Nationaal Coördinator
Terrorismebestrijding en Veiligheid
*Ministerie van Veiligheid en Justitie*

# Circulaire bewaken en beveiligen van personen, objecten en diensten 2015

# Circulaire bewaken en beveiligen van personen, objecten en diensten 2015

**Ons kenmerk**
658859

**Aard circulaire**
Bekendmaking van beleid

**Juridische achtergrond**
Vervangt circulaire d.d. 15 januari 2013 nr. 331437

**Geldig van/tot**
1 juli 2015 tot en met 30 juni 2019

# Inhoud


1 Algemeen 4
1.1 Doel van de circulaire 4
1.2 Ontwikkeling stelsel in vogelvlucht en totstandkoming van de circulaire 4
1.3 Leeswijzer circulaire 5

2 Het stelsel bewaken en beveiligen 6
2.1 Algemene uitgangspunten 6
2.2 Verantwoordelijkheidsverdeling 6
2.3 Relevante wet- en regelgeving 7

3 Systematiek stelsel: van dreiging naar beveiligingsmaatregelen 8
3.1 Informatie over dreiging en risico 8
3.1.1 Dreigingsniveaus 8
3.1.2 Risicoafweging 8
3.2 Informatieproducten 9
3.2.1 Dreigingsmelding 9
3.2.2 Informatierapport dreiging (IRD) 9
3.2.3 Dreigingsinschatting (DI) 9
3.2.4 Dreigingsanalyse (DA) 9
3.2.5 Risicoanalyse (RA) 9
3.3 Uitvoering 10

4 Uitgelicht: Decentraal domein 11
4.1 Reikwijdte van het decentraal domein 11
4.2 Taken en bevoegdheden in het kader van bewaken en beveiligen 11
4.3 Werkwijze decentraal gedeelte 12
4.4 Bedreigingen tegen leden van de lokale driehoek 12
4.5 Bijzondere situaties en het raakvlak tussen het decentraal- en het rijksdomein 13

5 Uitgelicht: Rijksdomein 14
5.1 Reikwijdte van het rijksdomein en limitatieve lijst 14
5.2 Rijksdomein: taken en bevoegdheden in het kader van bewaken en beveiligen 15
5.2.1 Persoonsbeveiliging 15
5.2.2 Bewaking en beveiliging van objecten en diensten in het rijksdomein 16
5.3 Rijksdomein: werkwijze 16
5.3.1 Afstemmingsoverleg Bewaken en Beveiligen (ABB) en Uitvoeringsoverleg (UO) 16
5.3.2 Buitenlandse bezoeken aan NL 16
5.4 Bewaken en beveiligen in het buitenland 17
5.5 Bijzondere situaties en het raakvlak tussen rijks- en decentraal domein 17

6 Overige aan bewaken en beveiligen gerelateerde onderwerpen 18
6.1 Nationale evenementen 18
6.2 Rol van de bedreigde persoon (medewerking, grenzen aan inspraak) 18
6.2.1 Grenzen aan inspraak bedreigde persoon 18
6.2.2 Deskundige begeleiding 19
6.3 Communicatie over bedreigingen en maatregelen 19

Bijlage 1 - Lijst van afkortingen 20
Bijlage 2 - Uitgebreid overzicht van de direct en indirect relevante wet- en regelgeving 21
Bijlage 3 - Tabellen Ernst en Waarschijnlijkheid 22
Bijlage 4 - De Limitatieve Lijst 24

# 1 Algemeen

In deze circulaire bewaken en beveiligen van personen, objecten, en diensten 2015 (hierna: de circulaire bewaken en beveiligen) worden de wet- en regelgeving en de werkafspraken met betrekking tot dit terrein weergegeven. Dit geheel van regelgeving en afspraken is het stelsel bewaken en beveiligen. Het doel van het stelsel bewaken en beveiligen is het voorkomen van (terroristische) aanslagen op personen, objecten en diensten. Het regelt op welke manier er beveiligd wordt als er sprake is van dreiging. Bij de beveiliging van personen staat het voorkomen van ernstige schending van de fysieke integriteit centraal. In dit hoofdstuk worden het doel van de circulaire en de ontwikkeling van het stelsel toegelicht. Dit hoofdstuk wordt afgesloten met een leeswijzer.

## 1.1 Doel van de circulaire

Het stelsel bewaken en beveiligen is een gelaagd stelsel dat gebaseerd is op (een beperkte hoeveelheid) wet- en regelgeving en verder bestaat uit (werk)afspraken tussen de betrokken partners. De circulaire bewaken en beveiligen geeft een overzicht van de regelgeving waarop het stelsel is gebaseerd en de (proces)afspraken en procedures die op basis hiervan zijn gemaakt. Het bewaken en beveiligen van personen, objecten en diensten is een beleidsterrein waarbij continu afwegingen worden gemaakt. Deze circulaire biedt geen uitputtend overzicht van alle (details in de) werkafspraken, dan wel de taken en bevoegdheden van de bij het stelsel betrokken partners.

De circulaire is bedoeld voor alle partners binnen het domein bewaken en beveiligen, zowel in het decentrale- als het rijksdomein. Dit zijn bijvoorbeeld het Openbaar Ministerie (OM), de regionale eenheden en landelijke eenheid van de politie (hierna: de politie), de inlichtingen- en veiligheidsdiensten, gemeentelijke overheden, de Koninklijke Marechaussee (KMar), de beveiligingsambtenaren van de departementen en de Staten-Generaal (BVA's), en de ministeries van Buitenlandse Zaken, Defensie, Veiligheid en Justitie, en Binnenlandse Zaken en Koninkrijksrelaties.

## 1.2 Ontwikkeling stelsel in vogelvlucht en totstandkoming van de circulaire

Het huidige Stelsel bewaken en beveiligen is in 2002 ingericht. De aanleiding hiervoor was de aanslag op de heer W.S.P. Fortuyn op 6 mei 2002 en het onderzoek dat hiernaar is verricht door de commissie Feitenonderzoek onder voorzitterschap van mr. H. F. van den Haak[1]. Bij brief van 20 juni 2003 is de voorzitter van de Tweede Kamer der Staten-Generaal geïnformeerd over het "nieuwe stelsel bewaken en beveiligen"[2].

Twee jaar na de moord op Fortuyn zijn de procedures en de verantwoordelijkheden voor het beschermen van personen en diensten wettelijk vastgelegd door middel van aanpassing van de Politiewet 1993. Tevens is de wet op de inlichtingen- en veiligheidsdiensten van 2002 (WIV 2002) aangepast. Hierin is vastgelegd dat de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) fungeren als leverancier van informatie ten behoeve van personen, objecten en diensten in het rijksdomein en wordt een beschrijving gegeven van de wijze waarop de diensten hun taken in de praktijk invullen.

Sinds het ontstaan is het stelsel bewaken en beveiligen beïnvloed door gebeurtenissen en ontwikkelingen in binnen- en buitenland. Voorbeelden hiervan zijn de aanslagen in Madrid en de moord op Theo van Gogh, beiden in 2004, en de aanslagen in Londen in 2005. De departementale herindeling met betrekking tot veiligheid in 2010 en de vorming van een nationale politie zijn eveneens van invloed op de werking en de inhoud van het stelsel en de circulaire bewaken en beveiligen. De meest recente aanpassing van de circulaire bewaken en beveiligen stamt uit 2008. Daarna is de circulaire op basis van de Politiewet 2012 technisch aangepast en nog twee keer verlengd.

[1] Commissie Feitenonderzoek veiligheid en beveiliging Pim Fortuyn. "De veiligheid en de beveiliging van Pim Fortuyn: feiten en verantwoordelijkheden", Den Haag 2002

[2] Tweede Kamer, vergaderjaar 2002-2003, 28 974, nrs. 1 en 2.

In 2013 heeft de minister van Veiligheid en Justitie – vanwege het ruim 10 jaar bestaan van het stelsel - de Inspectie Veiligheid en Justitie gevraagd een aantal gesprekken te voeren met betrokkenen van het stelsel en de werkprocessen na te lopen. De Inspectie concludeerde dat de kern van het stelsel voldoet maar dat een veranderende samenleving maakt dat een voortdurende professionalisering van het stelsel in overleg tussen alle betrokken partijen nodig blijft. Om hier invulling aan te geven komen bij het stelsel bewaken en beveiligen betrokken partners periodiek in een stuurgroep bijeen om van gedachten te wisselen en sturing te geven aan verbeteringen of ontwikkelingen die het stelsel aangaan[3]. Ook kunnen ideeën, opvattingen en meningen gedeeld worden ten aanzien van strategische of politiekgevoelige vraagstukken aangaande de bewaking en beveiliging van personen, objecten, en diensten. Deze circulaire is tot stand gekomen in overleg met de bij het stelsel betrokken partners en afgestemd binnen de stuurgroep bewaken en beveiligen.

## 1.3 Leeswijzer circulaire

In hoofdstuk twee van deze circulaire wordt een toelichting gegeven op de uitgangspunten en de werking van het stelsel, de belegging van verantwoordelijkheden en de afbakening. Vervolgens wordt in hoofdstuk drie weergegeven hoe de systematiek van het stelsel werkt: van dreiging naar bewakings- en beveiligingsmaatregelen. Daarna worden in de hoofdstukken vier en vijf zowel het decentrale domein als het rijksdomein uitgelicht. Hierin staan de reikwijdte, taken en bevoegdheden en bijzondere situaties binnen deze domeinen centraal. Tot slot worden in hoofdstuk zeven de onderwerpen nationale evenementen, rol van de bedreigde persoon en de grenzen aan inspraak, deskundige begeleiding en communicatie over bedreigingen en beveiligingsmaatregelen toegelicht. In de bijlagen is een lijst van gebruikte afkortingen met de bijbehorende organisaties ingevoegd, evenals een uitgebreid overzicht van wet- en regelgeving en de tabellen Ernst en Waarschijnlijkheid. Bijlage 4 is de limitatieve lijst. Deze is gerubriceerd en zodoende niet bij de openbare versie van de circulaire gevoegd.

[3] Dit is de stuurgroep bewaken en beveiligen onder voorzitterschap van de directie Bewaking, Beveiliging, Burgerluchtvaart van de NCTV. Het OM, de AIVD, de MIVD, de politie en de KMar nemen deel aan deze stuurgroep. Afstemming is niet beperkt tot de stuurgroep bewaken en beveiligen. Afstemming vindt ook plaats, buiten de stuurgroep, met bijvoorbeeld de ministeries van Buitenlandse Zaken en Defensie en binnen het ministerie van Veiligheid en Justitie.

# 2 Het stelsel bewaken en beveiligen

Dit hoofdstuk geeft een overzicht van de algemene uitgangspunten van het stelsel, de bijbehorende verantwoordelijkheidsverdeling, en de relevante wet- en regelgeving.

## 2.1 Algemene uitgangspunten

Het doel van het stelsel bewaken en beveiligen is het voorkomen van (terroristische) aanslagen op personen, objecten en diensten. Bij de beveiliging van personen staat het voorkomen van ernstige schending van de fysieke integriteit centraal. In het stelsel werken het OM, inlichtingen- en veiligheidsdiensten, politie en bestuurlijke organisaties samen om zorg te dragen dat personen, objecten en diensten, ondanks dreiging en risico, zo veilig en zo ongestoord mogelijk kunnen functioneren. In het stelsel is geregeld hoe op basis van informatie over dreiging en risico tot beveiligingsmaatregelen wordt besloten. De volgende uitgangspunten zijn bepalend voor het stelsel:

- Uitgangspunt van het stelsel is dat personen zelf verantwoordelijk zijn voor hun veiligheid. Ze mogen daarbij rekenen op de organisaties waar ze deel van uitmaken of voor werkzaam zijn. Bedrijven en instellingen dienen maatregelen te treffen om te voorkomen dat de veiligheid van medewerkers in gevaar komt als gevolg van hun werkzaamheden. De overheid kan aanvullende beveiligingsmaatregelen nemen als een persoon of de organisatie waar zij deel van uitmaken of waarvoor zij werken op eigen kracht geen weerstand kan bieden tegen de dreiging en het risico. De kostenverdeling volgt de verantwoordelijkheidsverdeling;
- Een ander uitgangspunt is dat het waken over de veiligheid voornamelijk decentraal is belegd (decentraal, tenzij…). Dit betekent in beginsel dat de veiligheidszorg voor alle personen, objecten en diensten onder verantwoordelijkheid van het decentrale gezag plaatsvindt. Het decentrale gezag wordt gevormd door de burgemeester en de hoofdofficier van justitie (HOvJ). Als uitzondering hierop is er sprake van een bijzondere verantwoordelijkheid van het centrale gezag (de rijksoverheid) voor bepaalde (groepen) personen, objecten en diensten die een nationaal belang vertegenwoordigen;
- Tevens geldt het uitgangspunt van proportionaliteit van de maatregelen. De inschatting van de dreiging en het risico is leidend voor het vaststellen van de benodigde beveiligingsmaatregelen. Op deze wijze wordt er voor gezorgd dat adequate beveiligingsmaatregelen worden getroffen. Beveiligingsmaatregelen hebben altijd een impact op de te beveiligen persoon, het object of de dienst en de omgeving. Beveiliging is erop gericht om met zo min mogelijk impact zoveel mogelijk weerstand te creëren tegen de dreiging en het risico;
- In het stelsel kan gebruik worden gemaakt van beveiligingsmaatregelen variërend van lichte maatregelen als extra politiesurveillance tot zware maatregelen als persoonsbeveiliging en objectbeveiliging. Hierdoor is maatwerk mogelijk;
- Bij het nemen van beveiligingsmaatregelen is er sprake van risico management, geen risico-uitsluiting. Veiligheid is een uitkomst van een zorgvuldige afweging door deskundigen, op dreiging, risico en het niveau van maatregelen. Veiligheid kan niet worden gegarandeerd.

## 2.2 Verantwoordelijkheidsverdeling

Het stelsel bewaken en beveiligen bestaat uit een decentraal domein en een rijksdomein. De veiligheid van personen, objecten en diensten is in beginsel decentraal georganiseerd. Het lokaal bevoegd gezag is verantwoordelijk voor het nemen van aanvullende beveiligingsmaatregelen op basis van (voorstelbare) dreiging en risico. Het lokale gezag wordt gevormd door de burgemeester en de HOvJ. De burgemeester is verantwoordelijk voor de handhaving van de openbare orde en veiligheid. De HOvJ is verantwoordelijk voor de strafrechtelijke handhaving van de rechtsorde, waaronder de veiligheid van personen (zie ook paragraaf 4.2 in het hoofdstuk 'Uitgelicht decentraal domein').

De rijksoverheid heeft een bijzondere verantwoordelijkheid voor een beperkte groep personen, objecten en diensten: het rijksdomein. Deze personen, diensten of objecten staan op de zogenoemde limitatieve lijst vanwege het nationale belang dat met hun veilig en ongestoord functioneren is gemoeid. Het centraal bevoegd gezag is de minister van Veiligheid en Justitie, gemandateerd aan de Coördinator Bewaking en Beveiliging (CBB) van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) (zie ook paragraaf 5.2 in het hoofdstuk 'Uitgelicht rijksdomein').

De AIVD, MIVD en de politie leveren informatie over concrete dan wel voorstelbare dreiging. Op basis van deze informatie kan worden besloten tot beveiligingsmaatregelen. De beveiligingsmaatregelen worden uitgevoerd door de politie en/of de KMar.

## 2.3 Relevante wet- en regelgeving

Het stelsel bewaken en beveiligen volgt de inrichting van het Nederlandse staatsbestel en de bestaande politiële en justitiële structuren en is gebaseerd op wet- en regelgeving waar deze in zijn vastgelegd.

De taak om te bewaken en te beveiligen maakt onderdeel uit van de politietaak om zorg te dragen voor de daadwerkelijke handhaving van de rechtsorde (artikel 3 van de Politiewet 2012). De handhaving van de rechtsorde bestaat uit openbare orde handhaving en strafrechtelijke handhaving.

Op basis van de Gemeentewet, artikel 172, is de burgemeester belast met de handhaving van de openbare orde. Hij bedient zich daarbij van de onder zijn gezag staande politie.

De HOvJ is verantwoordelijk voor de strafrechtelijke handhaving van de rechtsorde. Artikel 1, lid 2 van de Politiewet 2012 stelt dat "in deze wet en de daarop berustende bepalingen wordt onder strafrechtelijke handhaving van de rechtsorde mede verstaan: het waken voor de veiligheid van personen".

In Artikel 16 van de Politiewet 2012, lid 1 is bepaald dat de minister van Veiligheid en Justitie objecten en diensten kan aanwijzen waarvan bewaking of beveiliging door de politie noodzakelijk is in het belang van de veiligheid van de Staat of de betrekkingen van Nederland met andere mogendheden, dan wel met het oog op zwaarwegende belangen van de samenleving. Dit geldt eveneens voor personen hetgeen is geregeld in artikel 42 en 43 van de Politiewet. Deze artikelen zijn de basis voor het rijksdomein en de verantwoordelijkheid van de minister van Veiligheid en Justitie ten aanzien van de limitatieve lijst. De minister van Veiligheid en Justitie is op basis van deze artikelen de bevoegde autoriteit om de politie opdracht te geven tot persoonsbeveiliging voor personen binnen het rijksdomein. In het decentrale domein ligt het gezag over persoonsbeveiliging door de politie bij de HOvJ.

Aanvullend hieraan heeft de minister van Veiligheid en Justitie op grond van artikel 15, derde lid, van de Politiewet 2012 een aanwijzingsbevoegdheid jegens de burgemeesters. De minister van Veiligheid en Justitie kan de burgemeesters algemene en bijzondere aanwijzingen geven met betrekking tot de handhaving van de openbare orde, voor zover dat noodzakelijk is in het belang van de veiligheid van de Staat of de betrekkingen van Nederland met andere mogendheden, dan wel met het oog op zwaarwegende belangen van de samenleving. Een dergelijke aanwijzing van de minister van Veiligheid en Justitie moet worden aangemerkt als een volledig bindende aanwijzing. De burgemeester is derhalve verplicht met inachtneming van de aanwijzing te handelen.

Op grond van artikel 127 van de wet op de rechterlijke organisatie kan de minister van Veiligheid en Justitie algemene en bijzondere aanwijzingen geven betreffende de uitoefening van de taken en bevoegdheden van het OM.

De Politiewet regelt eveneens de taken van de politie en de KMar. Hoofdstuk 2 van de Politiewet beschrijft de algemene taak van de politie en de politietaken van de KMar. In hoofdstuk 5 is bepaald dat de politie en de KMar bijstand kunnen leveren aan elkaar en dat in bijzondere gevallen ook bijstand kan worden verleend door andere delen van de krijgsmacht.

In de WIV 2002 is het geheel aan taken vastgelegd dat door de AIVD en de MIVD wordt verricht. De inlichtingen- en veiligheidsdiensten leveren gevraagd en ongevraagd informatie aan de CBB van de NCTV.

De taak van de AIVD in relatie tot het Stelsel bewaken en beveiligen is vastgelegd in artikel 6, tweede lid, onderdeel e juncto artikel 6a van de WIV 2002. Voor de MIVD is de taak in relatie tot het stelsel bewaken en beveiligen vastgelegd in artikel 7, tweede lid, onderdeel f juncto artikel 7a van de WIV 2002. Deze artikelen vormen de basis voor de informatieproducten in het kader van het stelsel bewaken en beveiligen.

De wet politiegegevens regelt de verwerking en verspreiding van politiegegevens met het oog op de uitvoering van de politietaak.

In bijlage 2 is een uitgebreid overzicht opgenomen van de direct en indirect relevante wet- en regelgeving.

# 3 Systematiek stelsel: van dreiging naar beveiligingsmaatregelen

In dit hoofdstuk wordt de werkwijze binnen het stelsel om van dreiging en risico tot beveiligingsmaatregelen te komen toegelicht. Ook worden de bijbehorende informatieproducten benoemd. De beschreven systematiek en producten zijn grotendeels gelijk in zowel het decentrale- als het rijksdomein. Waar dit afwijkt wordt dit aangegeven. In de hoofdstukken vier en vijf waarin het decentrale- en het rijksdomein worden uitgelicht, wordt de werkwijze verder toegelicht en aangegeven welke partijen betrokken zijn in de uitvoering.

## 3.1 Informatie over dreiging en risico

Binnen het stelsel bewaken en beveiligen wordt specifieke informatie verzameld over dreiging en risico ten aan zien van personen, objecten en diensten. De opsporings-, inlichtingen- en veiligheidsdiensten bestaande uit de AIVD, MIVD, Dienst Landelijke Informatie Organisatie van de politie (DLIO) en Dienst Regionale Informatie Organisatie van de politie (DRIO) stellen informatieproducten op met specifieke informatie over personen, objecten en diensten[4]. Er wordt zowel op decentraal als rijksniveau gewerkt met een bepaalde systematiek voor het bepalen van het dreigingsniveau en het afwegen van risico's. Op basis hiervan wordt gefundeerd overwogen ten aanzien van welke personen, objecten en diensten bewaking en beveiliging nodig is.

### *3.1.1 Dreigingsniveaus*

Voor het vaststellen van het dreigingsniveau worden zowel in het decentrale- als in het rijksdomein dezelfde speciaal ontwikkelde tabellen gehanteerd. Aan de hand van de tabellen wordt een inschatting gemaakt van de mate van 'ernst' en 'waarschijnlijkheid' (effect en voorstelbaarheid) van de dreiging. Hierdoor ontstaat een glijdende schaal van dreigingsniveaus. De tabellen op basis waarvan aard en omvang van de dreiging worden ingeschat zijn als bijlage 3 bij deze circulaire gevoegd.

Voor het vaststellen van het dreigingsniveau wordt een model gehanteerd met een dubbele kwalificering. Maatwerk is hierdoor mogelijk. De tabellen (bijlage 3) geven inzicht in de afwegingen en uitkomst van de inschatting van de ernst van de gebeurtenis en de waarschijnlijkheid van het manifesteren van deze gebeurtenis. De twee elementen 'ernst' en 'waarschijnlijkheid' geven een indicatie van de aard/effect en voorstelbaarheid dat de dreiging zich openbaart. Op basis van deze informatie bepaalt de overheid of ze iets moet ondernemen tegen een dreiging.

De dreigingsinschatting ten behoeve van het decentrale domein wordt vervaardigd door de DRIO van de betreffende regionale eenheid. Indien daar aanleiding toe bestaat, bijvoorbeeld wanneer andere regionale eenheden mogelijk over relevante informatie beschikken, kan DLIO een dreigingsanalyse opstellen.

De inschatting ten behoeve van het rijksdomein, in de vorm van een dreigingsinschatting of een dreigings- of risicoanalyse, wordt, afhankelijk van de aard, gevraagd en ongevraagd door de AIVD, MIVD en/of DLIO vervaardigd. De BVA's leveren eveneens informatie ten behoeve van de beveiliging van de voor hen relevante personen, objecten en diensten aan de Coördinator Bewaking en Beveiliging (CBB).

### *3.1.2 Risicoafweging*

In het algemeen kan niet worden volstaan met een beoordeling van, al dan niet concrete, dreiging, maar zullen ook eventuele risico's moeten worden gewogen. Om risico's te beheersen kunnen maatregelen worden genomen. In elk individueel geval zal worden afgewogen of sprake is van een geaccepteerd risico. Indien daarvan sprake is, zullen veelal geen maatregelen worden genomen. Is er sprake van een onaanvaardbaar risico dan zullen maatregelen moeten worden genomen die het risico tot een geaccepteerd niveau terugdringen. De mate waarin sprake is van een geaccepteerd of onaanvaardbaar risico is niet op basis van concrete gegevens kwantificeerbaar.

[4] Daarnaast bestaat het Dreigingsbeeld Terrorisme Nederland (DTN). Het DTN geeft een algemeen sfeerbeeld en is niet direct gerelateerd aan het stelsel. Het DTN is een globale analyse van de nationale en internationale terroristische dreiging tegen Nederland en Nederlandse belangen in het buitenland. In het DTN wordt, naast de actuele zaken, verschillende thematiek behandeld, zoals radicalisering, extreemrechts, polarisatie, het internationale profiel van Nederland, tegenmaatregelen, en dergelijke. Op basis van het DTN wordt uiteindelijk het dreigingsniveau van Nederland bepaald (minimaal, beperkt, substantieel, kritiek).

## 3.2 Informatieproducten

Op basis van de onderstaande informatieproducten bepaalt de overheid of ze iets onderneemt tegen een dreiging. Het uniforme gebruik van deze producten zorgt voor eenduidigheid in gehanteerde begrippen. In deze paragraaf volgen de gehanteerde informatieproducten van de opsporings-, inlichtingen- en veiligheidsdiensten.

### 3.2.1 *Dreigingsmelding*

Een melding van een concrete dreiging tegen een persoon, object of dienst, zonder waardering van de ernst en waarschijnlijkheid. Een dreigingsmelding betreft altijd een concrete dreiging die zich zeer waarschijnlijk of zeker op korte termijn zal voordoen. Dreigingsmeldingen kunnen worden opgesteld voor zowel het decentrale als het rijksdomein en worden gevraagd en ongevraagd (zo nodig spoedshalve) verstrekt door de opsporings-, inlichtingen- en veiligheidsdiensten. In de dreigingsmelding wordt aandacht besteed aan zowel de dreiger als bedreigde.

### 3.2.2 *Informatierapport dreiging (IRD)*

Aanvullend op onderstaande stelselproducten is een decentraal format ontwikkeld: het IRD. Dit product is bedoeld om op decentraal niveau bij directe concrete dreiging een eerste indruk te geven van de situatie zodat op basis van de IRD de eerste (spoed)maatregelen getroffen kunnen worden.

### 3.2.3 *Dreigingsinschatting (DI)*

Dreigingsinschattingen worden voor zowel het decentrale als het rijksdomein opgesteld. En worden gevraagd en ongevraagd (zo nodig spoedshalve mondeling) verstrekt door opsporings-, inlichtingen- en veiligheidsdiensten.

Een dreigingsinschatting is doorgaans een beknopt product waarin de ernst en waarschijnlijkheid van de concrete en voorstelbare dreiging tegen een persoon, object of dienst wordt ingeschat. De inschatting is gebaseerd op feiten of omstandigheden met betrekking tot een dreiging en de ernst en waarschijnlijkheid van het manifesteren van de dreiging.

### 3.2.4 *Dreigingsanalyse (DA)*

Een dreigingsanalyse is een uitgebreide analyse van concrete (voorspelbare) en potentiële (voorstelbare) dreiging tegen één of meer bepaalde personen, objecten of diensten. De analyse is gebaseerd op feiten en omstandigheden met betrekking tot de dreiging en de ernst en waarschijnlijkheid van het manifesteren van de dreiging. Dreigingsanalyses kunnen worden opgesteld voor zowel het decentrale als het rijksdomein.

Voor het decentraal domein wordt op verzoek van de HOvJ de dreigingsanalyse opgesteld door de DRIO. Dreigingsanalyses voor personen, objecten en diensten in het rijksdomein worden op verzoek van de minister van Veiligheid en Justitie opgesteld door de AIVD, MIVD en DLIO[5].

### 3.2.5 *Risicoanalyse (RA)*

Een risicoanalyse is een uitgebreide analyse waarin het belang, de concrete en voorstelbare dreiging en de weerstand in onderlinge samenhang worden beoordeeld en inzicht wordt gegeven in de risico's die een persoon, object of dienst loopt. In een risicoanalyse wordt aangegeven wat het belang van de persoon, object of dienst is en wordt de concrete en voorstelbare dreiging tegen de persoon, het object of de dienst beschreven. In de vorm van scenario's wordt vervolgens beschreven in hoeverre de bestaande weerstand voldoende is om de geschetste dreiging te weerstaan. Tot slot worden belang, dreiging en weerstand in hun onderlinge samenhang beoordeeld. Het risico is vervolgens de mate waarin de weerstand tekort schiet tegen een bepaalde dreiging[6].

[5] Gelet op de verantwoordelijkheid van de minister van Defensie voor zijn organisatie en personeel kan, in aanvulling op het rijksdomein, de MIVD ook dreigingsanalyses opstellen van dreigingen tegen een bij de krijgsmacht werkzaam persoon of een bij de krijgsmacht in gebruik zijnde object. Gelet op het bijzondere karakter van die onderzoeken zal de minister van Defensie zelf bepalen (en derhalve niet in mandaat) of die onderzoeken worden verricht.

[6] Op grond van de WIV 2002 heeft de AIVD als enige dienst tot taak risicoanalyses op te stellen. Deze risicoanalyses zijn enkel op te stellen voor het rijksdomein. Dus ook ten behoeve van de beveiliging van personen, objecten en diensten in het rijksdomein met een militaire relevantie. De AIVD ontvangt hiervoor informatie van de andere diensten (bijvoorbeeld DLIO en MIVD).

## 3.3 Uitvoering

Op basis van de genoemde systematiek en betreffende informatieproducten voor dreiging en risico, wordt de verkregen informatie en analyses op hun onderlinge samenhang beoordeeld. De informatie kan voorts worden vergeleken met informatie verkregen uit andere bronnen. Op basis van een zo compleet mogelijk beeld wordt het niveau van de dreiging vastgesteld door het lokaal bevoegd gezag of door de CBB voor het rijksdomein.

Zowel in het decentrale als in het rijksdomein worden zogenoemde 'verhoogd risico momenten' aangemeld. Een 'verhoogd risicomoment' is een moment waarbij een persoon in het kader van het uitoefenen van zijn functie optreedt in een voor breed publiek toegankelijke plaats waarbij een risico kan worden verondersteld. Deze wordt aangemeld bij de CBB wanneer het een persoon in het rijksdomein betreft en bij de portefeuillehouder CCB (Conflict en Crisisbeheersing) van de regionale eenheid wanneer het een persoon in het decentraal domein betreft. De CBB (voor het rijksdomein) en CCB (voor het decentrale domein) stellen vast of op het te evalueren verhoogd risicomoment maatregelen worden geadviseerd.

Het is aan de uitvoeringsorganisatie (Politie of KMar) om een integraal inzetconcept (maatregelenpakket) uit te voeren dat weerstand biedt tegen het vastgestelde dreigingsniveau. De te treffen maatregelen worden voorgelegd aan, afgestemd met en uitgevoerd onder het bevoegde gezag.

Getroffen beveiligingsmaatregelen zijn, met uitzondering van categorie I van de limitatieve lijst (zie paragraaf 5.1), op basis van dreiging en risico en dus zelden van permanente aard. De geconstateerde concrete en/of potentiële dreiging en risico en de naar aanleiding daarvan getroffen maatregelen dienen periodiek te worden getoetst of voortzetting van de maatregelen nog opportuun is.

# 4 Uitgelicht: Decentraal domein

In dit hoofdstuk komt de reikwijdte van het decentrale domein aan de orde, evenals de werkwijze. Ook wordt aandacht besteed aan bedreigingen tegen de leden van de lokale driehoek. Om de raakvlakken tussen het decentrale en het rijksdomein helder weer te geven wordt tevens aandacht besteed aan de situaties waarin het decentrale domein en het rijksdomein elkaar overlappen of nauw met elkaar samenwerken.

## 4.1 Reikwijdte van het decentraal domein

De veiligheid van personen, objecten en diensten is in beginsel decentraal georganiseerd. In het decentrale deel van het stelsel bewaken en beveiligen neemt het lokaal bevoegd gezag zelf besluiten over extra beveiligingsmaatregelen om een dreiging in de richting van personen, objecten of diensten af te wenden. Het lokaal bevoegd gezag kan dezelfde beveiligingsmaatregelen treffen ten behoeve van personen, objecten of diensten als het gezag in het rijksdomein.

Er kan op decentraal niveau aanleiding bestaan om bepaalde personen, objecten of diensten voor te dragen voor (tijdelijke) toevoeging op de limitatieve lijst. Hierover vindt overleg plaats met de CBB. De NCTV beslist op voorstel van de CBB namens de minister van Veiligheid en Justitie of een persoon, object of dienst (tijdelijk) op de limitatieve lijst wordt geplaatst. (zie paragraaf 5.1 voor meer informatie over tijdelijke toevoeging aan het rijksdomein). Zolang de NCTV geen expliciet besluit hierover heeft genomen blijft de verantwoordelijkheid decentraal belegd.

## 4.2 Taken en bevoegdheden in het kader van bewaken en beveiligen

Wanneer er sprake is van een concrete of voorstelbare dreiging blijven de persoon en de werkgever zelf verantwoordelijk voor het treffen van (aanvullende) maatregelen die de gevolgen van eventuele inbreuken op de veiligheid voorkomen. Zij blijven in eerste instantie verantwoordelijk voor hun eigen veiligheid en het leveren van een bijdrage aan het bevorderen van de veiligheid, inclusief het treffen van maatregelen als daarvoor noodzaak is. Dit geldt zowel voor de werklocatie als het privédomein (woningen, werkplek, vervoersmiddel, etc.) van de betrokkene(n). Vanuit overheidszijde kan hierin worden geadviseerd. De overheid zal aanvullende beveiligingsmaatregelen treffen als de aard en de omvang van de dreiging dermate is dat persoon en werkgever daar zelf geen weerstand (meer) tegen kunnen bieden.

De taak om te bewaken en te beveiligen maakt onderdeel uit van de politietaak om zorg te dragen voor de daadwerkelijke handhaving van de rechtsorde. De daadwerkelijke handhaving valt uiteen in openbare orde handhaving onder verantwoordelijkheid van de burgemeester, en strafrechtelijke handhaving onder verantwoordelijkheid van de HOvJ (zie paragraaf 2.3. voor de bijbehorende wet- en regelgeving). In de praktijk liggen openbare orde- en strafrechtelijke handhavingstaken dicht bij elkaar. Bij ordeverstoringen worden vaak ook strafbare feiten gepleegd, terwijl sommige strafbare feiten op hun beurt weer een verstoring van de openbare orde kunnen inhouden. De ernst van de dreiging en in het bijzonder het effect en de aard van de verwachte gebeurtenis dienen bepalend te zijn voor de vraag bij wie het primaat ligt binnen het lokale gezag.

De burgemeester is op grond van zijn verantwoordelijkheid voor de openbare orde verantwoordelijk voor de bewaking en beveiliging van objecten en diensten. Indien er sprake is van strafrechtelijke handhaving van de rechtsorde, zoals in geval van een concrete dreiging waarbij beveiligingsmaatregelen worden genomen ter voorkoming van strafbare feiten, dan valt de bewaking en beveiliging van objecten en diensten onder verantwoordelijkheid van de HOvJ.

Het waken voor de veiligheid van personen is expliciet benoemd als onderdeel van de strafrechtelijke handhaving van de rechtsorde. De HOvJ draagt hierover het gezag. Hij is in deze gevallen verantwoordelijk voor de aanvraag van een dreigingsinschatting, het besluit tot het treffen van maatregelen, en het (laten) informeren van de betreffende persoon.

## 4.3 Werkwijze decentraal gedeelte

In het decentrale domein spelen veelal zaken van concrete (be)dreiging, bijvoorbeeld in de relationele of criminele sfeer die vallen onder het gezag van de HOvJ als onderdeel van de strafrechtelijke handhaving van de rechtsorde.

De HOvJ beoordeelt, op advies van de politie, in hoeverre de persoon en/of zijn werkgever in staat is weerstand te bieden aan de dreiging. De doelstelling is het voorkomen van ernstige misdrijven waarbij de aantasting van de veiligheid zulke gewelddadige vormen aanneemt dat het leven of de fysieke integriteit van de bedreigde ernstig in het geding komt. In het decentrale domein worden ook beveiligingsmaatregelen genomen op basis van voorstelbaarheid, bijvoorbeeld rondom bepaalde objecten.

Wanneer bij de politie een dreiging wordt gemeld of aangifte van een dreiging wordt gedaan, wordt deze dreiging ter kennis gebracht van de afdeling Regionale Conflict en Crisisbeheersing (RCCB) van de politie. Bij de RCCB vindt een eerste weging plaats of de dreiging op persoon, object, of dienst in aanmerking komt voor het stelsel bewaken en beveiligen. Is dit niet het geval dan valt deze casus onder de reguliere basispolitiezorg. Indien de dreiging wel in aanmerking komt voor het stelsel bewaken en beveiligen wordt de casus gemeld aan de beleidsmedewerker bewaken, beveiligen en crisisbeheersing (BB&C) van het OM. Deze overlegt met de HOvJ, die de politie opdracht geeft tot het opstellen van een DI of IRD, of legt de casus terug bij regulier basispolitiewerk.

Na ontvangst van het IRD wordt op advies van RCCB besloten tot het treffen van beveiligingsmaatregelen of wordt de casus alsnog terugverwezen naar de basispolitiezorg. Na ontvangst van de DI wordt door de HOvJ opdracht gegeven tot het opstellen van een maatregeladvies of wordt de casus alsnog terugverwezen naar de basispolitiezorg. Er wordt intensief samengewerkt tussen RCCB en DRIO.

Een aangifte/melding (van ketenpartners, een persoon of anonieme melding van Meld Misdaad Anoniem) of informatie uit een opsporingsonderzoek kan, nadat de HOvJ hiertoe opdracht heeft gegeven, leiden tot het opstellen van een DI door medewerkers van DRIO.

Wanneer er een aangifte, melding of informatie uit een onderzoek komt, dan wordt het doorgegeven aan de RCCB.

In onvoorziene- of spoedzaken worden onder verantwoordelijkheid van de portefeuillehouder CCB van de betreffende eenheid op voorhand maatregelen genomen in afwachting van definitieve besluiten. Deze voorlopige maatregelen worden afgestemd met de beleidsmedewerker BB&C van het OM.

Beveiligingsmaatregelen worden over het algemeen uitgevoerd door de politie. De KMar kan– in bijzondere gevallen - onder lokaal bevoegd gezag eveneens bewakings- en beveiligingstaken uitvoeren[7]. Persoonsbeveiliging wordt uitgevoerd door de Dienst Bewaken en Beveiligen van de politie (DBB) onder gezag van de HOvJ.

## 4.4 Bedreigingen tegen leden van de lokale driehoek

In het bijzondere geval dat een burgemeester of een politiechef zelf onderwerp is van dreiging, vindt een afweging ten aanzien van de volledigheid en proportionaliteit van de te treffen maatregelen plaats door de CBB van de NCTV. Hiermee wordt voorkomen dat deze functionarissen, door bespreking van de maatregelen in de lokale driehoek, betrokken raken bij de besluitvorming over beveiligingsmaatregelen die op henzelf betrekking hebben. Dit betekent niet dat de betrokkene daarmee wordt toegevoegd aan het rijksdomein. De HOvJ van het arrondissement van de woonplaats van de bedreigde persoon stelt de procedure in werking. Deze verloopt volgens het reguliere proces. De dreiging wordt lokaal door de politie ingeschat en vormt de basis van een maatregelenadvies voor de verantwoordelijke HOvJ. De NCTV adviseert in dit proces over de proportionaliteit van de maatregelen. De HOvJ beslist over de maatregelen, het advies van de NCTV gehoord hebbende.

Indien een HOvJ wordt bedreigd dan is de HOvJ van diens woonplaats verantwoordelijk voor het treffen van maatregelen. Indien de bedreigde HOvJ in hetzelfde arrondissement woont als werkt, draagt het College van procureurs-generaal de verantwoordelijkheid over het treffen van de maatregelen over aan een andere HOvJ. Het College van procureurs-generaal wijst deze HOvJ aan als waarnemer voor de behandeling van de dreiging. Verder wordt de reguliere procedure gevolgd waarbij, evenals bij een burgemeester of politiechef, de CBB van de NCTV een afweging maakt ten aanzien van de volledigheid en proportionaliteit van de maatregelen. Het College van procureurs-generaal wordt altijd geïnformeerd over de dreiging en de eventuele maatregelen die worden getroffen voor personen die werkzaam zijn bij het OM[8].

[7] Tweede Kamer, vergaderjaar 2014-2015. Brief versterking veiligheidsketen 27 februari 2015, referentie 3807309

[8] De verdere procedure wordt beschreven in de 'Aanwijzing beveiliging van personen, objecten en diensten' van het OM.

## 4.5 Bijzondere situaties en het raakvlak tussen het decentraal- en het rijksdomein

Het rijks- en decentrale domein zijn nauw met elkaar verbonden en de taken en bevoegdheden in de domeinen kunnen niet los van elkaar worden uitgeoefend. Bij advies, coördinatie of overdracht van het ene naar het andere domein is het van belang om afstemming te zoeken en elkaar te informeren.

De CBB speelt een signalerende en adviserende rol ten aanzien van het decentraal domein. De CBB kan zowel gevraagd als ongevraagd advies uitbrengen en het decentraal domein bij beveiligingsvraagstukken ondersteunen. Alvorens de CBB ongevraagd advies wil uitbrengen treedt de CBB daartoe altijd in contact met het bevoegd gezag in het decentraal domein.

De maatregelen ten aanzien van de beveiliging personen dienen in balans te zijn met de maatregelen die worden getroffen bij de objecten (woonhuis, werkplek) waar de betreffende persoon zich regelmatig bevindt. In de omgeving van personen uit het rijksdomein bevinden zich familieleden, vrienden, collega's etc. die niet tot het rijksdomein behoren. De verantwoordelijkheid voor de veiligheid van deze personen is een decentrale aangelegenheid.

Het komt veelvuldig voor dat een persoon, na een periode tot het rijksdomein te hebben behoord, overgeheveld wordt naar het decentrale domein. Bijvoorbeeld omdat de betreffende persoon van functie wisselt. Maatregelen eindigen vaak niet van de een op andere dag, maar vragen een periode van monitoring en afbouw. Deze overdracht verloopt altijd in nauwe afstemming met de persoon zelf, het decentrale gezag en de lokale politie eenheid. De afspraken over overheveling worden altijd schriftelijk bevestigd aan het lokaal bevoegd gezag.

Personen kunnen (tijdelijk) worden toegevoegd aan het rijksdomein (zie paragraaf 5.1). Indien de NCTV dit namens de minister van Veiligheid en Justitie beslist, zal altijd afstemming worden gezocht met het betreffende parket van het OM waar persoon woonachtig is. De overheveling wordt per brief bevestigd. Hierin staat onder andere de termijn benoemd waarvoor de (tijdelijke) toevoeging geldt.

# 5 Uitgelicht: Rijksdomein

In aansluiting op het decentrale stelsel dat in het vorige hoofdstuk is besproken, heeft de rijksoverheid een bijzondere verantwoordelijkheid voor een beperkte groep personen, objecten of diensten vanwege het nationale belang dat met hun veiligheid en hun ongestoord functioneren is gemoeid, het zogenoemde rijksdomein. In dit hoofdstuk komen de reikwijdte, de taken, bevoegdheden en de werkwijze van het rijksdomein aan de orde. Ook wordt aandacht besteed aan bewaken en beveiligen in het buitenland en, net als in het hoofdstuk over het decentrale domein, aan de raakvlakken tussen het rijksdomein en het decentrale domein.

## 5.1 Reikwijdte van het rijksdomein en limitatieve lijst

De personen, objecten en diensten waarvoor de rijksoverheid een bijzondere verantwoordelijkheid heeft en besluit op basis van dreiging en risico over beveiligingsmaatregelen, staan op een zogenoemde limitatieve lijst. Het limitatieve van de lijst betekent dat alle personen, objecten en diensten die niet op de lijst staan per definitie vallen onder het decentrale domein. Op de limitatieve lijst staan:

- Personen ten aanzien van wie en objecten ten aanzien waarvan door de aard en/of herkomst van de dreiging en de functie van de persoon of het object in beginsel de kans aanwezig is dat de nationale of internationale democratische rechtsorde wordt geschaad en/of de veiligheid van de Staat in het geding is;
- Bepaalde buitenlandse personen, objecten en internationale instellingen in Nederland;
- Enkele functionarissen in dienst van de rijksoverheid of werkzaam in de (straf)rechtspleging.

De limitatieve lijst is onderverdeeld in twee categorieën. Categorie I betreft de personen, objecten en diensten waarvoor de rijksoverheid als eerstverantwoordelijke standaard beveiligingsmaatregelen treft, dus ook in de gevallen waarin geen sprake is van dreiging en risico. Categorie II betreft de personen, objecten en diensten waarvoor de rijksoverheid als eerstverantwoordelijke beveiligingsmaatregelen treft op basis van dreiging en risico.

Tevens is er de mogelijkheid voor de rijksoverheid om (categorieën van) personen en objecten (tijdelijk) aan haar domein toe te voegen indien wordt voldaan aan één van de navolgende criteria:

- Er is sprake van een persoon die op andere wijze een bijzondere democratische plicht of functie heeft die hij ongestoord moet kunnen uitvoeren of vervullen;
- Er is sprake van een situatie waarin een ongewenste gebeurtenis disproportionele schade toe zou brengen aan het vertrouwen in de continuïteit en integriteit van de openbare sector;
- Een restcategorie waarbij de onderstaande voorwaarden in ogenschouw worden genomen:
  - Er is sprake van een ernstige en serieuze dreiging;
  - De bedreiging hangt samen met publieke uitingen of optreden;
  - De persoon heeft én landelijke bekendheid én beweegt zich (regelmatig) tussen verschillende 'politie eenheden (gebied waarin een regionale eenheid de politietaak uitvoert);
  - De persoon heeft geen werkgever die kan zorgdragen voor een adequate beveiliging.

Het lokale bevoegd gezag kan aan de CBB voorstellen een bedreigde persoon voor te dragen voor (tijdelijke) opname op de limitatieve lijst. De CBB kan ook op eigen initiatief bedreigde personen voordragen. De NCTV beslist op voorstel van de CBB namens de minister van Veiligheid en Justitie of iemand (tijdelijk) wordt geplaatst op de limitatieve lijst.
Gelet op het afbreukrisico van het bekend worden van de limitatieve lijst bij onbevoegden is deze gerubriceerd als "departementaal vertrouwelijk". De limitatieve lijst is als bijlage opgenomen in deze circulaire als bijlage 4.

## 5.2 Rijksdomein: taken en bevoegdheden in het kader van bewaken en beveiligen

De NCTV is onder verantwoordelijkheid van de minister van Veiligheid en Justitie o.a. belast met het opstellen, onderhouden en uitvoeren van het stelsel van bewaken en beveiligen[9]. De minister van Veiligheid en Justitie heeft zijn verantwoordelijkheden binnen het stelsel, die tot uitdrukking zijn gebracht in de Politiewet, gemandateerd aan de NCTV die deze op zijn beurt heeft gemandateerd aan de directeur van de Directie Bewaking, Beveiliging en Burgerluchtvaart (DB3) – tevens de CBB.

De CBB besluit namens de minister Veiligheid en Justitie tot het nemen van bewakings- en beveiligingsmaatregelen voor personen, objecten en diensten in het rijksdomein. De CBB heeft een spilfunctie ten aanzien van het evalueren van binnengekomen informatie in verband met het verstrekken van opdrachten en adviezen van bewaking en beveiliging, en de uitvoering daarvan ten aanzien van het rijksdomein.

De CBB bekijkt in hoeverre het nodig is om ten aanzien van de veiligheid van personen, objecten en diensten die staan vermeld op de limitatieve lijst maatregelen te treffen. De uitvoering van de persoonsbeveiligingsmaatregelen wordt in het rijksdomein gedaan door de DBB en de Brigade Speciale Beveiligingsopdrachten(BSB) van de KMar. De uitvoering van beveiligingsmaatregelen bij objecten en diensten behorende tot het rijksdomein wordt gedaan door politie en KMar. De CBB verzekert zich ervan dat geadviseerde maatregelen op gewenst niveau worden uitgevoerd. Daarnaast adviseert de CBB het decentrale domein gevraagd en ongevraagd over beleid en uitvoering.

De functionarissen werkzaam bij DB3 zijn belast met het verzamelen, evalueren en beoordelen van de verkregen informatie. Zij toetsen de (geanalyseerde) informatie op volledigheid en juistheid, vergelijken de onderlinge samenhang en vertalen dit naar een adequaat niveau van weerstand. Tevens heeft DB3 tot taak ervoor zorg te dragen dat de uitwisseling van relevante informatie - die bij de diensten, bij de politie en bij het OM aanwezig is - tot stand komt en optimaal verloopt.

De CBB kan indien nodig de opsporings-, inlichtingen- en veiligheidsdiensten verzoeken medewerking te verlenen aan het verstrekken van informatie. De verstrekking van informatie door de politie aan de CBB is in artikel 4:4 van het Besluit politiegegevens geformaliseerd.

### 5.2.1 *Persoonsbeveiliging*

De beveiliging van personen die vallen in het rijksdomein geschiedt onder directe verantwoordelijkheid van de minister van Veiligheid en Justitie. Deze verantwoordelijkheid van de minister van Veiligheid en Justitie wordt tot uitdrukking gebracht in zijn aanwijzingsbevoegdheid jegens de chef van de Landelijke Eenheid van de politie (artikel 43, lid 2 van de Politiewet 2012) met betrekking tot het waken voor de veiligheid van de leden van het Koninklijk Huis en andere door de minister van Veiligheid en Justitie aangewezen personen (limitatieve lijst).

Op het terrein van de persoonsbeveiliging heeft de KMar een zelfstandige taak uit hoofde van haar militaire politietaak, bedoeld in artikel 4, eerste lid, onder b van de Politiewet 2012. De beveiliging van personen, behorend tot Nederlandse en andere strijdkrachten en internationale militaire hoofdkwartieren, die vallen in het rijksdomein en als zodanig door de minister van Veiligheid en Justitie zijn aangewezen, wordt uitgevoerd door de BSB onder rechtstreekse verantwoordelijkheid van de minister van Veiligheid en Justitie. Overigens kan de beveiligingstaak van de BSB zich krachtens artikel 4, tweede lid van de Politiewet 2012, ook uitstrekken tot de echtgenoten en kinderen van de personen die behoren tot de andere strijdkrachten of internationale militaire hoofdkwartieren. De BSB kan in –bijzondere gevallen- in bijstand aan de Landelijke Eenheid van de politie eveneens persoonsbeveiligingsstaken uitvoeren.

Het voorgaande laat onverlet dat de minister van Defensie in voorkomende gevallen de KMar (maar ook de landmacht, luchtmacht en marine) opdracht kan geven tot beveiliging van militairen of militaire objecten die niet vallen binnen het rijksdomein.

[9] Organisatieregeling Ministerie van Veiligheid en Justitie 2011.

### 5.2.2 *Bewaking en beveiliging van objecten en diensten in het rijksdomein*

De uitvoering van bewakings- en beveiligingsmaatregelen van objecten en diensten in het rijksdomein geschiedt onder gezag van de burgemeester, voor zover het betreft de handhaving van de openbare orde, of de HOvJ, voor zover het betreft de strafrechtelijke handhaving van de rechtsorde. De NCTV stelt het dreigingsniveau vast.

De beveiliging van de burgerluchtvaart, de bewaking en beveiliging van de Koninklijke paleizen en woonhuizen, de bewaking en beveiliging van de ambtswoning van de minister-president en het verrichten van beveiligingswerkzaamheden ten behoeve van De Nederlandsche Bank (DNB) geschiedt door de KMar onder rechtstreekse verantwoordelijkheid van de minister van Veiligheid en Justitie.

## 5.3 Rijksdomein: werkwijze

Bij DB3 komt relevante informatie aangaande dreiging en risico, voor zover dit het rijksdomein raakt, ongevraagd en gevraagd samen. De informatie is niet uitsluitend opsporings-, inlichtingen- en veiligheidsdiensten maar tevens kan informatie van Dienst Kabinet en Protocol (DKP), Directie Veiligheid, Crisisbeheersing en Integriteit (VCI) van het ministerie Buitenlandse Zaken, BVA's en open bronnen worden betrokken. DB3 gaat na in hoeverre de persoon, object of dienst waarop de informatie betrekking heeft binnen het domein van de rijksoverheid valt. Zo niet, dan wordt de informatie ter beschikking gesteld aan het betreffende lokale gezag, eventueel vergezeld van een (on)gevraagd advies.

### 5.3.1 *Afstemmingsoverleg Bewaken en Beveiligen (ABB) en Uitvoeringsoverleg (UO)*

Het proces tot het komen van adviezen c.q. besluiten ten aanzien van operationele aangelegenheden vindt plaats onder de verantwoordelijkheid van de NCTV. De adviezen en besluiten worden voorbereid door de CBB. Deze wordt hierin geadviseerd door het ABB en het UO. De cyclus van het ABB en het UO vindt in de regel elke twee weken plaats.

Tijdens het ABB worden de verkregen dreigingsinformatie en -analyses besproken. Aan dit overleg nemen vertegenwoordigers van de opsporings-, inlichtingen- en veiligheidsdiensten deel onder voorzitterschap van DB3. Dit overleg is bedoeld om de verschillende bronnen te combineren en voor de opsporings-, inlichtingen- en veiligheidsdiensten om nadere uitleg en/of differentiatie aan te brengen in de informatie.

Ter verkrijging van eenduidigheid en afstemming tussen de verschillende partners vindt het UO plaats. Het UO wordt voorgezeten door DB3 en bestaat uit de vertegenwoordigers van de DBB en de Dienst Landelijke Operationele Samenwerking (DLOS) van de Landelijke Eenheid van de politie, de BSB, het OM, de KMar en de regionale eenheden Amsterdam, Den Haag, Rotterdam en Midden-Nederland. Ook andere regionale eenheden kunnen in voorkomend geval deelnemen aan het UO. Het UO beziet op welke wijze uitvoering wenselijk is en kijkt mede naar de haalbaarheid en de effectiviteit. Naast het adviseren over de uitvoering van de maatregelen op basis van het integrale inzetconcept verzekert de CBB zich ervan dat de geadviseerde maatregelen op gewenst niveau worden uitgevoerd.

Tot slot zullen, in sommige gevallen diplomatieke of militaire belangen een rol spelen bij het adviseren van maatregelen. De CBB kan zich dan bilateraal laten adviseren door de directeur DKP of Directie VCI van het ministerie van Buitenlandse Zaken, respectievelijk de directeur Juridische Zaken van het ministerie van Defensie.

### 5.3.2 *Buitenlandse bezoeken aan NL*

Wanneer buitenlandse hoogwaardigheidsbekleders in een formele hoedanigheid op bezoek komen in Nederland is vaak het ministerie van Buitenlandse Zaken hiervan op de hoogte. Deze meldt de bezoeken aan bij DB3, met het verzoek om zich te buigen over de beveiligingsmaatregelen. Indien dit bezoek iemand uit het rijksdomein betreft, handelt DB3 dit bezoek zelf af en legt DB3 contact met het betreffende lokaal bevoegd gezag.

Niet alle bezoeken zijn bekend bij het ministerie van Buitenlandse Zaken. Een buitenlandse gast kan bijvoorbeeld op uitnodiging van een private instantie in Nederland zijn of voor een privé bezoek. Wanneer het bezoek via een andere weg wordt aangemeld bij DB3, handelt DB3 dit bezoek zelf af als het een persoon uit het rijksdomein betreft. DB3 legt dan contact met zowel het betreffende lokaal bevoegde gezag als DKP van het ministerie van Buitenlandse Zaken om hen op de hoogte te stellen van dit bezoek.

Indien een delegatie Nederland bezoekt, waarvan gewapende beveiligingsfunctionarissen deel uitmaken, dient hiervan melding te worden gemaakt door de betrokken ambassade aan DKP van het ministerie van Buitenlandse Zaken. DKP zal vervolgens de melding van het bezoek aan de CBB doorgeleiden die de aanvraag toetst en een bewapeningsvoorschrift kan afgeven.

## 5.4 Bewaken en beveiligen in het buitenland

Bewaken en beveiligen is een nationale aangelegenheid. De Nederlandse overheid kan geen verantwoordelijkheid nemen voor beveiliging van personen in het buitenland. De Nederlandse overheid zorgt wel in nauwe samenwerking met buitenlandse autoriteiten voor beveiligingsmaatregelen wanneer het functionarissen betreft die een officiële functie voor de Nederlandse overheid vervullen en die vanwege het nationale belang dat is gediend met hun veiligheid en ongestoord functioneren is gemoeid permanent op de limitatieve lijst staan[10].

Bij de uitvoering van de persoonsbeveiligingstaak in het buitenland wordt door de NCTV een opdracht verstrekt aan de DBB of BSB.

Indien naar het oordeel van de NCTV[11] de beveiliging noodzakelijk is van personen die niet behoren tot de personen waarvoor de KMar krachtens artikel 4, eerste lid onder b, van de Politiewet 2012 de politietaak uitoefent, maar de inzet van de KMar wel gerechtvaardigd is, wordt door de minister van Defensie bijstand op grond van artikel 57 van de Politiewet 2012 verleend. Deze bijstand wordt uitgevoerd door de BSB in opdracht van de NCTV met inachtneming van de afspraken daarover tussen de betrokken ministers.[12]

Wanneer personen die tijdelijk opgenomen zijn op de limitatieve lijst geen officiële functie vervullen voor de overheid, worden er door de Nederlandse overheid in principe geen beveiligingsmaatregelen getroffen in het buitenland. In gevallen waarbij de betreffende persoon incidenteel en kortstondig naar het buitenland vertrekt voor een publiek optreden, kan het treffen van beveiligingsmaatregelen in samenwerking met buitenlandse autoriteiten en VCI van het ministerie van Buitenlandse Zaken in overweging worden genomen[13].

## 5.5 Bijzondere situaties en het raakvlak tussen rijks- en decentraal domein

Het rijks- en het decentrale domein zijn nauw met elkaar verbonden. Bij advies, coördinatie of overdracht van het ene naar het andere domein is het van belang om afstemming te zoeken en elkaar te informeren.

Indien een te beveiligen persoon op de limitatieve lijst vanwege dreiging en risico beveiligingsmaatregelen behoeft, betreft dit een palet aan maatregelen die beide domeinen raken. De CBB zal namens de minister van Veiligheid en Justitie opdracht verstrekken aan de DBB tot het uitvoeren van persoonsbeveiliging. Met betrekking tot de woning of werkplek van de te beveiligen persoon op de limitatieve lijst blijft het lokaal bevoegd gezag verantwoordelijk, de CBB geeft op basis van het dreigingsbeeld een advies aan het betreffende lokaal bevoegd gezag voor het treffen van beveiligingsmaatregelen. Hieruit volgt dat ook voor het rijksdomein het lokaal bevoegd gezag verantwoordelijk is voor de uitvoering van beveiligingsmaatregelen rondom woning en werkplek.

Indien een persoon op de limitatieve lijst wordt beveiligd betekent dit in veel gevallen dat ook het gezin van deze persoon te maken krijgt met beveiligingsmaatregelen. De verantwoordelijkheid voor de veiligheid van de gezinsleden van deze persoon is een decentrale aangelegenheid. Het is daarom van belang dat in deze gevallen het rijksdomein in contact staat en afstemming zoekt met het decentrale domein om de beveiliging en relevante dreigingsinformatie uit te wisselen.

Het kan nodig zijn om rondom een te beveiligen persoon die behoort tot het rijksdomein beveiligingsmaatregelen te treffen anders dan de plaats waar deze persoon woont of werkt. Het betreffende lokaal bevoegd gezag van de gemeente die wordt bezocht dient geïnformeerd te zijn om zo nodig beveiligingsmaatregelen te treffen in de openbare ruimte, al dan niet op advies van de CBB.

Over het overdragen van verantwoordelijkheden van het rijksdomein naar het decentrale domein en vice versa dient goede afstemming te bestaan. Dit is bijvoorbeeld het geval indien een functie op de limitatieve lijst niet langer door deze persoon wordt bekleed. De afspraken over overheveling worden altijd schriftelijk bevestigd aan het lokaal bevoegd gezag.

[10] Tweede Kamer, vergaderjaar 2007-2008, 28 974, nr. 6. Brief van de Minister van Justitie aan de Tweede Kamer d.d. 4 oktober 2007.

[11] Dit oordeel is gebaseerd op de volgende indicatoren: *hoogste geweldspectrum, uitzendgebied/oorlogsgebied of (burger)oorlogsomstandigheden, ontbreken van een staande/functionerende overheid, non-permissive environment (er heerst vijandigheid ten opzichte van Nederland in het te bezoeken gebied), hoge dreiging explosieven en/of buitensporig vuurwapengeweld, aanwezigheid BSB ter plaatse (bijv. BSB is aanwezig op ambassade).*

[12] Convenant van 17 mei 2013 tussen de ministers van Veiligheid en Justitie, en Defensie.

[13] Tweede Kamer, vergaderjaar 2007-2008, Handelingen 10-666, d.d. 9 oktober 2007.

# 6 Overige aan bewaken en beveiligen gerelateerde onderwerpen

In dit hoofdstuk wordt toegelicht de werkwijze nationale evenementen, de rol van de bedreigde persoon met betrekking tot zijn beveiligingsmaatregelen, en de communicatie over bedreigingen en maatregelen richting de bedreigde persoon.

## 6.1 Nationale evenementen

De NCTV, de politie, en de inlichtingen- en veiligheidsdiensten hebben gezamenlijk een 'werkwijze nationale evenementen' ontwikkeld. Een nationaal evenement wordt aangewezen door de minister van Veiligheid en Justitie. Het is een evenement dat bezocht wordt door personen die vermeld staan op de limitatieve lijst én waarbij het nationaal belang centraal staat én het karakter van het evenement een specifieke of verhoogde druk op de bewaking en beveiliging geeft. De werkwijze omvat onder andere:

- Een geïntegreerd dreigingsbeeld op basis van de landelijke en lokale dreigingsinschattingen.
- Een transparante en toetsbare risicoafweging aan de hand van een landelijke lijst dreigingsscenario's.
- Een integraal bewakings- en beveiligingsplan met de maatregelen inclusief de beveiligingsringen. Dit plan bevat het basispakket aan maatregelen en de eventuele extra gewenste maatregelen die uit de uitgewerkte scenario's voortvloeien.

Beveiligingsmaatregelen worden genomen onder bevoegdheid van het lokaal bevoegd gezag. Met de burgemeester en de HOvJ participeert de NCTV (CBB) in het gezagsoverleg met betrekking tot het nationale evenement over de te nemen maatregelen met betrekking tot bewaken en beveiligen. De NCTV is de namens de minister van Veiligheid en Justitie gezag over de beveiligingsmaatregelen met betrekking tot de aanwezige personen van de limitatieve lijst en daarmee opdrachtgever van de DBB die uitvoering geeft aan de persoonsbeveiliging.
De NCTV geeft bij nationale evenementen altijd advies over de samenhang en de afstemming tussen de betrokken partijen in het bewaking- en beveiligingsproces, ongeacht het dreigingsniveau en maakt deel uit van de daartoe relevante overleggen ter voorbereiding van deze evenementen.

## 6.2 Rol van de bedreigde persoon (medewerking, grenzen aan inspraak)

In het algemeen is het niet mogelijk bedreigde personen, organisaties, bedrijven of instellingen te dwingen mee te werken aan hun eigen beveiliging. De medewerking van bedreigde personen, organisaties, bedrijven of instellingen bij de uitvoering van maatregelen voor persoons- of objectbeveiliging is essentieel. Dit begint bij de mate van invulling van de eigen- en/of werkgeversverantwoordelijkheid. Indien de persoon, organisatie, bedrijf of instelling aantoonbaar niet instaat blijkt te zijn de noodzakelijke maatregelen te treffen of hierin te voorzien vallen deze onder de politietaak. Het is noodzakelijk voor de beveiliging van een bedreigde persoon dat deze de benodigde informatie verstrekt met betrekking tot zijn eigen veiligheidssituatie. In de praktijk werken personen niet altijd mee aan hun eigen beveiliging of geven zij, de organisatie, het bedrijf of de organisatie onvoldoende invulling aan hun eigen verantwoordelijkheid. Het niet invullen van de eigen verantwoordelijkheid, de weigering of beperkte medewerking leidt ertoe dat de overheid niet of minder goed haar (aanvullende) verantwoordelijkheid kan nemen.

### *6.2.1 Grenzen aan inspraak bedreigde persoon*

De essentie van persoons- en objectbeveiliging is dat er bepaalde beveiligingsmaatregelen moeten worden genomen omdat sprake is van dreiging en risico. Uitgangspunt daarbij is dat een beveiligd persoon - binnen de beperkingen van de beveiliging - zijn privé- en maatschappelijke activiteiten moet kunnen voortzetten en een zo normaal mogelijk leven moet kunnen leiden. Beveiligingsdeskundigen beoordelen welke beveiligingsmaatregelen noodzakelijk zijn, dit is uitdrukkelijk geen onderwerp van onderhandeling. Indien mogelijk wordt de keuze van het beveiligingspakket van te voren besproken met de bedreigde persoon. Vanzelfsprekend zijn de persoonlijke wensen en veiligheidseisen niet altijd verenigbaar. Bij een hoog dreigingsniveau is een beperking van de privacy niet altijd te voorkomen.

### 6.2.2 *Deskundige begeleiding*

Persoonsbeveiliging kan op de betrokkene en zijn directe omgeving een zware druk leggen. Bij hoge dreiging zijn permanent persoonsbeveiligers aanwezig en zijn woonvoorziening en vervoer aangepast. Bovendien ervaart de te beveiligen persoon mogelijk de psychische druk van de dreiging. Bij personen in het rijksdomein kan bij een dergelijke hoge dreiging een gesprek plaats vinden tussen de te beveiligen persoon en een deskundige. In één of meer adviesgesprekken kan nader worden ingegaan op de persoonlijke effecten en praktische aspecten van beveiliging en de consequenties daarvan voor de bedreigde persoon en zijn omgeving. In voorkomende gevallen kan ook het decentrale domein gebruik maken van deze faciliteiten van de CBB.

## 6.3 Communicatie over bedreigingen en maatregelen

Met betrekking tot persoonsbeveiliging is het begrijpelijk dat belang wordt gehecht aan het informeren van bedreigde personen over de aard van de dreiging en de getroffen maatregelen. Het te allen tijde informeren van personen over iedere bedreiging die is aangekondigd of verschenen via berichtgeving in de media en op internet is niet mogelijk en/of wenselijk. Als niet is vastgesteld of de bedreiging reëel is en hoe deze gewaardeerd moet worden, veroorzaakt deze informatie slechts onduidelijkheid.

Bedreigde personen worden periodiek geïnformeerd over het verloop van de dreiging en de getroffen maatregelen. Belangen rond inlichtingen, opsporing of vervolging kunnen aanleiding zijn om de bedreigde persoon niet tot in detail te informeren.

Het wordt onder de aandacht gebracht van de beveiligde persoon dat het wenselijk is dat er tegen derden geen uitlatingen worden gedaan over de genomen maatregelen. Deze terughoudendheid is zowel voor de veiligheid van de persoon als van de beveiligers. Indien de beveiligde persoon in het openbaar toch uitspraken doet over genomen beveiligingsmaatregelen, kan door de CBB of het lokaal bevoegd gezag worden besloten terughoudender te zijn met het verstrekken van informatie aan de te beveiligen persoon.

# Bijlage 1 - Lijst van afkortingen

| | |
|---|---|
| ABB | Afstemmingsoverleg Bewaken Beveiligen |
| AIVD | Algemene inlichtingen en veiligheidsdienst |
| BB&C | (Beleidsmedewerker) Bewaken, Beveiligen en Crisisbeheersing van de parketten bij het Openbaar Ministerie |
| BSB | Brigade Speciale Beveiligingsopdrachten van de Koninklijke Marechaussee |
| BVA | Beveiligingsambtenaar |
| CBB | Coördinator Bewaken en Beveiligen van de Nationaal Coördinator Terrorismebestrijding en Veiligheid |
| CCB | (Portefeuillehouder) Conflict en Crisisbeheersing van de regionale politie eenheid |
| DA | Dreigingsanalyse |
| DB3 | Directie Bewaking, Beveiliging, Burgerluchtvaart van de Nationaal Coördinator Terrorismebestrijding en Veiligheid |
| DBB | Dienst Bewaken en Beveiligen van de Landelijke Eenheid van de Nationale Politie |
| DI | Dreigingsinschatting |
| DKP | Directie Kabinet en Protocol van het ministerie van Buitenlandse Zaken |
| DLIO | Dienst Landelijke Informatie Organisatie van de Landelijke Eenheid van de Nationale Politie |
| DLOS | Dienst Landelijke Operationele Samenwerking van de Landelijke Eenheid van de Nationale Politie |
| DNB | De Nederlandsche Bank |
| DRIO | Dienst Regionale Informatie Organisatie van de Regionale Eenheid van de Nationale Politie |
| DTN | Dreigingsbeeld Terrorisme Nederland |
| HOvJ | Hoofdofficier van Justitie van het Openbaar Ministerie |
| IRD | Informatierapport dreiging |
| KMar | Koninklijke Marechaussee |
| MIVD | Militaire inlichtingen en veiligheidsdienst |
| NCTV | Nationaal Coördinator Terrorismebestrijding en Veiligheid |
| OM | Openbaar Ministerie |
| RA | Risicoanalyse |
| RCCB | (Afdeling) Regionale Conflict en Crisisbeheersing van de Regionale Eenheid van de Nationale Politie |
| UO | Uitvoeringsoverleg |
| VCI | Directie Veiligheid, Crisisbeheersing en Integriteit van het ministerie van Buitenlandse Zaken |
| WIV 2002 | Wet op de inlichtingen en veiligheidsdiensten 2002 |

# Bijlage 2 - Uitgebreid overzicht van de direct en indirect relevante wet- en regelgeving

Deze bijlage geeft een overzicht van de relevante wettelijke bepalingen met betrekking tot de bewaking en beveiliging van personen, objecten en diensten.

Politiewet 2012: artikelen 1, 3, 4, 11, 12, 14, 15, 16, 17, 42, 43, en 56-64.
De taak om te bewaken en te beveiligen maakt onderdeel uit van de politietaak om zorg te dragen voor de daadwerkelijke handhaving van de rechtsorde (artikel 3 van de Politiewet 2012). De daadwerkelijke handhaving valt uiteen in openbare orde handhaving en strafrechtelijke handhaving. Artikel 1, lid 2 van de Politiewet 2012 stelt dat "in deze wet en de daarop berustende bepalingen wordt onder strafrechtelijke handhaving van de rechtsorde mede verstaan: het waken voor de veiligheid van personen".

Gemeentewet: artikel 172.
Op basis van de Gemeentewet, artikel 172, is de burgemeester belast met de handhaving van de openbare orde. Hij bedient zich daarbij van de onder zijn gezag staande politie.

Wet en Besluit politiegegevens
De Wet politiegegevens regelt de verwerking en verspreiding van politiegegevens met het oog op de uitvoering van de politietaak. Artikel 4:4 van het Besluit politiegegevens regelt dat politiegegevens desgevraagd verstrekt worden aan de ministers van Veiligheid en Justitie en Binnenlandse Zaken en Koninkrijksrelaties, ten behoeve van het verrichten van dreigings- en risico-evaluaties en het vaststellen van bewakings- en beveiligingsopdrachten en adviezen met het oog op het bewaken en beveiligen van personen, objecten en diensten.

Wet op de inlichtingen- en veiligheidsdiensten 2002: artikelen 6, tweede lid, sub e, 6a, 7, tweede lid, sub f, 7a, 13, 36 en 62.
Op basis van artikel 6, lid 2, sub e van de Wet op de inlichtingen- en veiligheidsdiensten kan de AIVD op verzoek van de ministers van BZK en Veiligheid en Justitie gezamenlijk dreigings- en risicoanalyses vervaardigen ten behoeve van de beveiliging van personen in het rijksdomein en de bewaking en beveiliging van objecten en diensten in het rijksdomein. Bij dreigings- en risicoanalyses wordt behalve naar de concrete dreiging ook naar de potentiële dreiging gekeken.
De MIVD kan op basis van artikel 7, lid 2, sub f ook dreigingsanalyses opstellen. Het opstellen van risicoanalyses is een taak voorbehouden aan de AIVD.

Ambtsinstructie voor de politie, de Koninklijke Marechaussee en de buitengewoon opsporingsambtenaar: artikel 8.
In de ambtsinstructie is de geweldstoepassing voor de politie, de Koninklijke Marechaussee en de buitengewoon opsporingsambtenaar nader geregeld.

Wet op de rechterlijke organisatie: artikel 127.
Op grond van artikel 127 van de Wet op de rechterlijke organisatie kan de Minister van Veiligheid en Justitie algemene en bijzondere aanwijzingen geven betreffende de uitoefening van de taken en bevoegdheden van het Openbaar Ministerie.

Regeling beheer politie: artikelen 11d, 15c en 17d.
Op basis van de regeling beheer politie dienen regionale eenheden zelfstandig of samen te beschikken over onderdelen die werkzaamheden verrichten op het terrein van bewaken en beveiligen van personen, objecten en diensten (zoals mobiele eenheden en arrestatie- en ondersteuningseenheden).

Wetboek van Strafvordering: artikelen 226g t/m 226k.
Zoals vastgesteld bij de Wet tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering met betrekking tot verklaringen van getuigen die in ruil voor een toezegging van het Openbaar Ministerie zijn afgelegd (toezeggingen aan getuigen in strafzaken) Kamerstukken 26 294 en 28017, Staatsblad 2005, 254 en 255;

Convenant van 17 mei 2013 tussen de ministers van Veiligheid en Justitie, en Defensie:
Volledige naam; 'Convenant tussen de minister van Veiligheid en Justitie en de minister van Defensie inzake de inzet van de Koninklijke marechaussee ten behoeve van persoonsbeveiligingstaken in het buitenland'.

# Bijlage 3 - Tabellen Ernst en Waarschijnlijkheid

## Tabel 'Ernst'

| Classificatie | (Potentieel) Effect | | |
|---|---|---|---|
| | Personen | Objecten | Samenleving |
| 5 Zeer ernstig | Groot aantal dodelijke slachtoffers | Uitval/uitschakeling vitale objecten | Maatschappelijke ontwrichting |
| 4 Ernstig | Vrijheidsontneming bedreigde en/of één of enkele dodelijke of zwaargewonde slachtoffers | Grote schade aan vitale objecten en/of uitval/uitschakeling niet-vitale objecten | Samenleving geschokt en verstoring van de openbare orde |
| 3 Gemiddeld | Fysiek letsel bedreigde en/of één of enkele lichtgewonde slachtoffers | Grote schade aan niet-vitale objecten | Grootschalige verstoring van de openbare orde |
| 2 Matig | Verstoring en/of intimidatie bedreigde of fysieke integriteit bedreigde geschonden | Geringe schade aan vitale of niet-vitale objecten | Kleinschalige verstoring van de openbare orde en/of bezetting |
| 1 Niet ernstig | Geen effect op personen | Geen schade aan objecten of infrastructuur | Geen effect op de samenleving |

## Tabel 'Waarschijnlijkheid'

| Classificatie | Intentie<br>**de mate waarin een dreiger voornemens is een gebeurtenis te laten plaatsvinden** | Potentie<br>**de mate waarin een dreiger de kennis en middelen heeft en in de gelegenheid is om een gebeurtenis te laten plaats vinden** | Concreetheid<br>**zijn er feiten en omstandigheden (handelingen) bekend waaruit blijkt dat een gebeurtenis gaat plaatsvinden** | |
|---|---|---|---|---|
| **5** Zeker | Sterke intentie aanwezig | Potentie aanwezig | Concrete uitvoeringshandelingen bekend | **Concrete dreiging** |
| **4** Zeer waarschijnlijk | (Sterke) Intentie aanwezig | Potentie (deels) aanwezig | Concrete voorbereidingshandelingen bekend | |
| **3** Waarschijnlijk | Intentie aanwezig | Potentie (deels) aanwezig | Geen concrete handelingen bekend | **Voorstelbare dreiging** |
| **2** Mogelijk | Latente intentie aanwezig | Potentie (deels) aanwezig | Geen concrete handelingen bekend | |
| **1** Onwaarschijnlijk | Geen intentie aanwezig | Potentie niet aanwezig | Geen concrete handelingen bekend | |

# Bijlage 4 - De Limitatieve Lijst

De limitatieve lijst is gerubriceerd en zodoende niet bij de openbare versie van de circulaire gevoegd. Voor de relevante partners is de limitatieve lijst op te vragen bij de NCTV.

## Colofon

**Uitgave**
Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)
Postbus 20301
2500 EH Den Haag
Turfmarkt 147
2511 DP Den Haag
070 751 5050

**Meer informatie**
www.nctv.nl
info@nctv.minvenj.nl
@nctv_nl

Augustus 2015