook middels diplomacy wordt bijgedragen aan meer stabiliteit in het cyberdomein. De NCTV neemt deel aan verschillende internationale werkgroepen en organiseert GFCE (samen met BZK).	Nederland zet in op het duurzaam stimuleren van cybercapaciteitsopbouw in internationaal verband, zowel in minder cyber-ontwikkelde landen als in landen waar het cyberdomein relatief ver ontwikkeld is. Het gaat daarbij om het delen van kennis en expertise op een aantal centrale cyberthema's tussen internationale publieke en private partners. Het belangrijkste instrument daarvoor is het, tijdens de GCCS gelanceerde, mondiale Global Forum on Cyber Expertise (GFCE). Het GFCE is een concreet initiatief van landen, bedrijven en intergouvernementele organisaties om door middel van capaciteitsopbouw brede inspanning te doen op het gebied van cybersecurity[219]. Meeste initiatieven zijn gestart aan het einde of na de periode van de evaluatie.	
Nederland zorgt voor adequate en actuele dreiging- en risicoanalyses			
Gezamenlijk integraal beeld van de actuele dreigingen en kwetsbaarheden ICT			
4.	*Risico's in kaart brengen van legacy systemen in vitale processen en diensten* Legacy systemen zijn systemen die zijn gebouwd met technologie die niet of nauwelijks meer wordt ondersteund door externe leveranciers en/of de eigen organisatie. Qua beschikbaarheid, integriteit en vertrouwelijkheid zijn legacysystemen in vergelijking met modernere systemen kwetsbaarder en daarmee onveiliger. Als het	De minister van VenJ heeft in mei 2015 middels een brief de kamer geïnformeerd over de uitkomsten van een herijking van de vitale infrastructuur. De herijking heeft geleid tot een actueel en eenduidig zicht op wat vitaal is voor onze samenleving, waarbij de impact op de samenleving centraal staat: één integrale lijst vitale infrastructuur[220]. In 2015 heeft het NCSC een methodiek ontwikkeld om de risico's voor legacysystemen binnen de vitale infrastructuur in kaart te brengen[221]. Deze is eind november 2015 gepubliceerd.	

219 Kamerbrief, vergaderjaar 2015–2016, 26 643, nr. 369, 14 oktober 2015
220 Kamerbrief, vergaderjaar 2014–2015, 30 821, nr. 23, 12 mei 2015.
221 Publicatie NCSC, Zicht op risico's van legacysystemen: Een self-assessmentmethode om de risico's van (vitale) legacysystemen in kaart te brengen, 1 november 2015.

	gaat om systemen bij organisaties in vitale sectoren kan deze kwetsbaarheid grote gevolgen hebben, zowel voor de eigen organisatie als voor de maatschappij. Het is dan ook van belang dat organisaties zich bewust zijn van deze relatieve onveiligheid en dat deze organisaties weten bij welke systemen dergelijke onveiligheden zich voordoen en om welke specifieke onveiligheden het gaat. Maar ook dat zij beschikken over strategieën voor het wegnemen of verkleinen van de risico's. Om organisaties hierbij te helpen is ingezet op de ontwikkeling van een self-assessment.		
5.	*Coördineren, faciliteren, samenvoegen en delen dreigings- en risicoanalyses* Naast het in kaart brengen van risico's is het vergaren van inzichten binnen het cyberdomein vanuit andere partijen een belangrijke taak. Daarom heeft de NCSC ook een coördinerende en faciliterende rol om informatie te verkrijgen voor een integraal dreigingsbeeld. De AIVD en de MIVD brengen kennis in ten behoeve van dit beeld, maar ook private partijen doen dat. Het integraal beeld vindt zijn weerslag in het Cybersecuritybeeld Beeld Nederland en geeft input voor vervolgactie van verschillende partijen, ieder vanuit zijn eigen verantwoordelijkheid.	Het Cybersecuritybeeld Nederland (CSBN) is een jaarlijkse publicatie en bevat inzicht in ontwikkelingen, belangen, dreigingen en weerbaarheid op het gebied van cybersecurity. Het CSBN komt tot stand in samenwerking met publieke en private partijen, en bevat een feitelijke beschrijving op basis van inzicht en expertise vanuit overheidsdiensten, vitale sectoren en wetenschap. Sinds 2011 is jaarlijks het CSBN uitgebracht[222].	

222 Website www.ncsc.nl.

Versterken van onderzoeks- en analysecapaciteit			
6.	*NCSC uitbreiden met meer analisten en inventariseren van samenwerkingsmogelijkheden.* Om de onderzoeks- en analysecapaciteit te verwerken, heeft NCSC ingezet op de inzet van meer analisten. Ook wil NCSC samenwerkingsmogelijkheden met inlichtingendiensten inventariseren.	In de voortgangsrapportages is opgenomen dat de NCSC is versterkt. Uit een addendum op het O&F van 2013 blijkt dat de analysecapaciteit met 6 fte is toegenomen[223]. Ook is verkend hoe de samenwerking tussen de inlichtingendiensten kan worden versterkt op het gebied van informatiedeling over digitale aanvallen en gezamenlijke analyses, binnen de geldende juridische kaders[224].	
7.	*Oprichten nationaal detectie- en responsnetwerk voor de Rijksoverheid en overige vitale sectoren*. Een trainingsprogramma wordt opgericht voor respons op grootschalige ICT-incidenten. In samenwerking met haar partners richt het NCSC een nationaal detectie- en responsnetwerk in voor de Rijksoverheid en overige vitale sectoren. Met deze netwerken wordt, omkleed met waarborgen op het gebied van onder meer vertrouwelijkheid en privacy, toegewerkt naar het real-time analyseren en delen van dreigingsinformatie.	In 2014 is een basisnetwerk ontwikkeld en gerealiseerd. Het Nationaal Detectie Netwerk (NDN) bevond zich in de periode van de doorlichting in de pilotfase. De werking van het NDN is aanvullend op de eigen detectie-inspanningen van de organisaties. Het NDN sluit aan op het eveneens publiek-private Nationaal Respons Netwerk (NRN) dat, onder de coördinatie van het NCSC, de gezamenlijke respons op cybersecurity-incidenten versterkt. Het NRN is op 17 april 2014 met vijf organisaties gelanceerd en is daarna verder uitgebouwd[225].	Het NDN wordt gezien als een belangrijk instrument om cyberaanvallen te onderkennen, beheersbaar te maken en informatie te delen met private partijen. Zo is in de begroting van 2017 opgenomen dat het kabinet, in het licht van de toenemende dreiging, het Nationaal Detectie Netwerk (NDN) verder zal versterken en uitbouwen[226].

223 Addendum op O&F Nationaal Coördinator Terrorismebestrijding en Veiligheid betreffende de Directie Cyber Security, 27 januari 2013.
224 Kamerbrief, vergaderjaar 2015–2016, 26 643, nr. 369, 14 oktober 2015.
225 Kamerbrief, vergaderjaar 2014-2015, 26 643, nr. 341, 18 december 2014.
226 Kamerbrief, vergaderjaar 2016-2017, 34 550 VI, nr. 2, 20 september 2016.

Versterken van de weerbaarheid tegen ICT-verstoringen en Cyberaanvallen			
Vergroten en ontwikkelen cybersecurity experts			
8.	*Ontwikkelplan gericht op kwalificering en certificering* Voor de beroepsgroepen en het onderwijsveld wordt een plan ontwikkeld voor het uitbreiden van het aandeel van ICT-veiligheid in de daarvoor geschikte opleidingen. Ook wordt voortgebouwd op een onderzoek naar de mogelijkheden van certificering en kwalificering van informatiebeveiliging professionals.	Via overheidsinterne opleidingstrajecten, zoals binnen het NCSC reeds wordt toegepast (samenwerking TNO en HEC) wordt getracht cyber specialisten te trainen en te werven. Daarnaast kunnen samenwerkingsverbanden met private partijen worden opgezet om cyber specialisten uit te wisselen[227]. In een beleidsreactie is opgenomen dat in 2015 een stevige impuls is gegeven aan de acties op het gebied van onderwijs uit de NCSS 2. Gelet op het belang van een veilige digitale omgeving wordt de noodzaak van voldoende cybersecurityspecialisten breed onderschreven. Zo maakt de beroepsgroep cybersecurityspecialisten onderdeel uit van de Human Capital Agenda die door het ministerie van Economische Zaken wordt ontwikkeld. Cybersecurityspecialisten is een van de doelgroepen waar de acties uit de HCA ICT-innovatie zich op richten[228].	
9.	*Oprichten PPS taskforce Cybersecurity* In de tweede Cybersecurity strategie is als actie opgenomen om een PPS taskforce Cybersecurity in te stellen, die zich richt op advisering van het cybersecurity onderwijsaanbod.	Gedurende de periode van de evaluatie was nog geen taskforce ingesteld. Sinds april 2016 is het dutch cybersecurity platform for higher education and research (dcypher) opgericht door de Ministeries van Veiligheid en Justitie, Onderwijs, Cultuur en Wetenschap en Economische Zaken en de Nederlandse Organisatie voor Wetenschappelijk Onderzoek[229]. Dcypher verenigt onderzoekers, docenten, producenten, gebruikers en beleidsmakers in Nederland om kennis en kunde over cyberveiligheid te verbeteren. De missie van dcypher is als volgt:	

227 Brief NCTV, kenmerk: 275614 , onderwerp: Voortgang Nationale Cyber Security Strategie, 6 juli 2012.
228 Staatscourant, nr. 28095, 1 oktober 2014.
229 Website www.nwo.nl; & Brief NCTV, kenmerk: 793052, onderwerp: Beleidsreactie Cyber Security Beeld Nederland 2016, 5 september 2016.

		dcypher zorgt voor (bottom-up) agendering en coördinatie van (wetenschappelijk en praktijk gericht) cybersecurity onderzoek en - hoger onderwijs. Dat wil zeggen dat onderzoeks- en onderwijsagenda's tot stand komen na brede raadpleging van het veld (kennis-en onderwijsinstellingen, ondernemingen, overheden)[230].Dcypher is ondergebracht bij NWO. De NCTV levert een bijdrage aan dcypher middels subsidie[231].	
Stimuleren onderzoek Cybersecurity			
10.	*Afstemmen onderzoeksprogramma's via de research cyber security agenda* Het kabinet zal onderzoeksprogramma's van in ieder geval de overheid en waar mogelijk van wetenschappelijke onderzoekscentra en het bedrijfsleven beter op elkaar afstemmen in de Nationale Cyber Security Raad. Hieruit volgt de research cyber security agenda.	Tijdens haar eerste vergadering heeft de Cyber Security Raad de Nationale Cyber Security Research Agenda (NCSRA) vastgesteld. Deze onderzoeksagenda sluit aan op de NCSS door invulling te geven aan actielijn 6 van de strategie, het stimuleren van onderzoek en onderwijs en prioriteit 5 van de CSR. De onderzoeksagenda stelt vijf hoofddoelen centraal: 1. Verbeteren van veiligheid van en vertrouwen in ICT-infrastructuur en diensten; 2. Nederland voorbereiden op veiligheidsuitdagingen in de komende 6 tot 12 jaar; 3. Stimuleren van de Nederlandse cyber security economie; 4. Versterken en verbreden van kennis en innovatie tav cyber security; 5. Onderzoekprogramma's cyber security bij de overheid verbinden[232].	
11.	*Ondersteunen bij aanboren onderzoeksgelden* De overheid gaat de genoemde partijen nog actiever dan nu begeleiden bij het aanboren van multiplicerende onderzoeksgelden bij bijvoorbeeld	Agentschap NL/RvO en NWO hebben, binnen de kaders van de in 2012 gelanceerde Nationale Cyber Security Research Agenda II (NCSRA II), een tweede tender voor de NCSRA in juni 2014 uitgeschreven ter waarde van ongeveer € 5,5 miljoen, ongeveer	

230 Website www.dcypher.nl/nl/content/over-ons.
231 Brief NCTV, kenmerk: 2022653, Onderwerp: Verlening subsidie dcypher, 7 december 2016.
232 Brief NCTV, kenmerk: 275614 , onderwerp: Voortgang Nationale Cyber Security Strategie, 6 juli 2012.

	Europese en Euregionale fondsen. De NCTV levert een bijdrage vanuit een coördinerende taak om te faciliteren bij het verkrijgen van financiële middelen voor onderzoeken. Een andere bijdrage is dat de NCTV betrokken is bij de inhoudelijke beoordeling van onderzoeksvoorstellen als lid van de beoordelingscommissie.	gelijk verdeeld over een SBIR programma voor korte termijn R&D en lange termijn onderzoek[233].	
12.	*Lanceren van cybersecurity platform* Lanceren van cybersecurity platform voor nieuwe en gevestigde bedrijven, studenten en onderzoekers.	Zie ook instrument 10. Na de periode van deze doorlichting is het platform dcypher van start gegaan. Dcypher vormt ook de opvolger van het voormalige ICT Innovatieplatform Veilig Verbonden (IIP-VV), dat zich vooral richtte op de agendering van het onderzoek naar security en privacy[234].	
Vergroten kennis over en veiligheidsbewustzijn van ICT-producten en diensten bij de gebruikers (burgers en bedrijven)			
13.	*Beter beschikbaar maken van informatie* over veiligheid van ICT-producten en -diensten bij de gebruiker. Vanuit het NCSC wordt actief bijgedragen aan de bewustwording van publiek, overheid en het bedrijfsleven via publicaties, de website en het delen van concrete expertise met belanghebbende partijen. *Publicatie kennisdocumenten en beveiligingsadviezen* Het NCSC publiceert kennisdocumenten die informatie en inzicht bieden over cyber aanval-	*Publicatie kennisdocumenten en beveiligingsadviezen* 'ICT- beveiligingsrichtlijnen voor webapplicaties' en factsheets rond de beveiliging van SCADA- systemen zijn uitgebracht. Daarnaast wordt de website van het NCSC dagelijks aangevuld met technische beveiligingsadviezen voor ICT professionals[235]. De beveiligingsadviezen van de NCTV zijn erop gericht om informatie over kwetsbaarheden onder de aandacht te brengen van aangesloten organisaties[236]. In het onderzoek van de Inspectie VenJ naar het gebruik van beveiligingsadviezen komt naar voren dat betrokken partijen de kennis en expertise van het NCSC waarderen. Dit betreft niet alleen de beveiligingsadviezen, maar ook de andere producten die het NCSC levert (bijvoorbeeld	De inspectie van VenJ heeft onderzocht wat aangesloten organisaties doen met de beveiligingsadviezen van het NSCS en wat de meerwaarde ervan is voor de ontvangende partijen. De inspectie concludeert dat de beveiligingsadviezen in huidige vorm beperkte meerwaarde hebben. Het advies is het product beveiligingsadviezen te heroverwegen[240]. In opdracht van de NCTV worden in het kader van Alert online jaarlijks

233 Kamerbrief, vergaderjaar 2014-2015 , 26 643, nr. 341, 18 december 2014.
234 Brief NCTV, kenmerk: 793052, onderwerp: Beleidsreactie Cyber Security Beeld Nederland 2016, 5 september 2016.
235 Brief NCTV, kenmerk: 275614 , onderwerp: Voortgang Nationale Cyber Security Strategie, 6 juli 2012.
236 Rapport Inspectie Veiligheid en Justitie, Gebruik van beveiligingsadviezen van het Nationaal Cyber Security Centrum, mei 2015.
240 Rapport Inspectie Veiligheid en Justitie, Gebruik van beveiligingsadviezen van het Nationaal Cyber Security Centrum, mei 2015.

	technieken, preventie, kwetsbaarheden en dreigingen en daarnaast ook specifieke tools voor het bieden van concrete handelingsperspectieven. *Alert Online* Internet wordt tegenwoordig de hele dag door gebruikt. Uit onderzoek blijkt dat mensen zich vaak onvoldoende bewust zijn van de risico's van het gebruiken van internet. Daarom is in 2012 Alert Online geïntroduceerd. Alert Online is een jaarlijkse campagne om mensen en organisaties bewust te maken van hun internet- en mobiel gebruik en de risico's die dit met zich meebrengt. *Veiliginternetten.nl* Onderzoek, in het kader van de cybersecurity awareness campagne Alert Online 2014, laat zien dat internetgebruikers behoefte hebben aan informatie van internetproviders, consumentenorganisaties of de overheid over veilig gebruik van internet. De website van Veilig Internetten (www.veiliginternetten.nl) is het actuele kanaal met informatie over veilig internetten voor burgers en het MKB. Het NCSC heeft in samenwerking met het ministerie van Economische Zaken en ECP, het Platform voor Informatiesamenleving, veiliginternetten.nl gelanceerd.	factsheets, white papers en sectorale overlegvormen)[240]. *Alert Online* Alert Online is in 2012 gestart op initiatief van de NCTV. Sinds 2013 staat er elk jaar een thema centraal, namelijk: "Smart security" (2013), "Kennis" (2014), "Digitaal verantwoord ondernemen" (2015)[237]. *Veiliginternetten.nl* De website www.veiliginternetten.nl is gelanceerd tijdens de Alert Online campagne in 2014[238]. Dit is een website waar mensen tips, tricks en praktische stap voor stap uitleg kunnen vinden over wat zij kunnen doen en laten om veilig te internetten. Ze vinden er tips hoe ze veilig omgaan met hun online privacy, hoe ze veilig gebruik maken van wifi, wat ze kunt doen en laten op sociale media, en ze vinden er uitleg over hoe zij kinderen helpen veilig online te zijn. Deze site is bedoeld voor iedereen met vragen over veilig gebruik van internet[239].	bewustzijnsonderzoeken uitgevoerd.. Deze onderzoeken geven meer input voor beleid. Het hoofddoel van het onderzoek in 2015 was bv: het verkrijgen van inzicht in hoe veilig of onveilig men zich online gedraagt (op basis van zelfgerapporteerd gedrag). In de jaren ervoor lag de nadruk in het onderzoek meer op cyber awareness (kennis en houding)[241]. Verder is in een beleidsreactie van 2016 aangegeven dat website veiliginternetten.nl inmiddels 100.000 maal is bezocht en daarmee heeft bijgedragen aan bewustwording en heeft geleid tot aanpassingen bij diverse marktpartijen en overheden[242].

237 Website, www.alertonline.nl.
238 Brief NCTV, Kenmerk 596960, onderwerp: Voortgangsbrief realisatie werkprogramma Nationale Cyber Security Strategie 2, 18 december 2014
239 Website, www.veiliginternetten.nl.
241 Rapport GfK BV, Cybersecurity 2015 Awareness, gedrag & digitaal verantwoord ondernemen, 25 september 2015.
242 Brief NCTV, kenmerk: 793052, onderwerp: Beleidsreactie Cyber Security Beeld Nederland 2016, 5 september 2016.

Bewerkstelligen dat publieke en private leveranciers voldoen aan minimumeisen op het gebied van continuïteitsdienstverlening en spionage			
14.	*Stimuleren minimale ICT beveiligingsstandaarden op basis van good practices* De overheid gaat samen met de vitale organisaties het gebruik van de gangbare minimale ICT beveiligingsstandaarden op basis van good practices stimuleren.	Voorts is in 2014 een publiek privaat platform internetstandaarden ingericht om de toepassing van moderne internetstandaarden te stimuleren. De website www.internet.nl, gelanceerd tijdens de GCCS 2015, checkt op de compliance met internetstandaarden zoals IPv6, DNSSEC en veiligheidsstandaarden van websites[243].	
15.	*Beschikbaar stellen handleiding Kwetsbaarhedenanalyse Spionage* Specifiek ter voorkoming van (digitale) spionage heeft het kabinet een maatregelenpakket ontwikkeld. Voor bedrijven is er een handleiding Kwetsbaarhedenanalyse Spionage beschikbaar waarmee zij hun weerbaarheid tegen spionage kunnen vergroten.	Zie matrix crisis beheersing bijlage II.	N.v.t.
16.	*Inzetten voor internationale afspraken over veilige hard- en software en zorgen dat Nederland actief deelneemt in het Internet Governance Forum* Het kabinet wil in overleg met de ICT-leveranciers zoeken naar mogelijkheden om de veiligheid van hard- en software te verbeteren en zet zich ervoor in om ook op internationaal niveau afspraken te maken over veilige hard- en software. Daarnaast neemt Nederland actief deel in het Internet Governance Forum dat door de Verenigde Naties wordt gefaciliteerd. Doel hiervan is om een actieve rol te spelen om in de mondiale context van een open en transparante dialoog onderwerpen aan te snijden die kunnen bijdragen	Zie toelichting onder instrument drie waar ook verschillende internationale activiteiten zijn benoemd.	

243 Brief NCTV, kenmerk: 793052, onderwerp: Beleidsreactie Cyber Security Beeld Nederland 2016, 5 september 2016.

	aan deze strategie, zoals de spelregels op het internet te verbeteren en misbruik tegen te gaan.		
17.	*Haalbaarheidsonderzoek gescheiden netwerk vitaal* Er wordt een verkenning uitgevoerd in hoeverre het realiseren van een gescheiden ICT-netwerk voor (publieke en private) vitale processen op technisch en organisatorisch vlak mogelijk en wenselijk is. Met een gescheiden netwerk nemen de mogelijkheden om de continuïteit van vitale processen te borgen toe. Ook kunnen binnen het gescheiden netwerk eigen dataopslag of een cloud worden ontwikkeld. Hierdoor kan de privacy/integriteit van de data in deze opslag of cloud worden verbeterd.	De verkenning is uitgevoerd in 2014. De hoofdvraag van de verkenning was: zijn gescheiden ICT-netwerken in Nederland haalbaar en wenselijk?[244] Het rapport geeft inzicht in het feit dat een volledig gescheiden netwerk op zichzelf geen realistische optie is. Dit geldt eveneens voor het gesloten maken van delen van het internet[245].	
Versterken responscapaciteit om ICT-verstoringen en cyberaanvallen te pareren			
Zorgen voor duidelijke crisisstructuur bij cyberincidenten			
18.	*Opstellen Nationaal Crisisplan ICT* De NCTV levert in 2011 het Nationaal Crisisplan ICT op (NCP-ICT). Onderdeel hiervan is een oefenplan, dat zowel nationale als internationale oefeningen op elkaar afstemt.	Eind 2011 is het NCP-ICT opgeleverd. Het crisisplan beoogt steun te bieden aan de crisisbeleidsadviseurs in de voorbereiding op en tijdens de situatie waarbij een maatschappelijke ontwrichting dreigt of plaatsvindt als gevolg van een ICT-verstoring of –uitval. Het crisisplan draagt bij aan een verkorting van de reactietijd van de nationale crisisorganisatie en aan een effectieve crisisbestrijding[246]. Het crisisplan is in 2012 geactualiseerd[247].	De Inspectie VenJ concludeert in haar evaluatie dat de rijkscrisisorganisatie tijdens de DigiNotar-crisis doeltreffend heeft gefunctioneerd. De rijkscrisisstructuur is tijdens de DigiNotar-crisis grotendeels ingericht zoals beschreven in de planvorming. Daarnaast is deze generieke structuur

244 Rapport PWC, Verkenning naar gescheiden ICT-netwerken en –diensten in Nederland, september 2014.
245 Kamerbrief, vergaderjaar 2014–2015, 26 643, nr. 337, 24 november 2014.
246 Brief NCTV, kenmerk: 275614 , onderwerp: Voortgang Nationale Cyber Security Strategie, 6 juli 2012.
247 Nationaal Crisisplan ICT, versie 2.0, 7 september 2012.

			uitgebreid met een crisisspecifieke structuur zoals beschreven in het NCP-ICT. Dit betreft de organisatieonderdelen de IRB, de CSR en de ICCIO. Dit plan is ten tijde van deze crisis nog niet vastgesteld[248]. Een directie relatie tussen het NCP-ICT en het effect ervan op het doeltreffend functioneren van de crisisorganisatie tijdens de DigiNotar-crisis is niet expliciet gesteld in de evaluatie. Wel worden ook andere factoren genoemd die hebben bijgedragen aan het doeltreffend functioneren van de rijkscrisisorganisatie, zoals de korte lijnen, de goede samenwerking en het doortastende optreden van de belangrijkste sleutelfunctionarissen. Tevens is het aannemelijk dat het NCP-ICT heeft bijgedragen aan een doeltreffende adressering van een crisis.
19.	*ICT Response Board onderbrengen bij NCSC* De ICT Response Board (IRB), een publiek-private samenwerking die de crisisbesluitvormings-organisaties advies geeft over maatregelen om grootschalige ICT-verstoring tegen te gaan of te bestrijden, wordt in 2011 geoperationaliseerd en als functie ondergebracht in het Nationaal Cyber Security Centrum.	In een voortgangsbrief van 2012 is opgenomen dat de IRB als functie is ondergebracht bij het NCSC. De IRB is tevens ingebed in het Nationaal Crisisplan ICT van de Rijksoverheid[249].	
20.	*Versterken internationale samenwerking CERT-organisaties* Internationaal zet NCSC in op de versterking van	Nederland heeft een vooruitstrevende rol gespeeld in het verder vormgeven en implementeren van vertrouwenwekkende maatregelen, bijvoorbeeld in de OVSE. Deze kunnen een bijdrage	De European Union Agency for Network and Information Security (ENISA) heeft een publicatie uitgebracht waarin het belang van

248 Inspectie VenJ, Evaluatie van de rijkscrisisorganisatie tijdens de DigiNotar-crisis, 2011.
249 Brief NCTV, kenmerk: 275614 , onderwerp: Voortgang Nationale Cyber Security Strategie, 6 juli 2012.

	de samenwerking bij de operationele respons tussen de CERT-organisaties in Europa en wordt gestreefd naar versterking van het International Watch and Warning Network (IWWN), dat nu als informeel mondiaal operationeel overleg fungeert bij ICT-incidenten.	leveren aan het vergroten van de internationale stabiliteit en aan het voorkomen van escalatie van cyberconflicten. Hierbij kan gedacht worden aan het opstellen van consultatiemechanismen en contactpunten, het voeren van formele en informele dialogen, het versterken van de contacten tussen Computer Emergency Respons Team's (CERT's) en het delen van nationale cyberstrategieën, doctrines en informatie over de aanpak van cyberincidenten[250].	de internationale samenwerking tussen CERT-organisaties is benoemd. "(…) in order to effectively and efficientlyrespond to threats and attacks against information infrastructure a coordinated approach at European level is needed. One way to facilitate that goal is to support the Member States in enhancing cooperation among national / governmental CERTs, with regards to information sharing and coordinated incident response"[251].
21.	*Inventariseren accreditatie bedrijven als digitale brandweer.* Het gaat daarbij om cybersecuritydienstverleners die andere partijen kunnen bijstaan bij digitale incidenten. Dit naast de eigen verantwoordelijkheid van partijen en de rol die het NCSC heeft als CERT voor de Rijksoverheid en de vitale infrastructuur.	In 2015 is een verkenning afgerond naar diverse internationale accreditatiesystemen voor bedrijven die als 'digitale brandweer' kunnen optreden. In het rapport "verkenning accreditatiesysteem voor trusted hulpverleners" wordt aanbevolen om op basis van de thans gestarte discussie over standaardisering van cybersecurity in Europa, in de diverse Europese gremia actief te pleiten voor de opzet van een certificeringssysteem voor cybersecuritydienstverleners dat breed in Europa van toepassing is. In de tussentijd wordt voor Nederland het systeem van trusted Introducer aanbevolen om tot een voorlopig overzicht te komen van vertrouwde cybersecuritydienstverleners voor de Nederlandse cybersecuritymarkt[252].	Een evaluatie is niet van toepassing, omdat dit een verkenning betreft waarna mogelijk wordt overgegaan tot implementatie van een instrument.
Informeren van de burger en bedrijven bij cyberincidenten			
22.	De maatschappelijke impact van een grootschalige terroristische aanval op of via het internet kan groot zijn. De NCTV heeft daarom ingezet op uitbreiding van het Alerteringsysteem	Ten behoeve van de inbedding van cyber security in het ATb is in 2012 een pilot van start gegaan voor de ATb-sector Financieel. De uitkomsten van deze pilot dienden als input voor de aansluiting van de overige ATb-sectoren[253]. In een beleidsreactie van 2016 is	

250 Kamerbrief, vergaderjaar 2015–2016, 26 643, nr. 369, 14 oktober 2015.
251 ENISA, National/governmental CERTs: ENISA's recommendations on baseline capabilities, december 2014
252 Brief NCTV, kenmerk: 793052, onderwerp: Beleidsreactie Cyber Security Beeld Nederland 2016, 5 september 2016.
253 Brief NCTV, kenmerk: 275614 , onderwerp: Voortgang Nationale Cyber Security Strategie, 6 juli 2012.

	Terrorismebestrijding (ATb) met cyber component en beoefend deze uitbreiding.	aangegeven dat Cybersecurity is geïntegreerd in de systematiek van het ATb[254].	
23.	Veiliginternetten.nl bevat algemene informatie over veilig internetten en ook waarschuwingen voor computervirussen, wormen en beveiligingslekken in software.	Zoals eerder aangegeven in deze tabel is de website www.veiliginternetten.nl in 2014 gelanceerd. Via nieuwsberichten op de website worden burgers en bedrijven geïnformeerd over cyberincidenten[255].	
Stimuleren kennis(deling) en oefening			
24.	Door kennisdeling en oefenen van cyberscenario's is Nederland beter in staat te reageren op cyberincidenten. De NCSC levert een bijdrage aan een trainingsprogramma voor respons op grootschalige ICT-incidenten ingericht. De NCSC wil ook grote en kleine oefeningen organiseren en aan deelnemen.	De Nationale Academie voor Crisisbeheersing cybersecurity in de basis- en verdiepingstraining opgenomen, waarbinnen een trainingsprogramma voor respons op grootschalige ICT-incidenten is opgenomen. Met en binnen vitale sectoren vinden regelmatig oefeningen plaats, zowel voor afzonderlijke als samenwerkende bedrijven. Van 22 tot 25 juni 2015 heeft een publiek-private operationele ICT-crisisoefening Isidoor op nationaal niveau plaatsgevonden. De deelnemers hebben in drie dagen de gelegenheid gehad met elkaar te werken aan het oplossen van het aan hen voorgelegde scenario[256].	In het rapport van de Inspectie VenJ over de DigiNotar-crisis wordt het belang van oefenen benadrukt. Een advies is: Blijf investeren in een vaste kernbezetting van de rijkscrisisorganisatie, met deelnemers die door opleiding en oefening over de juiste crisiscompetenties beschikken[257].

254 Brief NCTV, kenmerk: 793052, onderwerp: Beleidsreactie Cyber Security Beeld Nederland 2016, 5 september 2016.
255 Website. www.veiliginternetten.nl
256 Brief NCTV, kenmerk: 793052, onderwerp: Beleidsreactie Cyber Security Beeld Nederland 2016, 5 september 2016.
257 Inspectie VenJ, Evaluatie van de rijkscrisisorganisatie tijdens de DigiNotar-crisis, 2011.

Afkortingen

ADR	Auditdienst Rijk
Atb	Alerteringssysteem Terrorismebestrijding
BDUR	Brede Doel Uitkering Regio
BPV	Besluit Personeel Veiligheidsregio's
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CBRN	Chemische, biologische, radiologische, nuceaire incidenten
COA	Centraal Opvangorgaan Asielzoekers
CSBN	Cyber Security Beeld Nederland
CT	Contra Terrorisme
DJI	Dienst Justitiële Inrichtingen
DGSenB	Directeur Generaal Straffen en Beschermen
DTN	Dreigingbeeld Terrorisme Nederland
GHOR	Geneeskundige hulpverleningsorganisatie in de regio
GOVCERT.NL	Computer Emergency Response Team (CERT) NL
GRIP	Gecoördineerde regionale incidentenbestrijdingsprocedure
GCTF	Global Counter Terrorism Forum
IFV	Instituut Fysieke Veiligheid
IND	Immigratie en Naturalisatie Dienst
IVenJ	Inspectie van het Ministerie van Veiligheid en Justitie
JBZ-raad	Raadsformatie Justitie en Binnenlandse Zaken
JenV	Ministerie van Justitie en Veiligheid
LCMS	Landelijk Crisis Management Systeem
LOCC	Landelijk Operationeel Coördinatiecentrum
KNMR	Koninklijke Nederlandse Redding Maatschappij
MCCB	Ministeriele Commissie Crisis Beheersing
NAC	Nationale Academie voor Crisisbeheersing
NCC	Nationaal Crisis Centrum
NCSC	Nationaal Cyber Security Centrum
NCSS	Nationale Cyber Security Strategie
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NKC	Nationaal Kernteam Crisiscommunicatie
NP	Nationale Politie
NRB	Nationale Risico Beoordeling
NVI	Nationaal Veiligheidsinstituut
OM	Openbaar Ministerie
OTOTEL	Opleiden, trainen, oefenen, testen, evalueren en leren
PPS	Publiek Private Samenwerking
RPE	Regeling Periodiek Evaluatieonderzoek
SMART	Specifiek Meetbaar Acceptabel Realistisch en Tijdgebonden
TA	Terroristen Afdeling
TRIP	Travel Information Portal
VenJ	Ministerie van Veiligheid en Justitie
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum

Geraadpleegde bronnen

- Actieprogramma integrale aanpak Jihadisme, 29 augustus 2014
- ADR, Rapport evaluatieonderzoek Bewaken en Beveiligen Nationale Evenementen, 24 oktober 2013
- Aland, Matthijsse, Meijer, Post, Eindrapportage Van project Water en Evacuatie naar een resultaat voor 'Watercrises en ernstige wateroverlast', 1 juni 2017
- Algemene Rekenkamer, Zicht overheden op beschermen burgers en bedrijven, 11 november 2014
- Analisten netwerk Nationale Veiligheid, Nationaal Veiligheidsprofiel 2016 - Een All Hazard overzicht van potentiële rampen en dreigingen die onze samenleving kunnen ontwrichten, november 2016
- Andersson Elffers Felix, Evaluatie Wet Veiligheidsregio's, 3 juli 2013
- Bakker, E. en De Roy van Zuijdewijn, J., Barometer van de dreiging, Tien jaar Dreigingsbeeld Terrorisme Nederland 2005-2015
- Berenschot, Herijking Rollenhuis Crisisbeheersing Rijksoverheid, 3 september 2013
- Boon Registeraccountants b.v., Jaarverslag 2016 Stichting Nationaal Veiligheidsinstituut, 28 juni 2017
- Brandweer Nederland, rapport Rembrand – brandveiligheid is een coproductie, mei 2015
- Bureau Secretaris Generaal, PPAC, ministerie van VenJ, Evaluatie NCTV organisatie 2012, eindrapport, 15 september 2016
- BZK, Factsheet Strategie Nationale Veiligheid 2013
- BZK, directie Nationale Veiligheid, Programmacontract 2011, Nationale Veiligheid Veiligheidsregio's, 4 november 2011
- BZK, Werkwijze Nationale Veiligheid, 2010
- Comptabiliteitswet 2001, artikel 20, tweede lid
- Evaluatiecommissie Hoekstra, Eindrapportage Evaluatiecommissie Wet veiligheidsregio's en het stelsel van Rampenbestrijding en Crisisbeheersing, d.d. 18 september 2013
- Evaluatie NCTV organisatie 2012, Eindrapport, 15 september 2016
- EU CBRN Action Plan, 24 juni 2009
- Inspectie VenJ, Evaluatie Stelsel Bewaken en Beveiligen, oktober 2013
- Inspectie VenJ, Evaluatie van het Actieprogramma Integrale Aanpak Jihadisme, 2017
- Inspectie VenJ, Evaluatie van de rijkscrisisorganisatie tijdens de DigiNotar-crisis,
- Inspectie VenJ, Gebruik van beveiligingsadviezen van het Nationaal Cyber Security Centrum, mei 2015.
- Inspectie VenJ, Staat van de rampenbestrijding 2013 - Onderzoek Rampenbestrijding op Orde periode maart 2010 - oktober 2012, 2013
- Inspectie VenJ, Staat van de rampenbestrijding 2016 – Landelijk Beeld, oktober 2016
- Inspectie VenJ, Staat van de rampenbestrijding 2016 Landelijk beeld, oktober 2016
- Ministers van Justitie en Binnenlandse Zaken en Koninkrijksrelaties, Koninginnedag 2009, kenmerk 32054, 4 september 2009
- KPMG, Beleidsdoorlichting crisisbeheersing, 20 maart 2009
- Kwink groep & TU Delft, Inzicht in presterend vermogen veiligheidsregio's - onderzoek naar de mogelijkheid en wenselijkheid van een stelsel van indicatoren voor het presterend vermogen van veiligheidsregio's, 17 augustus 2015
- Ministerie van VenJ, DFEZ Meerjarig uitgavenkaderoverzicht: overzicht met goedgekeurde IBOS uitgavenmutaties vanaf 2007 bijgewerkt tot en met de stand ontwerpbegroting 2017
- Ministerie van VenJ, Nationale Cybersecurity Strategie, Slagkracht door samenwerking, 22 februari 2011
- Ministerie van VenJ, Nationale Cybersecurity Strategie 2, Van bewust naar bekwaam, 28 oktober 2013
- Minister van VenJ, Ontwerpvoorstel Besluit van tot wijziging van het Besluit personeel veiligheidsregio's in verband met de aanpassing van enkele functies van de GHOR en functies en rangen van de brandweer
- Minister van VenJ, Besluit van tot wijziging van het Besluit veiligheidsregio's in verband met de flexibilisering van de samenstelling van de crisisteams, een aanscherping van de regels over de rampbestrijdingsplannen voor inrichtingen en enkele andere onderwerpen
- Minister van VenJ, Beleidsnota rampenbestrijding, kenmerk 26956 nr. 136, 3 juli 2012
- Minister van VenJ, Informatie- en communicatietechnologie (ICT), kenmerk 26643, 12 december 2013
- Minister van VenJ, Informatie- en communicatietechnologie (ICT), kenmerk 26643, 18 december 2014
- Minister van VenJ, Informatie- en communicatietechnologie (ICT), kenmerk 26643, 14 oktober 2015
- Minister van VenJ, Veiligheidsregio's – Nationale Veiligheid, kenmerk 29517 30821 nr. 62, 5 juli 2012
- Minister van VenJ, Veiligheidsregio's, kenmerk 29517 nr. 69, 23 mei 2013
- Minister van VenJ, Veiligheidsregio's, kenmerk 29517 nr. 76, 22 november 2013
- Minister van VenJ, Veiligheidsregio's, kenmerk 29517 nr. 85, 2 juli 2014
- Minister van VenJ, Veiligheidsregio's, kenmerk 29517 nr. 90, 16 december 2014
- Minister van VenJ, Veiligheidsregio's, kenmerk 29517 nr. 101, 26 juni 2015
- Minister van VenJ, Veiligheidsregio's, kenmerk 29517 nr. 105, 25 november 2015
- Minister van VenJ, Veiligheidsregio's, kenmerk 29517 nr. 117, 25 oktober 2016
- Minister van VenJ, Veiligheidsregio's, kenmerk 29517 nr. 120, 17 mei 2017
- Minister van VenJ, Veiligheidsregio's, kenmerk 29517 nr. 121, 17 mei 2017
- Minister van VenJ, Veiligheidsregio's, kenmerk 29517 nr. 123, 27 juni 2017
- Minister van VenJ, Nationale Veiligheid, kenmerk 30821, nr. 16, 5 juni 2012

- Minister van VenJ, Nationale Veiligheid, kenmerk 30821, nr. 19, 8 november 2013
- Minister van VenJ, Nationale Veiligheid, kenmerk 30821, nr. 22, 10 juni 2014
- Minister van VenJ, Nationale Veiligheid, kenmerk 30821, nr. 23, 12 mei 2015
- Minister van VenJ, Nationale Veiligheid, kenmerk 30821, nr. 32, 15 september 2016
- Minister van VenJ, Nationale Veiligheid, kenmerk 30821, nr. 33, 12 oktober 2016
- Minister van VenJ, Nationale Veiligheid, kenmerk 30821, nr. 37, 12 december 2016
- Minister van VenJ, Nationale Veiligheid, kenmerk 30821, nr. 38, 22 mei 2017
- Minister van VenJ, reactie op Staat van de rampenbestrijding 2016, kenmerk 2023712, 7 december 2016
- Minister van VenJ, Vaststelling van de begrotingsstaten van Koninkrijksrelaties (IV) en het BES-fonds (H) voor het jaar 2016, kenmerk 34 300 IV, 15 april 2016
- Minister van VenJ, Staatsblad van het Koninkrijk der Nederlanden, Convenant Versterking Brandweeronderwijs in Nederland, kenmerk nr. 15261, 24 juli 2012
- Minister van VenJ, Staatsblad van het Koninkrijk der Nederlanden, Wet van 27 september 2012 tot wijziging van de Wet veiligheidsregio's in verband met de oprichting van het Instituut Fysieke Veiligheid en in verband met de volledige regionalisering van de brandweer, kenmerk 443, 27 september 2012
- Minister van VenJ, Staatsblad van het Koninkrijk der Nederlanden, Besluit van 26 oktober 2012 tot vaststelling van het tijdstip van inwerkingtreding van de Wet van 27 september 2012 tot wijziging van de Wet veiligheidsregio's in verband met de oprichting van het Instituut Fysieke Veiligheid en in verband met de volledige regionalisering van de brandweer (Stb. 2012, 443) en het Besluit rijksbijdragen IFV, kenmerk 526, 26 oktober 2012
- Minister van VenJ, Staatsblad van het Koninkrijk der Nederlanden, Besluit van 15 oktober 2015, houdende wijziging van het Besluit veiligheidsregio's, ter vereenvoudiging, actualisering en verbetering van dat besluit, alsmede ter aanpassing van de verdeelformule van de brede doeluitkering rampenbestrijding, kenmerk 381, 15 oktober 2015
- Minister van VenJ, Staatsblad van het Koninkrijk der Nederlanden, kenmerk nr. 27142, 25 september 2014
- Ministers van Justitie en BZK, Terrorismebestrijding, kenmerk 29 754, 1 juli 2010
- Nationale Contraterrorisme strategie 2011-2015,
- NCTb. Jaarplan 2011, definitief, 2011
- NCTV, Afronding project 'Solistische Dreigers' en vervolg, kenmerk 422909, 5 september 2013
- NCTV, Brief Verkenning regionale risicoprofielen, kenmerk 2015137, 18 november 2016
- NCTV, Exceloverzicht Apparaat, 7 november 2016
- NCTV, Jaarplan 2012, definitief, 15 februari 2012
- NCTV, Jaarplan 2013, definitief, 27 mei 2013
- NCTV, Jaarplan 2014, definitief, 31 oktober 2013
- NCTV, Jaarplan intern, 14 november 2013
- NCTV, Jaarplan 2015, definitief, 29 oktober 2014
- NCTV, Jaarplan intern 2015, januari 2015
- NCTV, kenmerk 420789, Versterking crisiscommunicatie, 19 augustus 2013
- NCTV, kenmerk 581475, Voortgang Actieprogramma integrale aanpak Jihadisme, 12 november 2014
- NCTV, kenmerk 630329, Voortgang Actieprogramma integrale aanpak Jihadisme, 7 april 2015
- NCTV, kenmerk 661133, Voortgang Actieprogramma integrale aanpak Jihadisme, 29 juni 2015
- NCTV, kenmerk 699134, Voortgang Actieprogramma integrale aanpak Jihadisme, 9 november 2015
- NCTV, kenmerk 661133, Voortgang Actieprogramma integrale aanpak Jihadisme, 29 juni 2015
- NCTV, kenmerk 743549, Voortgang Actieprogramma integrale aanpak Jihadisme, 16 maart 2016
- NCTV, kenmerk 779815, Voortgang Actieprogramma integrale aanpak Jihadisme, 11 juli 2016
- NCTV, 44e Dreigingsbeeld Terrorisme Nederland (DTN), april 2017
- NCTV, Nationaal Crisisplan Luchtvaartongevallen Burgerluchtvaart, september 2016
- NCTV, Organisatie & formatierapport, definitief, 5 juni 2012
- NCTV, Reactie op concept rapport Zicht overheden op beschermen burgers en bedrijven, kenmerk 567212, 3 oktober 2014
- NCTV, Rijksbrede rapportage voorbereiding op rampenbestrijding en crisisbeheersing in Caribisch Nederland
- NCTV, Voortgang Nationale Strategie Cybersecurity, kenmerk 275614, 6 juli 2012
- Nelen, Leeuw, Bogaerts, Antiterrorismebeleid en evaluatieonderzoek - framework, toepassingen en voorbeelden, 2010.
- Potomac Institute for Policy Studies, The Netherlands Cyber readiness at a glance, Cyber Readiness Index 2.0, all rights reserved
- PWC, Monitor Versterkingsgelden lokale aanpak Jihadisme, 29 september 2016
- Telecommunicatiewet, 1998
- TNO, The cost of cyber crime: Case of The Netherlands, 6 december 2011
- TNO, De staat van Netcentrisch Werken -update 2015 eindrapport, juni 2015
- Universiteit Maastricht, Pilot Dreigingsmanagement, een ex ante evaluatie, april 2012
- Universiteit Maastricht, Impact R&D, Pilot Dreigingsmanagement, De implementatie en wijze van uitvoering onder de loep, mei 2013
- Universiteit Twente, Broekema W.G., Giebels E., Gutteling J.M., Moorkamp M., Torenvlied R., Wessel R.A., Rapport Evaluatie Nationale Crisisbeheersingsorganisatie Vlucht MH17, 9 december 2015
- USBO Advies, Evaluatie CT strategie 2011 -2015: Gericht, gedragen en geborgd interventievermogen?, 8 april 2016
- Van Kempen, P.H.P.H.M.C, Fedorova, M.I., 'FOREIGN TERRORIST FIGHTERS': STRAFBAARSTELLING VAN VERBLIJF OP EEN TERRORISTISCH GRONDGEBIED?, 2015
- Veiligheidsberaad, Advies Bestuurlijke Werkgroep Bovenregionale Samenwerking, juni 2012
- Veiligheidsberaad, Bestuurlijke eindrapportage Project Continuïteit van de Samenleving

- Veiligheidsberaad, Eindrapportage Project Kwaliteit en vergelijkbaarheid, juni 2017
- Veiligheidsberaad, Eenheid in verscheidenheid – uitwerking advies Bestuurlijke werkgroep Bovenregionale Samenwerking, maart 2013
- Voorzitter Stuurgroep Versterking Brandweeronderwijs, Verantwoording project Vbo, 1 juli 2015
- Wet Veiligheidsregio's, 11 februari 2010
- WRR Wetenschappelijke Raad voor het Regeringsbeleid, De publieke kern van het internet – naar een buitenlands internetbeleid, 18 maart 2015

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00