Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2002–2003

28 974 Nieuw stelsel bewaken en beveiligen

Nr. 2

NOTA

Samenvatting

Bij brief van 17 december 2002 bent u in kennis gesteld van het standpunt van het kabinet naar aanleiding van de bevindingen van de Commissie feitenonderzoek inzake de veiligheid en beveiliging van de heer W. S. P. Fortuyn (Kamerstukken II, 2002–2003, 28 374, nr. 13). In dit kader informeren wij u thans nader over de voornemens met betrekking tot een nieuw stelsel van bewaken en beveiligen.

Uitgangspunt van het nieuwe stelsel is dat de verantwoordelijkheid voor de eigen veiligheid primair ligt bij de burger zelf, de organisatie waartoe deze behoort (zoals het bedrijf waar hij werkzaam is) en het decentrale gezag. In aanvulling daarop is er sprake van een bijzondere verantwoordelijkheid van de Rijksoverheid voor een bepaalde groep personen, objecten en diensten. Wanneer een persoon, object of dienst niet op de limitatieve lijst van het Rijksdomein voorkomt dan valt deze dus in principe binnen de actieradius van het decentrale domein. Het decentrale niveau beschikt daartoe over dezelfde maatregelen als die getroffen kunnen worden ten behoeve van het Rijksdomein.

In navolging van de Politiewet is op decentraal niveau de burgemeester het bevoegd gezag als het bij bewaken en beveiligen om de openbare orde gaat. Voor de strafrechtelijke handhaving van de rechtsorde is de officier van justitie op decentraal niveau het bevoegde gezag. Het doel waarvoor de bewakings- en beveiligingsmaatregelen ten aanzien van bepaalde personen, objecten en diensten worden getroffen, is bepalend voor de vraag bij wie het bevoegde gezag ligt. Persoonsbeveiliging wordt in de regel ingezet wanneer bij een gebeurtenis voor het leven van personen of hun fysieke integriteit of voor andere ernstige delicten valt te vrezen. De officier van justitie is dan de bevoegde autoriteit vanwege zijn taak om in concrete gevallen ernstige strafbare feiten te voorkomen of te beëindigen.

In het nieuwe stelsel zal ten eerste meer structureel, transparanter en beter gefundeerd overwogen worden ten aanzien van welke personen, objecten en diensten bewaking en beveiliging mogelijk dient te worden. Ten tweede wordt de gewenste bewaking en beveiliging van een persoon

KST68954
0203tkkst28974-2
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2003

of object niet meer hoofdzakelijk gebaseerd op dreigingsgerelateerde informatie afkomstig uit onderzoek door politie, inlichtingen- en veiligheidsdiensten, maar zullen ook potentiële dreigingen worden geïnventariseerd en geanalyseerd. Met betrekking tot de zogenoemde potentiële dreigingen is wel additionele wetgeving nodig.
Verder zal er een glijdende schaal van maatregelen en dreigingsniveaus in het nieuwe systeem worden geïntroduceerd, waardoor meer flexibiliteit en maatwerk mogelijk wordt. Waar nodig zal hiertoe capaciteitsuitbreiding plaats hebben. Voorts zal de informatiehuishouding c.q. het informatieproces sterk worden verbeterd. Ten slotte wordt in het nieuwe stelsel bewaken en beveiligen niet meer alleen gesproken van «personen en objecten» waarvoor extra veiligheidsmaatregelen worden getroffen, maar ook van «diensten». Daarmee is het eenvoudiger om extra veiligheidsmaatregelen ter bescherming van bepaalde diensten en sectoren (zoals geld- en andere transporten) te duiden.

Inleiding

Naar aanleiding van de aanslag op de heer W. S. P. Fortuyn op 6 mei 2002 werd door ons op 14 mei 2002 een onafhankelijke commissie ingesteld die de opdracht kreeg onderzoek te doen naar de gang van zaken met betrekking tot de veiligheidssituatie van Fortuyn voorafgaande aan de aanslag en naar de verantwoordelijkheid van overheidsinstanties voor zijn veiligheid en beveiliging. Deze Commissie feitenonderzoek inzake de veiligheid en beveiliging Pim Fortuyn, onder voorzitterschap van de heer mr. H. F. van den Haak, beschreef en analyseerde bij haar onderzoek tevens de besluitvorming rond de beveiliging van de heer Fortuyn in het kader van het toen geldend stelsel van regels en uitgangspunten. Één van de belangrijkste aanbevelingen in het eindrapport van de commissie, dat 13 december 2002 aan ons werd aangeboden, betrof de noodzaak tot wijziging van het stelsel bewaken en beveiligen. In de eerdergenoemde kabinetsreactie van 17 december 2002 werd deze noodzaak onderschreven.

In navolging van de aanbevelingen van de commissie feitenonderzoek is per 1 januari 2003 door de regering bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) een projectdirecteur-generaal Beveiliging en Crisisbeheersing benoemd, die tevens functioneert als Nationaal Coördinator Bewaking en Beveiliging (NCBB). De NCBB is verantwoording verschuldigd aan zowel de minister van BZK als de minister van Justitie. Een voorname taak voor de nationaal coördinator is het entameren van een integraal bewakings- en beveiligingsbeleid. Voor dit doel is door hem een beschrijving gemaakt van het nieuwe stelsel bewaken en beveiligen. Daarbij zijn de aanbevelingen van de commissie feitenonderzoek alsmede de uitgangspunten van het kabinetsstandpunt richtinggevend geweest. Van de politieberaden, het Korps landelijke politiediensten (KLPD), de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en het openbaar ministerie (OM) zijn adviezen ontvangen over het concept-stelsel. Tevens heeft de NCBB in januari en maart van dit jaar uitvoerig gesproken met een aantal leden van de Commissie feitenonderzoek.

Hieronder treft u een beschrijving aan van de hoofdlijnen van het nieuwe stelsel bewaken en beveiligen, gebaseerd op de eerdergenoemde uitgangspunten.

Het stelsel kent de volgende elementen die achtereenvolgens zullen worden beschreven:
1. Domeinen en verantwoordelijkheden;
2. Nieuw stelsel risicobenadering: producten en instrument voor het decentrale en Rijksdomein;

3. Leveranciers producten en instrument;
4. Weging en toetsing;
5. Advisering en besluitvorming;
6. Uitvoering;
7. Implementatietraject nieuw samenhangend stelsel.

1 Domeinen en verantwoordelijkheden

1.1 Uitgangspunt: eigen verantwoordelijkheid en decentraal stelsel

Algemeen uitgangspunt is dat de burger zelf in eerste instantie verantwoordelijk is voor de eigen veiligheid van zowel persoon als goed. Burgers mogen daarbij rekenen op hulp van de organisaties en netwerken waartoe zij behoren. Het gemeentelijk en landelijke gevoerde (integraal) veiligheidsbeleid kan hen daarbij van dienst zijn. Bedrijven, organisaties en instellingen dienen zelf beschermende maatregelen te treffen om te voorkomen dat als gevolg van hun werkzaamheden de veiligheid van werknemers en anderen in gevaar komt. Burgers en organisaties mogen echter van de overheid verwachten dat die hen door het treffen van veiligheidsmaatregelen te hulp schiet op het moment dat de aantasting van hun veiligheid zulke gewelddadige vormen dreigt aan te nemen, dat zij daar op eigen kracht geen weerstand meer tegen kunnen bieden. In het geval er sprake is van een dergelijke bedreiging aan het adres van personen of hun organisaties, dan dient men de plaatselijke politie daarvan in kennis te stellen. Het bevoegde gezag op lokaal niveau wordt daarmee in de gelegenheid gesteld om eventueel noodzakelijk geachte veiligheidsmaatregelen te treffen en/of om een opsporingsonderzoek te starten.

1.2 Reikwijdte van het decentraal domein: alle burgers, objecten of diensten

Het decentrale deel van het stelsel voor bewaken en beveiligen betreft de normale situatie waarin het lokaal bevoegde gezag zelf besluiten neemt over extra veiligheidsmaatregelen om een dreiging in de richting van personen, objecten of diensten af te wenden. In Nederland is het waken voor de veiligheid decentraal belegd (decentraal, tenzij). In het gehele overheidsdomein is het decentraal gezag als eerste verantwoordelijk voor bewaking en beveiliging. Dat betekent dat in beginsel de veiligheidszorg voor *alle* personen, objecten of diensten onder verantwoordelijkheid van het decentraal niveau plaatsvindt. In het nieuwe stelsel heeft het lokaal gezag een glijdende schaal van veiligheidsmaatregelen ter beschikking, variërend van lichte maatregelen als extra politiesurveillance tot zware maatregelen als persoonsbeveiliging en objectbeveiliging (zie paragraaf 6.1. voor een nadere opsomming). Hierdoor is maatwerk mogelijk. Het lokaal gezag zal over afdoende instrumenten beschikken om besluiten uit te voeren.

In het nieuwe stelsel wordt niet meer alleen gesproken van «personen en objecten» waarvoor extra veiligheidsmaatregelen worden getroffen, maar ook van «diensten». Daarmee is het eenvoudiger om extra veiligheidsmaatregelen ter bescherming van bepaalde diensten en sectoren te duiden. Te denken valt aan extra veiligheidsmaatregelen ter bescherming van een bepaald transport (bijvoorbeeld luchtvaart/scheepvaart of het transport van bepaalde gevaarlijke stoffen of van geld) of ter bescherming van vitale infrastructuur zoals telecommunicatie/ICT etcetera.

1.3 Decentrale verantwoordelijkheden van het lokaal gezag nader geduid

De politie heeft tot taak in ondergeschiktheid aan het bevoegd gezag te

zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven. De politie treedt bij de handhaving van de openbare orde en de hulpverlening op onder gezag van de burgemeester. Openbare orde kan worden uitgelegd als de – naar tijd en plaats bepaalde – normale gang van zaken op voor het publiek toegankelijke plaatsen, welke gang van zaken wordt gekenmerkt door een overwegende mate van algemene vrijheid deze plaatsen overeenkomstig hun bestemming te gebruiken. De strafrechtelijke handhaving van de rechtsorde betreft in het algemeen het voorkomen, opsporen en beëindigen van strafbare feiten, alsmede het vervolgen en berechten van de daders van die feiten en de tenuitvoerlegging van de hen opgelegde straffen en maatregelen. Deze taak verricht de politie onder gezag van de officier van justitie.

De taak om te bewaken en beveiligen maakt onderdeel uit van de politietaak om zorg te dragen voor de daadwerkelijke handhaving van de rechtsorde (artikel 2 van de Politiewet 1993). Dat blijkt ook uit het Besluit beheer regionale politiekorpsen (28 maart 1994, Stb. 224), op basis waarvan regionale politiekorpsen zelfstandig of samen dienen te beschikken over eenheden (zoals mobiele eenheden en aanhoudings- en ondersteuningseenheden) die werkzaamheden verrichten op het terrein van bewaken en beveiligen van personen, objecten en transporten. Voor wat betreft persoonsbeveiliging opent het besluit de mogelijkheid dat de ministers eenheden aanwijzen, bestaande uit ambtenaren van politie van een of meer regionale korpsen, die zijn belast met het waken voor de veiligheid van de daartoe door het bevoegde gezag aangewezen personen.

In de praktijk lopen de openbare ordehandhavings- en de strafrechtelijke handhavingstaken veelal dooreen. Bij ordeverstoringen worden vaak ook strafbare feiten gepleegd, terwijl sommige strafbare feiten op hun beurt weer een verstoring van de openbare orde kunnen inhouden. Het treffen van adequate veiligheidsmaatregelen om strafbare feiten of ordeverstoringen te voorkomen maakt in ieder geval deel uit van de verantwoordelijkheid van het lokale gezag. Het is niet altijd eenvoudig om van te voren te bepalen of de preventieve inzet van veiligheidsmaatregelen om een bepaalde gebeurtenis en haar mogelijke consequenties te voorkomen plaatsvindt voor het doel van openbare ordehandhaving dan wel onder strafrechtelijke handhaving (zie ook de discussie over politie-inzet tijdens de Eurotop). De inzet van extra veiligheidsmaatregelen dient om die reden onderwerp van gesprek te zijn in de lokale gezagsdriehoek (burgemeester, officier van justitie en politiechef). Over de wijze waarop die beslissing tot stand komt en op basis van welke informatie en producten wordt in de hiernavolgende hoofdstukken nader in gegaan. De ernst van de dreiging (concreet en potentieel), en in het bijzonder het effect en de aard van de verwachte gebeurtenis dient bepalend te zijn voor de vraag bij wie het primaat ligt binnen de driehoek. Wanneer bij een gebeurtenis voor het leven van personen of hun fysieke integriteit of voor andere ernstige delicten valt te vrezen, dan zal het primaat liggen – en daarmee de beslissingsbevoegdheid – bij het openbaar ministerie vanwege zijn taak om in concrete gevallen ernstige strafbare feiten te voorkomen of beëindigen. Extra veiligheidsmaatregelen worden dan onder verantwoordelijkheid van de officier van justitie ingezet. Ligt het te verwachten effect en de aard van de gebeurtenis op het terrein van de openbare orde dan zal het primaat liggen bij de burgemeester. In dat geval worden extra veiligheidsmaatregelen ingezet onder verantwoordelijkheid van de burgemeester.

1.4 Lokaal gezag treft alle noodzakelijke veiligheidsmaatregelen

Algemeen uitgangspunt is dat hoe ernstiger de dreiging, hoe zwaarder de te nemen extra veiligheidsmaatregelen zullen zijn. Het lokaal bevoegd

gezag staat een glijdende schaal van maatregelen ter beschikking. Lichtere maatregelen dragen over het algemeen vaak meer het karakter van openbare orde handhaving, terwijl in de regel zwaardere middelen zoals persoonsbeveiliging pas worden ingezet als meer concreet voor mensenlevens of zeer ernstige delicten valt te vrezen. Veiligheidsmaatregelen in die sfeer zullen veelal onder het gezag en verantwoordelijkheid van het OM worden bevolen. Incidenteel kan door de lokale gezagsdriehoek worden overwogen om het besluit over te nemen maatregelen omwille van de beheersconsequenties ter consultatie voor te leggen aan de korpsbeheerder.

Door het invoeren van een glijdende schaal verdwijnt het digitale onderscheid tussen bewaken en beveiligen. De glijdende schaal begint bij de lichtere maatregelen die onder de algemene noemer van «bewaken» kunnen worden gebracht. Bij bewaken gaat het in de eerste plaats om het observeren van (de omgeving van) bepaalde objecten of diensten zodat bij het signaleren van onregelmatigheden zo spoedig mogelijk kan worden ingegrepen dan wel assistentie kan worden ingeroepen. Onder bewaken wordt tevens begrepen het treffen van (preventieve) veiligheidsmaatregelen. Wanneer actief rekening wordt gehouden met de inzet van zwaardere geweldmiddelen wordt «bewaken» opgeschaald naar «beveiligen». Bij beveiliging van personen, objecten of diensten wordt er in beginsel al vanuit gegaan dat fysiek handelend optreden door politie noodzakelijk is of zal zijn om ernstige strafbare feiten te voorkomen of beëindigen of voor het afwenden van dreigende situaties of aanslagen.

1.5 Aanvullende verantwoordelijkheid Rijksoverheid: Rijksdomein

In aansluiting op het decentrale stelsel 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 regeringsstandpunt benoemde reeds een aantal categorieën van personen en objecten waarvan de bewaking of beveiliging tot de verantwoordelijkheid van de rijksoverheid valt. Het gaat om:
- bepaalde buitenlandse personen, objecten en internationale instellingen in Nederland;
- Nederlandse 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;
- personen, werkzaam in de strafrechtspleging.

Tevens werd in het regeringsstandpunt de mogelijkheid geschapen voor de rijksoverheid om categorieën van personen en objecten 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.

Aan de hand van die categorieën en criteria is een *limitatieve* lijst opgesteld van personen, objecten en diensten waarvoor de Rijksoverheid een bijzondere verantwoordelijkheid heeft en beslist over extra veiligheidsmaatregelen. Personen, objecten of diensten die niet op de lijst staan

vermeld, vallen gewoon binnen het decentrale stelsel van veiligheidszorg. In het decentrale domein kunnen dezelfde veiligheidsmaatregelen voor personen, objecten en diensten worden getroffen als ten behoeve van het Rijksdomein. Een goed geëquipeerd decentraal stelsel en een heldere limitatieve lijst voor het Rijksdomein schept duidelijkheid. Wanneer men op decentraal niveau twijfelt over de vraag of bepaalde personen, objecten of diensten alsnog op de lijst van de Rijksoverheid dienen te worden geplaatst dan dient men zich te wenden tot de NCBB. Zolang hierover geen expliciet besluit is genomen ligt de verantwoordelijkheid decentraal. In uitzonderlijke gevallen kan op Rijksniveau worden besloten incidenteel personen, objecten of diensten toe te voegen aan de limitatieve lijst van het Rijksdomein. Daartoe kan de Evaluatiedriehoek beslissen op voordracht van de NCBB (zie verder paragraaf 5.2). De aangepaste lijst wordt goed gecommuniceerd met het decentraal gezag. Het spreekt voor zichzelf dat wanneer besloten wordt veiligheidsmaatregelen te treffen ten behoeve van een bepaalde persoon, het ook kan gaan om een aantal objecten waar de te beveiligen persoon zich (regelmatig) bevindt.

Limitatieve lijst van personen, objecten of diensten waarvoor de Rijksoverheid als eerstverantwoordelijke besluit over extra veiligheidsmaatregelen

Categorie I
Personen, objecten of diensten waarvoor de Rijksoverheid als eerstverantwoordelijke *standaard* **extra veiligheidsmaatregelen (veelal persoonsbeveiliging) treft**

- de leden van het Koninklijk Huis
- de Minister-President
- Koninklijk bezoek
- Buitenlandse staatshoofden/regeringsleiders
- Buitenlandse ministers van buitenlandse zaken tijdens officiële bezoeken

Categorie II
Personen, objecten of diensten waarvoor de Rijksoverheid als eerstverantwoordelijke extra veiligheidsmaatregelen treft op basis van risico/dreiging (niet standaard)

- De overige leden van de Koninklijke familie (art. 6 en 38 Politiewet 1993)

- Bepaalde nationale politici, te weten
  - de bewindslieden
  - fractievoorzitters in en de lijsttrekkers voor de Tweede Kamer
  - de Voorzitters van de Eerste en Tweede Kamer

- Bepaalde gezichtsbepalende en daardoor risico-aantrekkende personen die werkzaam zijn in de (straf)rechtspleging, te weten:
  - de president en de procureur-generaal van de Hoge Raad
  - de leden van het College van procureurs-generaal;
  - de voorzitter van de Raad voor de Rechtspraak

- Bepaalde gezichtsbepalende en daardoor risicoaantrekkende functionarissen (veelal voorzitters) van een aantal Hoge Colleges van Staat, te weten
  - de vice-president van de Raad van State
  - de president van de Algemene Rekenkamer
  - de Nationale Ombudsman

- Bepaalde hoge buitenlandse gasten of diplomatieke posten in Nederland, te weten
  – buitenlandse bewindslieden in Nederland
  – alle ambassadeurs en ambassades alsmede consuls-generaal en consulaten, en de militaire attachés
  – SG's of voorzitters van enkele internationale verdragsorganisaties, te weten NAVO, EU, WEU, VN
  – President van de Wereldbank

- Bepaalde hoge militaire bezoekers, of militaire objecten, bijvoorbeeld:
  – US Chairman Joint Chiefs of Staff, Chairman Military Committee Nato, Supreme Allied Commander Europe/Atlantic
  – Afnorth

- Bepaalde buitenlandse gezichtsbepalende en daardoor risico-aantrekkende functionarissen van internationale organisaties die in Nederland zijn gevestigd alsmede hun gebouwen, te weten
  – International Criminal Tribunal for the Former Yugoslavia (ICTY), te weten hoofdaanklagers en fungerend rechter en bedreigde getuigen en verdachten)
  – International Criminal Court (ICC) (idem.) en
  – Internationaal Gerechtshof/Vredespaleis alsmede
  – Organisation for Prohibition of Chemical Weapons (OPCW)

- Bepaalde personen, objecten of diensten, die mogelijk risico-aantrekkend zijn en bij uitval of verstoring nationale impact hebben:
  – De directeur en het gebouw van de Nederlandse Bank NV (zie artikel 6 lid 1 sub 9 Politiewet 1993) alsmede bepaalde geldtransporten
  – Burgerluchtvaart (zie ook artikel 6 lid 3 Politiewet 1993)

Tevens vervult de NCBB een rol als intermediair ten behoeve van het ministerie van Buitenlandse Zaken richting het lokaal bevoegd gezag als het gaat om personen, objecten en diensten waarvoor de Nederlandse overheid als ontvangende staat (bijvoorbeeld op basis van een verdrag) de algemene verplichting heeft voor veiligheid van genoemden, die niet in de limitatieve lijst van het Rijksdomein zijn opgenomen, te waken. Het ministerie van Buitenlandse zaken geeft relevante meldingen hieromtrent door aan de NCBB. Te denken valt aan een melding van bedreiging aan het adres van een van de medewerkers op een ambassade. De NCBB zorgt ervoor dat een dergelijk bericht wordt doorgeleid naar bijvoorbeeld (het lokaal gezag van) de politie in de woonplaats van mogelijk bedreigde.

1.6 Rol Nationaal Coördinator Bewaking en Beveiliging

Zoals al eerder gesteld zal in navolging van de aanbevelingen van de Commissie van den Haak voor het nieuwe stelsel de Nationaal Coördinator Bewaking en Beveiliging (NCBB) worden aangesteld. De NCBB legt verantwoording af aan de ministers van BZK en Justitie en heeft van hen bevoegdheden gemandateerd gekregen. Het gezagsdualisme in de taakuitoefening van de NCBB alsmede de beheersmatige onderbrenging wordt nader uitgewerkt in paragraaf 5.2. De NCBB zal in het nieuwe stelsel belast worden met de hierna te noemen taken:

- Verder ontwikkelen van een integraal bewakings- en beveiligingsbeleid, alsmede het beheer van het integrale beleid;
- Leiding geven aan een eigen staf Bewaking en Beveiliging;
- Inzamelen van bij de diensten aanwezige informatie ten behoeve van het uitvoeren van dreigings- en risico-evaluaties. De NCBB kan indien nodig de diensten en via hen de regio's (dringend) verzoeken medewerking te verlenen aan het verstrekken van informatie;
- (laten) Inventariseren van risicogroepen;

- (laten) Toetsen van de informatie op volledigheid, actualiteit, juistheid en tijdigheid;
- (laten) Evalueren van de binnengekomen informatie;
- Voorzitten Afstemmingsoverleg Bewaking en Beveiliging (ABB);
- Lid en voorzitter Evaluatiedriehoek en in overeenstemming met de vaste leden de directeur-generaal Openbare Orde en Veiligheid (dgOOV) van BZK en de directeur-generaal Rechtshandhaving (dgRH) van Justitie vaststellen van bewakings- en beveiligingsopdrachten enadviezen. In spoedeisende gevallen besluit hij zelfstandig en informeert hij de dgOOV en dgRH achteraf. De opdrachten en adviezen worden verstrekt namens de minister van Justitie respectievelijk de minister van BZK;
- Zorgdragen voor afstemming met en tussen de AIVD, de MIVD, het KLPD en de ministeries van Algemene Zaken, van Buitenlandse Zaken en van Defensie;
- Aansturen van het Uitvoeringsoverleg en zich ervan verzekeren dat de opdrachten daadwerkelijk worden uitgevoerd;
- Communiceren met de betrokken (bedreigde) personen;
- Zorgdragen voor een administratieve afhandeling van de adviezen (registratie en documentatie);
- Begeleiden van implementatie door de lokale autoriteiten en regionale politiekorpsen van de landelijke kaders;
- Zorgdragen voor helderheid in de te onderscheiden domeinen;
- Optreden als intermediair ten behoeve van het ministerie van Buitenlandse Zaken richting het lokaal bevoegd gezag als het gaat om personen, objecten en diensten waarvoor de Nederlandse overheid als ontvangende staat (bijvoorbeeld op basis van verdrag) de algemene verplichting heeft voor veiligheid van genoemden, die niet in de limitatieve lijst van het Rijksdomein zijn opgenomen, te waken;
- Adviseren decentraal niveau over reikwijdte domein Rijksoverheid;
- Het voor het decentrale niveau aangeven van de informatiebehoefte voor het Rijksniveau, definiëren op welke doelgroep, aard en delictsoort gerubriceerd moet worden;
- Ontplooien van initiatieven ter innovatie van het proces van bewaken en beveiligen, in het bijzonder op het vlak van de uitvoering van (technische en technologische) maatregelen;

2 Nieuw stelsel: risicobenadering

2.1 Uitgangspunt

Naar de mening van de Commissie feitenonderzoek kan niet worden volstaan met te reageren op concrete dreigingen, maar zal ten behoeve van het nieuwe stelsel bewaken en beveiligen een bredere analyse van mogelijke dreigingen en risico's nodig zijn. In dat verband gaf de commissie in overweging mee om «voor een kleine kring van personen die reeds het voorwerp uitmaken van een gericht beveiligingsbeleid ook een systeem van *protective intelligence* op te zetten zoals dit in de Verenigde Staten tot ontwikkeling is gebracht. Een dergelijk systeem maakt het immers mogelijk om in een zo vroeg mogelijk stadium al die (stukjes) beschikbare informatie bij elkaar te brengen die wijzen op onwenselijke of onaanvaardbare acties in hun richting» (*De veiligheid en de beveiliging van Pim Fortuyn*, pagina 367). In zijn algemeenheid wordt bij «protective intelligence» de inzet van bijzondere inlichtingenmiddelen niet uitgesloten. Zoals ook in het Regeringsstandpunt van 17 december 2002 was aangekondigd is zorgvuldig onderzocht in hoeverre een systeem van «protective intelligence» wenselijk en noodzakelijk is. Er is voor gekozen om de systematiek van «protective intelligence» voor een groot deel over te nemen. In het nieuwe stelsel zal worden uitgegaan van een drieledige oriëntatie: belang, dreiging en weerstand. Deze drie elementen

worden in hun onderlinge samenhang onderzocht en leiden uiteindelijk tot een uitspraak over risico. Echter, geopteerd is voor een onderzoeksmethodiek waarbij, voor het doen van onderzoek naar potentiële dreiging, geen bijzondere inlichtingenmiddelen worden ingezet. Om die reden wordt gekozen voor het begrip «risicobenadering» in plaats van «protective intelligence». De inzet van bijzondere inlichtingenmiddelen is daarbij alleen dan gerechtvaardigd indien, in overeenstemming met artikel 8 EVRM, de inbreuk op de privacy evenredig is aan de ernst van de bedreiging (proportionaliteitsbeginsel) en de benodigde gegevens niet of niet tijdig via algemeen toegankelijke bronnen kunnen worden verkregen (subsidiariteitsbeginsel). Het gaat dan ook om het afluisteren van telefoongesprekken, volgen, observeren etcetera. Gelet op de grote aantasting van de persoonlijke levenssfeer van betrokkenen en zijn of haar omgeving, achten wij de inzet van bijzondere inlichtingenmiddelen en bijzondere opsporingsmethoden in het kader van beveiligingstaken te ingrijpend en niet proportioneel.

In het stelsel bewaken en beveiligen zal derhalve niet worden volstaan met het reageren op concrete dreigingen, maar zal in het kader van een risicobenadering een bredere analyse van mogelijke dreigingen en risico's plaatsvinden.[1]
Ingeval een crisis of ramp zich reeds manifesteert dan gelden de procedures zoals beschreven in het Nationaal Handboek crisisbeheersing (NHC).

2.2 Producten en instrument

Om een inschatting te kunnen maken van de dreiging en/of het risico leveren de (inlichtingen)diensten een aantal producten aan:
- dreigingsmeldingen/-inschattingen;
- dreigingsanalyses;
- risicoanalyses;
- een risicogerelateerd instrument, namelijk geëvalueerde momenten.

De producten en instrument worden als volgt omschreven:

Dreigingsmelding/-inschatting
Dreigingsmeldingen en dreigingsinschattingen worden gevraagd en ongevraagd verstrekt aan de NCBB door opsporings-, veiligheids- en/of inlichtingendiensten. Dreigingsmeldingen en inschattingen gaan over concrete (voorspelbare) dreigingen die zich op korte termijn zou kunnen voordoen tegen personen, objecten en diensten die binnen het domein vallen van de overheid, zowel de Rijksoverheid als de decentrale overheid. De bedreiger staat centraal. Ook voor bijvoorbeeld internationale terroristische dreigingen in relatie tot bewaken en beveiligen geldt dat deze door de diensten aan de NCBB worden gemeld.
De dreigingsinschatting is gebaseerd op feiten en omstandigheden met betrekking tot de dreiging en de ernst en waarschijnlijkheid van het manifesteren van de dreiging. Dreigingsmeldingen en inschattingen zijn de enige vormen van informatieverstrekking die zonodig spoedshalve ook mondeling kunnen plaatsvinden.

Dreigingsanalyse en Risicoanalyse
Voor het inventariseren en analyseren van *potentiële* dreiging zal worden gewerkt met dreigingsanalyses en risicoanalyses. Voor het vervaardigen van een dreigingsanalyse of risicoanalyse hoeft nog geen sprake te zijn van een ernstig vermoeden van een strafbaar feit of een concrete aanwijzing voor een serieuze dreiging. Door middel van persoons – en functiegerelateerde profielen (de functiegerelateerde profielen worden onder andere aangeleverd door de BVA's) worden over de betrokken persoon

[1] Er is bij een aantal landen (onder meer Engeland, Spanje, Zweden, Duitsland) navraag gedaan naar de wijze waarop het bewaken en beveiligen van personen en objecten is geregeld. Over het algemeen kan worden gesteld dat men in andere landen in Europa voor het nemen van veiligheidsmaatregelen «dreiging» als uitgangspunt neemt. Men bedient zich daarbij van een aantal dreigingsniveau's. Het belangrijkste verschil is dat in het nieuwe stelsel ook potentiële dreigingen geïnventariseerd en geanalyseerd zullen worden. Hiervoor zullen de Wet op de Inlichtingen- en Veiligheidsdiensten (WIV) 2002 en de Wet Politieregisters worden aangepast (zie paragraaf 2.5. voor een nadere toelichting).

gegevens verzameld over functie, gedrag en aard. Andere instrumenten om gegevens te krijgen over de te beveiligen persoon, object of dienst zijn bijvoorbeeld interviews, raadplegen privé- en publieke agenda, registreren incidenten uit privé- en publieke sfeer, beveiligingssurveys en scans van open bronnen.

Als randvoorwaarde geldt dat voor het verkrijgen van zicht op de privégegevens en situatie van betrokkene de eigen inbreng van betrokkene essentieel is. Afhankelijk van de mate van medewerking van betrokkene kan sprake zijn van een onvolledige dreigings- of risicoanalyse. Immers, zonder zijn of haar medewerking kan de analyse voor een groot deel alleen betrekking hebben op de publieke sfeer. Weigering of beperkte medewerking leidt er toe dat de overheid minder goed haar (aanvullende) verantwoordelijkheid kan nemen. Benadrukt wordt dat het verlenen van medewerking door betrokkene voor het verkrijgen van informatie over de privésfeer, geen automatisch recht geeft op beveiliging/bescherming door de Rijksoverheid.

Dreigings- en risicoanalyses kunnen als volgt worden gedefinieerd:
Een *dreigingsanalyse* is een gevraagde of ongevraagde (continue) analyse van concrete en potentiële dreigingen tegen één of meer bepaalde personen, objecten en/of diensten binnen het domein van de overheid (zowel decentraal als Rijksdomein). Zowel de bedreigde persoon, object en/of dienst(belang) als de bedreiger staan bij de dreigingsanalyse centraal.

Een *risico-analyse* is een continue analyse waarbij uitvoerig gekeken wordt naar en drietal elementen: belang, dreiging (concreet en potentieel) en weerstand in hun onderlinge samenhang. Allereerst wordt gekeken welke belangen in het geding zijn. Daarna wordt beschreven welke signalen er zijn over een concrete en/of potentiële dreiging en hoe deze dreiging er naar ernst en waarschijnlijkheid uitziet. Tot slot worden de reguliere mogelijkheden van de belangendragers om zich tegen deze dreiging te weer te stellen (het zogenoemde weerstandsvermogen) aan een nadere beschouwing onderworpen en worden deze drie elementen met elkaar in verband gebracht. Het risico is vervolgens de mate waarin de weerstand tekort schiet tegen een bepaalde dreiging. Op basis van de geconstateerde risico's kunnen vervolgens maatregelen genomen worden.

Geëvalueerde momenten
Een geëvalueerd moment is een door de lokale c.q. Evaluatiedriehoek vastgesteld moment waarbij een persoon in het decentrale dan wel Rijksdomein (bijvoorbeeld een bewindspersoon of fractievoorzitter) in het kader van het uitoefenen van zijn ambt optreedt in een voor breed publiek toegankelijke plaats waarbij een risico aanwezig is of verondersteld kan worden.
Deze momenten worden voor wat betreft het Rijksdomein via de beveiligingsambtenaar (BVA) gemeld aan de NCBB (zie ook paragraaf 3.2.3). Voor wat betreft het decentrale domein wordt het moment gemeld aan de lokale driehoek door de portefeuillehouder conflict- en crisisbeheersing binnen de politiekorpsen.

2.3 Domein: voor wie welke producten

A. De producten dreigingsmeldingen/-inschattingen en dreigingsanalyses zijn van toepassing op ieder persoon, object of dienst die binnen het decentrale en Rijksdomein valt. De noodzaak tot het vervaardigen van dreigingsanalyses voor het decentrale domein zal slechts sporadisch voorkomen (zie ook hoofdstuk 1 (domein). Veel veiligheidsmaatregelen

worden gewoonlijk getroffen op basis van de algemene politietaak zonder dat daarvoor een dreigingsanalyse wordt opgesteld. In het geval er daadwerkelijke indicaties aanwezig zijn die noodzaken tot een dreigingsanalyse dan dient een verzoek daartoe te worden ingediend bij het Nationaal Informatie Knooppunt (NIK) van het KLPD. Bovenregionale belegging vindt plaats om redenen van efficiëncy en adequate benutting van schaarse expertise vanwege de geringe frequentie. Bovendien wordt op deze manier zoveel mogelijk op eenduidige wijze omgegaan met informatie en het duiden van (potentiële) dreiging. Er zijn criteria ontwikkeld waaraan een dreigingsanalyse moet voldoen.

B. Het instrument geëvalueerde momenten geldt voor personen in functie binnen zowel het decentrale als Rijksdomein.

C. Het product risicoanalyse geldt voor een beperkte groep binnen het Rijks- domein. Voor een vaste groep binnen het Rijksdomein betreft het vervaardigen van risicoanalyses een continu proces: de Koningin en haar woning/paleizen, de Minister-President en zijn woning en de bewindslieden en hun woningen.[1] Voor een flexibele groep binnen het Rijksdomein worden risicoanalyses vervaardigd afhankelijk van het beleid en te voorziene gebeurtenissen.[2] Alhoewel risico-analyses in principe alleen voor het Rijksdomein gelden, kan het incidenteel voorkomen dat, op verzoek en mits het raakt aan de nationale veiligheid, een risicoanalyse ook voor het decentrale domein wordt vervaardigd (zie ook paragraaf 4.1). Op basis van een risico-analyse kunnen door de NCBB extra veiligheidsmaatregelen worden geadviseerd of bevolen. Van belang daarbij is dat de NCBB zich voor zijn beoordeling niet uitsluitend richt op de risico-analyse maar ook diplomatieke, politieke en andere belangen mee laat wegen.

2.4 Glijdende schaal van dreigingsniveaus

Op zowel decentraal als Rijksniveau worden dezelfde speciaal ontwikkelde formats en tabellen inzake dreigingsniveaus gehanteerd. Aan de hand van de tabellen wordt een inschatting gegeven van de mate van ernst en waarschijnlijkheid (omvang en effect) van de dreiging, waardoor een glijdende schaal van dreigingsniveaus wordt gerealiseerd. De producten worden, afhankelijk van de aard, gevraagd en ongevraagd door de diensten vervaardigd. Schematisch kan de glijdende schaal van dreigingsniveaus als volgt worden weergegeven:

[1] De reden dat voor deze vaste groep risicoanalyses worden gemaakt is gelegen in het feit dat hun veiligheid en ongestoord functioneren van groter belang is dan bij andere personen, objecten of diensten, vanwege de prominente plaats en/of functie die zij in de Nederlandse maatschappij innemen en het vitale belang dat zij vertegenwoordigen voor deze maatschappij. Er is sprake van een nationaal belang.

[2] Gebeurtenissen zoals nationale verkiezingen, Eurotop, oorlog etcetera. Daarbij spreekt het enerzijds voor zich dat volledige risico-analyses niet op korte termijn kunnen worden gemaakt. Bij bijvoorbeeld een plotselinge en kortstondig bezoek van een hoge buitenlandse bezoeker kan slechts sprake zijn van een dreigingsinschatting of dreigingsanalyse. Anderzijds is het wel wenselijk en praktischer om in geval van bijzondere gebeurtenissen voor een op dat moment relevante, specifieke groep van personen, objecten en diensten risico-analyses te vragen. Denk hierbij bijvoorbeeld aan vertegenwoordigers van landen in conflictgebieden waaruit bepaalde minderheden in Nederland afkomstig zijn, of voor de diplomatieke vertegenwoordigers van de vijf permanente leden van de Veiligheidsraad.

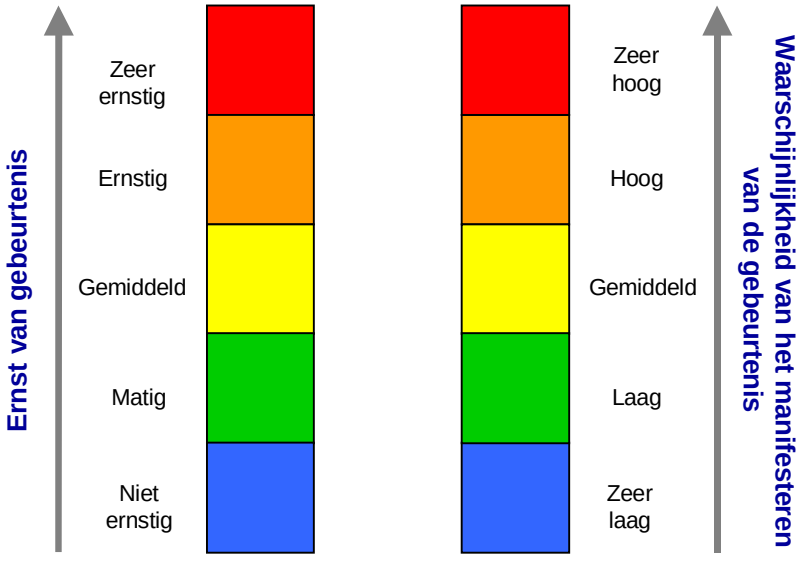
ERNST VAN DE GEBEURTENIS

Categorie	Effect	Aard
Zeer ernstig	– Massaal aantal dodelijke slachtoffers – Uitval van (delen van) vitale infrastructuren (eventueel, zonder dat direct mensenlevens in gevaar worden gebracht) – Maatschappij ontwrichting	Grootschalige aanslag met gebruik van NBC-middelen of conventionele middelen met een NBC-effect
Ernstig	– Vrees voor het leven van één of enkele personen – Samenleving ernstig geschokt	Aanslag, doodslag, moord, gijzeling, ontvoering, sabotage, brandstichting, (terroristische) aanslag in het buitenland met massaal aantal slachtoffers
Gemiddeld	– Grootschalige openbare ordeverstoringen – Grote zaakschade aan niet-vitale objecten – Fysieke integriteit VIP geschonden	Handgemeen tijdens openbaar bezoek VIP, gewelddadige confrontaties tussen (politieke) groeperingen, mishandeling
Matig	– Kleinschalige openbare ordeverstoringen – Intimidatie VIP	Burgerlijk ongehoorzame acties (bijvoorbeeld bezetting, opstootjes/demonstraties met gewelddadige elementen)
Niet ernstig	– Geen effecten voor de nationale veiligheid (inclusief openbare orde)	Vreedzame demonstratie, aanbieden petitie

WAARSCHIJNLIJKHEID VAN DE GEBEURTENIS

Categorie	Beschikbare informatie
Zeer hoog	Concrete aanwijzingen (feiten en omstandigheden) dat een gebeurtenis geëffectueerd zal worden: bekendheid van plaats en tijd
Hoog	Concrete aanwijzingen dat een gebeurtenis zich zal voordoen, alleen plaats en tijd zijn niet bekend. En/of een gebeurtenis wordt zeer voorstelbaar geacht
Gemiddeld	Geen concrete aanwijzingen, maar de gebeurtenis is voorstelbaar
Laag	Geen concrete aanwijzingen, maar de gebeurtenis wordt nog enigszins voorstelbaar geacht
Zeer laag	Geen concrete aanwijzingen en de gebeurtenis wordt evenmin voorstelbaar geacht

Ter duiding voor de ernst en waarschijnlijkheid wordt een model gehanteerd dat een (dubbele) kwalificering van de dreiging aangeeft. De twee elementen ernst en waarschijnlijkheid bepalen of de overheid iets zou moeten ondernemen tegen een gebeurtenis. Onderstaande kolommen kunnen daarbij behulpzaam zijn. Doel hiervan is om bijvoorbeeld bij een zeer ernstige situatie en een zeer lage waarschijnlijkheid niet tot een overreactie te komen en andersom. Maatwerk wordt hierdoor mogelijk.



In de (Evaluatie)driehoek kunnen ook andere parameters in overweging worden genomen, zoals politieke en/of diplomatieke belangen. Alle parameters tezamen bieden de basis voor de uiteindelijke totale afweging.

2.5 Aanpassing wet- en regelgeving

Een absolute voorwaarde voor het invoeren van een volledig systeem van risicobenadering is dat de huidige wet- en regelgeving wordt aangepast. Het gaat dan om aanpassing van de WIV 2002 en de Wet Politieregisters. Onder de huidige regelgeving kunnen opsporings- en veiligheidsdiensten in voldoende mate aandacht besteden aan bestaande dreigingen. Voor onderzoek naar bestaande dreigingen is tevens de inzet van bijzondere inlichtingenmiddelen gerechtvaardigd en toegestaan. Voor wat betreft onderzoek naar *potentiële* bedreigingen kan nu alleen naslag worden verricht naar bij de diensten reeds aanwezige informatie, die in het kader van hun taakstelling reeds met bijzondere inlichtingenmiddelen kan zijn verkregen. Deze informatie kan ook worden meegewogen bij het opstellen van dreigings- en risicoanalyses. Voor het doen van nader onderzoek naar personen en organisaties waarvan een mogelijke (potentiële) dreiging uitgaat naar een te beveiligen en bewaken persoon, object of dienst, bijvoorbeeld door middel van het raadplegen van niet-openbare gegevensbronnen en het raadplegen van informanten, alsmede voor het kunnen vastleggen van dit soort informatie, dient voor de AIVD additionele regelgeving tot stand te worden gebracht. In concreto betekent dit dat additionele regelgeving nodig is voor het vervaardigen van zowel dreigingsanalyses en risicoanalyses, daar voor beide producten potentiële dreigingen moeten worden geïnventariseerd en geanalyseerd. Ook voor verstrekking van door de politie van informatie aan de NCBB is aanpassing van wetgeving noodzakelijk.

Benadrukt wordt dat, ook na een wetswijziging, voor het doen van onderzoek naar potentiële bedreigers in ieder geval geen bijzondere inlichtingenmiddelen of bijzondere opsporingsmethoden worden ingezet. Het gebruik van dergelijke middelen wordt door ons in sterke mate een aantasting geacht van de persoonlijke levenssfeer van betrokkene en zijn of haar omgeving. Immers, het gaat dan ook om het afluisteren van telefoongesprekken, volgen, observeren etcetera. Dit laatste achten wij in het kader van beveiligingstaken te ingrijpend en niet proportioneel.

3 Leveranciers producten en instrument

3.1 Decentraal

Voor wat betreft het verkrijgen van dreigingsinformatie, te weten dreigingsmeldingen/-inschattingen ten behoeve van het decentrale domein is een voorname rol weggelegd voor de Regionale Informatieknooppunten (RIK's). Daar dient de informatie samen te komen van de Criminele Inlichtingeneenheden (CIE), Regionale Inlichtingendiensten (RID, ten behoeve van openbare orde informatie) en andere relevante politie-informatie. Het welslagen van het Project Landelijke Informatiecoördinatie DNP (De Nederlandse Politie) is daarbij een *randvoorwaarde.* Dit project heeft tot doel te komen tot een landelijke infrastructuur op het gebied van politiële informatiecoördinatie. Hiertoe zijn in de regiokorpsen de eerder genoemde Regionale Informatieknooppunten (RIK's) ingericht.

Het vervaardigen van dreigingsanalyses voor het decentrale domein zal, zoals eerder aangegeven, op landelijk niveau worden uitgevoerd door het Nationaal Informatie Knooppunt (NIK) van het KLPD. Er zullen criteria ontwikkeld moeten worden aan de hand waarvan dreigingsanalyses ingegeven zijn. Via deze constructie kan beter aansluiting worden verkregen

met de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), die voor dit doel reeds een liaison bij het NIK heeft geplaatst (zie ook paragraaf 3.2 Rijksdomein). Opgemerkt wordt hierbij dat ook de AIVD voor het decentrale domein dreigingsinformatie kan aanleveren, indien vanuit haar wettelijke taakstelling aanleiding daartoe bestaat, i.e. indien het raakt aan de nationale veiligheid. De AIVD levert de informatie in zo'n geval aan de regionale portefeuillehouder conflict- en crisisbeheersing.

3.2 Rijksdomein

Ten behoeve van het rijksdomein zal informatie uit open en gesloten bronnen worden aangeleverd door het KLPD (NIK), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), de AIVD en de beveiligingsambtenaren (BVA's).

3.2.1 Nederlandse politie/NIK

Voor wat betreft de Nederlandse politie speelt het NIK, dat is ondergebracht bij het KLPD, een centrale rol. De producten die het NIK levert aan de NCBB zijn dreigingsmeldingen/-inschattingen en (criminele en openbare orde) dreigingsanalyses. Regionale informatie komt via de RIK's samen in het NIK. Dit betekent niet dat alle regionale informatie aan het NIK wordt aangeboden maar alleen de informatie die via de landelijke behoeftestelling is bepaald. Zo is recent in het kader van bewaken en beveiligen via het NIK aan de regiokorpsen gevraagd informatie te verstrekken omtrent (incidenten tijdens) de landelijke verkiezingen. Op basis van een informatiestrategie (wat is er aan de hand en wat willen we weten?) en een informatie-inwinplan (welke informatie komt waar vandaan?) is de informatiebehoefte die op landelijk niveau aanwezig is vertaald naar de regiokorpsen. Het NIK coördineert en veredelt deze informatie en biedt deze in de vorm van dreigingsanalyses of situatierapportages aan de NCBB aan en koppelt deze eveneens terug aan de regiokorpsen.

In het nieuwe stelsel bewaken en beveiligen is aangesloten bij het traject Landelijke Informatiecoördinatie DNP. Dit betekent niet alleen dat het NIK, voor wat betreft de politie-informatie, het eerste aanspreekpunt is voor de NCBB, maar dat ook de landelijke informatiebehoefte via het KLPD/NIK vertaald wordt naar de regiokorpsen. Om de informatie-uitwisseling tussen het NIK en de AIVD te optimaliseren is er een liaison van de AIVD geplaatst bij het NIK. Ook vanwege het feit dat de AIVD risicoanalyses gaat vervaardigen (zie paragraaf 3.2.2) is het van belang dat via deze constructie (RIK en NIK) centraal informatie aan de AIVD wordt aangereikt. Om op decentraal/lokaal niveau die informatie te verzamelen die van belang is in het kader van bewaken en beveiligen wordt helder gedefinieerd op welke doelgroep, aard en delictsoort gerubriceerd dient te worden. Op Rijksniveau wordt de informatiebehoefte op het gebied van bewaken en beveiligen ten behoeve van het Rijksdomein aangegeven. Voor de ontsluiting van informatie uit politie- en justitieregisters worden in nauw overleg met het Openbaar Ministerie (OM) adequate afspraken gemaakt en voorzieningen getroffen. Op dit moment werkt een interdepartementale werkgroep aan de juridische consequenties welke gemoeid zullen zijn met de (landelijke) informatiecoördinatie. Indien aanpassingen in dit kader noodzakelijk zijn, zullen deze worden meegenomen in het traject van de herziening van de Wet Politieregisters (WPolR).

3.2.2 MIVD en AIVD

De MIVD en AIVD leveren dreigingsmeldingen/-inschattingen en dreigingsanalyses (inclusief dreigingsanalyses over potentiële dreiging).

Uitvoering (dreigings- en) risicoanalyses
Het vervaardigen van dreigings- en risico-analyses zou in principe een taak kunnen zijn van een nieuwe organisatie, de NCBB, het KLPD, of de AIVD. Een nieuwe organisatie voor het vervaardigen van risico-analyses (en ook dreigingsanalyses, als input voor de risico-analyse) is naar onze inschatting geen reële optie. Een organisatie die naast bijvoorbeeld het KLPD, de AIVD en de NCBB een wezenlijke taak krijgt op het vlak van bewaken en beveiligen vergroot de onoverzichtelijkheid en levert extra afstemmingsproblemen op. Dit achten wij niet wenselijk. Het laten vervaardigen van dreigingsanalyses en risicoanalyses door de NCBB zelf, zoals ook voorgesteld in het regeringsstandpunt, is ook denkbaar maar heeft als nadeel dat dan analyse, advisering en besluitvorming over het dreigingsniveau en te nemen maatregelen in één hand komt te liggen.

Voor zowel de AIVD als het KLPD zou het vervaardigen van risico-analyses (en volgens de nieuwe definities ook dreigingsanalyses) een nieuwe taak zijn. Noodzakelijk is dan om naast concrete dreigingen ook potentiële dreigingen te kunnen inschatten, waarbij van belang is dat specifieke informatie rondom de bedreigde wordt verzameld. Het KLPD verzamelt en analyseert alleen openbare orde- of strafrechtelijke informatie. Het vervaardigen van risico-analyses op nationaal niveau, waar nationale belangen in het geding zijn en er een relatie bestaat met bedreigingen voor de nationale veiligheid, past hier niet bij. De AIVD is primair belast met het verzamelen en analyseren van informatie over dreigingen die zich voordoen op zijn taakvelden en niet met openbare orde- of strafrechtelijke informatie. Het vervaardigen van risico-analyses in het kader van persoonsbeveiliging heeft ook nooit tot de taken van de AIVD behoord.

Samenvattend komt het er op neer dat de risicobenadering een taak met zich meebrengt die niet eerder op deze wijze door de overheid is uitgevoerd. Er is dan ook geen organisatie aan te wijzen die reeds volledig geëquipeerd is voor deze taak. De voorkeur gaat naar een organisatie die meer geschikt is dan de andere genoemde organisatie(s): wij kiezen derhalve voor de AIVD. De relatie naar werkzaamheden in het kader van de nationale veiligheid vloeit direct voort uit de Wet op de inlichtingen- en veiligheidsdiensten 2002 (WIV 2002). Daarnaast heeft deze dienst ruime ervaring in het opstellen van (dreigings)inschattingen, beschikt hij over goed opgeleide en deskundige analisten en is hij gewend informatie uit (open) bronnen te volgen, te analyseren en te vatten tot volwaardige producten en adviezen. Tevens beschikt de AIVD over een optimaal beveiligde werkomgeving, wat in verband met het beschikken over vertrouwelijke informatie een primair vereiste is. Ten slotte is het voor de AIVD, gelet op de wettelijke bevoegdheden (WIV 2002, artikel 60 en met name 62) minder problematisch om benodigde informatie van de regiokorpsen te verkrijgen dan andersom.

Als randvoorwaarde geldt dat de regiopolitie, KLPD en MIVD hun medewerking verlenen aan de AIVD door het verstrekken van relevante informatie. Voor wat betreft het KLPD dient dit via de in paragraaf 3.2.1 beschreven proces (RIK en NIK) plaats te vinden. Dit betekent wel dat het KLPD relevante criminele- en openbare orde dreigingsinschattingen en -analyses zal moeten vervaardigen en verstrekken aan de AIVD. Tevens dient de AIVD ook van andere instanties tijdig relevante informatie te ontvangen, bijvoorbeeld van de Veiligheidsdienst Buitenlandse Zaken (VDB, analyses naar aanleiding van buitenlandse reizen bewindslieden. Deze analyses kunnen dan als input gebruikt worden voor de inschattingen en analyses van de AIVD). Omwille van de effectiviteit en zuiverheid valt te overwegen dit product binnen de AIVD separaat van het inlichtingeninwinnende werkproces te organiseren. Personele capaciteitsuitbreiding is dan ook noodzakelijk, niet alleen voor het vervaardigen van

de risicoanalyses maar ook voor het vervaardigen van dreigingsscenario's of dreigingsanalyses, als input voor de risico-ananalyse, omdat in het nieuwe stelsel ook potentiële risico's in kaart gebracht moeten worden.

3.2.3 BVA's

De departementale leiding, in casu de secretaris-generaal (SG) is verantwoordelijk voor de beveiliging van het departement en van de aan het departement toevertrouwde overheidsgeheimen (Beveiligingsvoorschrift 1949). Namens de SG wordt deze taak uitgevoerd door de beveiligingsambtenaar (BVA), die in een hiërarchische relatie staat met de departementsleiding (SG).

In het nieuwe stelsel krijgen de beveiligingsambtenaren (BVA's) een vaste rol toebedeeld voor het leveren van functiegerelateerde profielen en het instrument geëvalueerde momenten. Dit geldt niet alleen de departementale BVA's maar ook de BVA's voor Hoge College's van Staat. De functiegerelateerde profielen worden opgesteld voor bewindspersonen en fractievoorzitters en leveren een bijdrage aan de dreigingsinschattingen, dreigings- en/of risico-analyses zoals die door de AIVD wordt opgesteld. De functiegerelateerde profielen worden niet beschouwd als apart product maar als input voor de NCBB. De BVA's dienen de functiegerelateerde profielen inhoud te geven en tevens te beheren. Dit gebeurt op basis van een gestandaardiseerd format ontwikkeld door de AIVD.

Daarnaast speelt de BVA een initiërende rol in het systeem van geëvalueerde momenten. Deze momenten zullen via de BVA gemeld worden aan de NCBB. Communicatie over eventueel te nemen maatregelen of het bestaan van risico of dreiging dient ook tussen de NCBB en de BVA te verlopen. Uitgangspunt hierbij is dat de BVA-functie over de juiste competenties beschikt evenals over de juiste bevoegdheden en verantwoordelijkheden.
De departementale leiding ziet er op toe dat de BVA's voldoen aan de benodigde kwaliteits- en opleidingseisen.

4 Weging en toetsing

4.1 Decentraal

Verschillende soorten politie-informatie (openbare orde, opsporingsinformatie) worden samengebracht bij de Regionale Informatie Knooppunten (RIK's). Bij concrete dreigingsinformatie wordt door de portefeuillehouder conflicten crisisbeheersing[1] van het regionale politiekorps de lokale gezagsdriehoek geadviseerd over de mate van dreiging en de uitvoering van te nemen maatregelen. Voor wat betreft het vervaardigen van dreigingsanalyses geldt dat het lokale gezag, via de portefeuillehouder, daartoe een verzoek indient bij het NIK, dat de informatie analyseert, veredelt en doorgeeft aan het lokaal gezag. Geadviseerd wordt ten behoeve van de eenduidigheid en uniformiteit criteria op te stellen aan de hand waarvan beoordeeld kan worden of een dreigingsanalyse is geïndiceerd. Risico-analyses gelden in principe uitsluitend voor het Rijksdomein. Incidenteel kan het voorkomen dat vanuit het decentrale domein behoefte bestaat aan een risico-analyse. De portefeuillehouder conflict- en crisisbeheersing dient hiertoe een verzoek in bij de NCBB, die het verzoek bespreekt met de AIVD. Indien het verzoek wenselijk en haalbaar wordt geacht, en het raakt aan de nationale veiligheid, zal de AIVD de analyse uitvoeren. Benadrukt wordt dat net zoals voor het centrale domein zeer selectief met verzoeken om dreigingsanalyses en risico-analyses dient te worden omgegaan.
Voor het wegen en toetsen van de informatie worden op decentraal

[1] Bij het kiezen van deze functionaris wordt zoveel mogelijk aangesloten bij bestaande structuren. Deze functionaris kan tevens functioneren als centraal aanspreekpunt voor de NCBB, voor het alerteren op ontwikkelingen en ontvangen van signalen over dreiging op het vlak van bewaken en beveiligen. Hij vervult op deze wijze de rol die in het Regeringsstandpunt van 17 december 2002 was toegedicht aan eenheden binnen de regionale politiekorpsen.

niveau dezelfde criteria gehanteerd als op het Rijksniveau. De informatie over dreiging kan ook leiden tot (intensivering van) recherche-onderzoek. De inzet van strafvorderlijke dwangmiddelen, zoals aanhouding, kan ook leiden tot het wegnemen van de dreiging. Het is echter niet te beschouwen als een extra veiligheidsmiddel in de zin van bewaken en beveiligen.

4.2 Rijksdomein

4.2.1 NCBB

Bij de NCBB komt relevante informatie aangaande risico en dreiging, voorzover dit het Rijksdomein raakt, ongevraagd en gevraagd samen. De informatie is niet uitsluitend afkomstig van de «diensten» (KLPD/NIK, AIVD en MIVD) maar wordt ook betrokken van open bronnen (ANP, kranten, publicaties). Als randvoorwaarde geldt dat het KLPD er op toeziet dat de relevante informatie vanuit de regio's via de Regionale Informatie Knooppunten (RIK's) en het Nationaal Informatie Knooppunt (NIK) bij de NCBB binnenkomt.

De NCBB wordt ondersteund door een eenheid bestaande uit functionarissen die belast zijn met het verzamelen, evalueren en beoordelen van de verkregen informatie. Deze eenheid wordt de Eenheid Bewaken en Beveiligen genoemd (EBB). Zij toetsen de (geanalyseerde) informatie op volledigheid en juistheid en vergelijken de onderlinge samenhang. De personen werkzaam bij en voor de NCBB dienen te beschikken over een aantal kerncompetenties, zoals relevante ervaring en een brede maatschappelijke oriëntatie, affiniteit met politieke en bestuurlijke processen alsmede affiniteit met de werkwijze en informatieprocessen van inlichtingendiensten en het proces van uitvoering van veiligheidsmaatregelen. Het verdient voorts aanbeveling dat de functionarissen bij de NCBB en hun contactpersonen bij de uitvoerende diensten zoveel mogelijk, en voorzover mogelijk kennis nemen van elkaars expertise, bijvoorbeeld via tijdelijke detacheringen over en weer. Tevens zullen bij de NCBB initiatieven worden ontplooid ter innovatie van het proces van bewaken en beveiligen, in het bijzonder op het vlak van de uitvoering van (technische en technologische) maatregelen. Dit in samenwerking met het KLPD.

4.2.2 Proces van weging en toetsing

Informatievergaring naar aanleiding van dreigingsmelding en/of incident
De NCBB gaat na in hoeverre de persoon, object of dienst waarop de melding betrekking heeft binnen het domein van de Rijksoverheid valt. Zoniet, dan verifieert hij bij het relevante lokale gezag of de informatie aldaar aanwezig is en in behandeling wordt genomen. De diensten wordt gevraagd om informatie, in de vorm van dreigingsmeldingen/informatie, dreigings-analyses over zowel concrete en potentiële dreigingen en risicoanalyses. De diensten kunnen ook ongevraagd informatie leveren. De NCBB kan indien nodig de diensten en via hen de regio's (dringend) verzoeken medewerking te verlenen aan het verstrekken van informatie. Als randvoorwaarde geldt dat voor de ontsluiting van informatie uit politie- en justitieregisters bedoeld voor de opsporing van strafbare feiten ten behoeve van de producten inzake bewaken en beveiligen, adequate afspraken worden gemaakt en voorzieningen worden getroffen. Het OM zal er op toezien dat zaaksofficieren en CIE-officieren relevante opsporingsinformatie doorgeven aan een bij het landelijk parket aan te stellen officier, zodat deze kan toetsen of die informatie kan/moet worden verstrekt voor bewakings- en beveiligingsdoeleinden (voor dreigings- en/of risicoanalyses).

Eerste beoordeling
De NCBB beoordeelt of de verkregen informatie voldoet aan de vastgestelde eisen van berichtgeving (schriftelijk), compleetheid, juistheid, tijdigheid en actualiteit en hanteert voor dit doel de speciaal ontwikkelde formats (zie ook paragraaf 2.3). De NCBB beoordeelt in hoeverre aanvullende informatie van de diensten benodigd is.

Evaluatie
De functionarissen werkzaam voor de NCBB evalueren, onder anderen aan de hand van de ontwikkelde modellen voor dreiging en risico, de verkregen informatie en analyses op hun onderlinge samenhang. De informatie wordt voorts vergeleken met informatie verkregen uit andere bronnen. Vervolgens wordt de informatie tijdens een vast overleg (Afstemmingsoverleg Bewaking en Beveiliging, ABB) onder voorzitterschap van de NCBB besproken met zware, gemandateerde vertegenwoordigers van de diensten. De vertegenwoordigers kunnen zich laten vergezellen van een expert van hun organisatie. De expert kan dus in principe steeds een andere persoon zijn, afhankelijk van het onderwerp. Als randvoorwaarde geldt daarbij dat de expert de informatie/analyse zo open mogelijk toelicht, uiteraard met inachtneming van bronbescherming. Een additionele randvoorwaarde is dat de informatie als vertrouwelijk dan wel zeer vertrouwelijk wordt beschouwd, met andere woorden een beperkte verspreiding kent. Tijdens het ABB wordt alvast aan de hand van een ontwikkeld format bezien welke maatregelen grosso modo geïndiceerd zijn bij de vastgestelde mate van dreiging en/of risico. Vooruitlopend op het besluit van de Evaluatiedriehoek over te nemen maatregelen zal het Uitvoeringsoverleg (zie ook hierna) worden gevraagd om een advies op hoofdlijnen. Het ABB komt in de plaats van de voormalige TEC en het huidige Evaluatieoverleg (EO).

5 Advisering en besluitvorming

5.1 Decentraal

Net zoals voor het centrale niveau geldt kan op decentraal niveau het eerdergenoemde Uitvoeringsoverleg advies worden gevraagd over de uitvoering van maatregelen. De adviezen worden via de portefeuillehouder conflict- en crisisbeheersing voorgelegd aan de lokale gezagsdriehoek. De ernst van de dreiging (concreet en potentieel), en in het bijzonder het effect en de aard van de verwachte gebeurtenis is bepalend te zijn voor de vraag bij wie het primaat ligt binnen de driehoek.

Indien de lokale gezagsdriehoek moet besluiten over zichzelf, met andere woorden als een lid van deze driehoek zelf onderwerp is van dreiging, vindt besluitvorming plaats door de Evaluatiedriehoek. In geval van risico of dreiging jegens personen werkzaam in de (straf)rechtspleging dan geldt dat het College van procureurs-generaal wordt gehoord, alvorens een besluit op decentraal dan wel Rijksniveau wordt genomen.

5.2 Rijksdomein

De Evaluatiedriehoek (ED) buigt zich over de adviezen van het ABB. De ED bestaat naast de NCBB als voorzitter (en vast lid) in ieder geval uit de vaste leden, de directeur-generaal rechtshandhaving (dgRH) van het ministerie van Justitie en Directeur-generaal Openbare Orde en Veiligheid (dgOOV) van het ministerie van BZK. Het gezagsdualisme in de lokale gezagsdriehoek met betrekking tot de uitoefening van de politietaak is daarmee «doorvertaald» naar Rijksniveau en strookt met de politieke (eind)verantwoordelijkheid van beide politieministers. Zo heeft de minister van Binnenlandse Zaken een generieke verantwoordelijkheid

voor de handhaving van de openbare orde waarin bovenlokale of nationale belangen een rol spelen. De minister van Binnenlandse zaken en Koninkrijksrelaties kan de Commissarissen van de Koningin (CdK's) en burgemeesters namelijk aanwijzingen geven met betrekking tot het door hen ter handhaving van de openbare orde te voeren beleid, indien door een ordeverstoring (of ernstige vrees dat die ontstaat) de veiligheid van de Staat in gevaar komt, of de betrekkingen van Nederland met andere mogendheden, dan wel zwaarwegende belangen van de samenleving, kunnen worden geschaad (artikel 16 lid 2 Politiewet 1993). Wanneer in een concreet geval ernstige strafbare feiten moeten worden voorkomen of beëindigd, dan zal het primaat liggen bij justitie vanwege de verantwoordelijkheid voor de strafrechtelijke handhaving van de rechtsorde. Te denken valt aan de voorkoming van terreurdaden en andere gewelds-delicten tegen het leven of ernstige delicten tegen bepaalde objecten of diensten. De minister van Justitie is op basis van de Politiewet 1993 de bevoegde autoriteit om het KLPD opdracht te geven tot persoonsbeveiliging voor personen binnen het Rijksdomein en is daarnaast verantwoordelijk voor de inzet van de Bijzondere Bijstandseenheden (BBE). Daar waar de BBE wordt ingezet in het kader van bewaken en beveiligen heeft de NCBB een adviserende riol richting de minister van Justitie.
Daarnaast draagt de minister van Justitie een bijzondere verantwoordelijkheid voor de beveiliging van een aantal objecten en diensten waarmee de KMar ingevolge de Politiewet 1993 is belast, zoals de Nederlandse Bank, de koninklijke paleizen en de burgerluchtvaart. De minister van Justitie geeft de commandant van de Koninklijke marechaussee daartoe de nodige algemene en bijzondere aanwijzingen.

De NCBB wordt aangestuurd door de minister van BZK en de minister van Justitie. De zeggenschap van beide ministers loopt via de lijn van de dgOOV en dgRH. Het proces van komen tot adviezen c.q. besluiten dat in dit hoofdstuk verder is uitgewerkt, vindt derhalve plaats onder de verantwoordelijkheid van beide ministers. Beheersmatig worden de NCBB en zijn ondersteunende eenheid als aparte entiteit ondergebracht bij het ministerie van BZK. De NCBB legt verantwoording af aan de ministers van BZK en Justitie en zal van hen daartoe de nodige bevoegdheden gemandateerd krijgen.

Tevens neemt de directeur Juridische Zaken van het ministerie van Defensie deel aan de besluitvorming van de ED voor zover er Defensiebelangen in het geding zijn Daarnaast zal een vertegenwoordiger van het ministerie van Buitenlandse Zaken (plaatsvervangend SG) deelnemen aan de besluitvorming voor zover er BZ-belangen in het geding zijn, vanwege het feit dat dikwijls politieke en diplomatieke belangen aan de orde komen. Afhankelijk van het onderwerp en de belangen kunnen incidenteel ook vertegenwoordigers van andere departementen als adviseur deelnemen. Dit laat onverlet dat, gezien de eerdergenoemde politieke eindverantwoordelijkheid van de ministers van Justitie en BZK, de stem van de vaste leden NCBB, dgOOV en dgRH voor wat betreft de besluitvorming in de Evaluatiedriehoek doorslaggevend is.

Advisering en besluitvorming
De ABB legt het eindadvies (inclusief het advies op hoofdlijnen van het Uitvoeringsoverleg) voor aan de NCBB. De NCBB stelt zelfstandig de meest routinematige adviezen vast. In gevallen met een spoedeisend karakter neemt de NCBB reeds voorafgaand aan besluitvorming in de Evaluatiedriehoek (ED) passende maatregelen en informeert hij vervolgens de leden van de Evaluatiedriehoek achteraf. Over de niet-routinematige adviezen pleegt de NCBB overleg met de twee overige vaste leden van de ED en de eventueel deelnemende adviserende leden. Zonder

instemming van de vaste leden van de ED kan de NCBB niet-routinematige adviezen niet zelfstandig vaststellen.

In de ED kunnen naast de parameters dreiging en risico ook andere parameters aan de orde komen, zoals diplomatieke, politieke of financiële belangen en overwegingen. De beraadslaging van de ED leidt tot besluitvorming over de reikwijdte van het Rijksdomein en geeft richting aan de vraag voor wie risico-analyses binnen het Rijksdomein dienen te worden opgesteld. Beleidsvoorbereiding en effectuering is in handen van de NCBB. Nadat de leden van de ED tot een standpunt zijn gekomen op basis van de adviezen, verzekert de NCBB zich ervan dat de veiligheidsmaatregelen worden uitgevoerd.

6 Uitvoering

6.1 Decentraal

Indien de lokale gezagsdriehoek besluit tot het nemen van maatregelen worden deze in beginsel uitgevoerd door de politie van de betreffende regio. Op decentraal niveau kunnen dezelfde veiligheidsmaatregelen worden getroffen als op landelijk niveau. Voorbeelden van maatregelen, oplopend van licht naar zwaar zijn: begeleiding, doorlaatposten op afstand, liaison, wegafsluiting, roadblocks, omgevingsalertering, camera-observatie, beveiligingsadvies, routeverkenning, bouwtechnisch advies, pasjesregeling, volgauto, schouw, voorverkenauto, verscherpt rijdend toezicht, VIP-auto, bewakingscontainer, persoonsbegeleiding, persoonsbeveiliging en de mogelijkheid om bepaalde (semi-)automatische vuurwapens te gebruiken. Het gebruik van zware middelen, zoals een pantservoertuig of zeer zware geweldmiddelen, is voorbehouden aan de Kmar en bijzondere bijstandeenheden. Voor de inzet van de Kmar en bijzondere bijstandeenheden moet het lokaal gezag een verzoek tot bijstand indienen (via de reguliere bijstandsregeling, dus ofwel bij Justitie, ofwel bij de Commissaris van de Koningin).

Op basis van het Besluit beheer regionale politiekorpsen dienen regionale politiekorpsen zelfstandig of samen te beschikken over eenheden die werkzaamheden verrichten op het terrein van bewaken en beveiligen van personen, objecten en diensten (zoals mobiele eenheden, arrestatieteams en bijzondere bijstandeenheden). Ter uitvoering van hun taken kunnen de leden van de mobiele eenheden en de arrestatieteams onder meer bewapend worden met een semi-automatisch vuurwapen. Leden van arrestatieteams zijn daarenboven bewapend met automatisch vuur terwijl de leden van de bijzondere bijstandeenheden onder omstandigheden een vuurwapen kunnen gebruiken waarmee lange afstandsprecisievuur kan worden afgegeven.
Voor wat betreft persoonsbeveiliging opent het besluit de mogelijkheid dat de ministers eenheden aanwijzen, bestaande uit ambtenaren van politie van een of meer regionale korpsen, die zijn belast met het waken voor de veiligheid van de daartoe door het bevoegde gezag aangewezen personen. Daarvoor wordt per regio gemiddeld een aantal fte's ter beschikking gesteld. Wij denken aan een model waarbij korpsen gezamenlijk of centraal beschikken over een eenheid voor deze specialistische taken (vergelijkbaar met de arrestatieteams of via onderbrenging bij de KLPD). Over de uiteindelijke «modelkeuze» zullen de adviezen van het Korpsbeheerdersberaad (KBB), de Raad van Hoofdcommissarissen (RvHC) en het OM – Politieberaad richtinggevend zijn.

6.2 Rijksdomein

Ook voor het Rijksdomein geldt dat het lokaal bevoegd gezag verantwoor-

delijk is voor de uitvoering van de veiligheidsmaatregelen. Uitvoering van de maatregelen geschiedt door de regiopolitie. In voorkomende gevallen kan het lokale bevoegd gezag via de gebruikelijke procedure verzoeken om bijstand van andere regiokorpsen, het KLPD of de KMar, dan wel – in zeer bijzondere gevallen – van andere onderdelen van de krijgsmacht. Het onderscheid tussen bewaken en beveiligen heeft zijn belang verloren (zie paragraaf 1.4). Dit geldt ook voor de uitvoeringspraktijk, waar gewerkt wordt met een glijdende schaal van maatregelen. Daarbij geldt dat regiokorpsen meer veiligheidsmaatregelen ten aanzien van objecten moeten gaan uitvoeren. Hiervoor zijn overigens bepalingen in het Besluit Beheer Regionale Politiekorpsen opgenomen (ME, AT), maar deze worden niet of nauwelijks door de politie ingevuld of tot uitvoering gebracht.

De verantwoordelijkheid van de minister van BZK voor het rijksdomein zal tot uitdrukking worden gebracht in zijn aanwijzingsbevoegdheid jegens de burgemeesters. De huidige aanwijzingsbevoegdheid van de Minister van BZK (artikel 16, tweede lid, Politiewet 1993) heeft uitsluitend betrekking op het door de burgemeesters ter handhaving van de openbare orde te voeren beleid. Om zijn verantwoordelijkheid voor de veiligheid van objecten en diensten in het Rijksdomein te kunnen waarmaken, dient de minister van BZK ook de mogelijkheid te hebben de burgemeesters aanwijzingen te geven met betrekking tot de wijze waarop en de middelen waarmee zij de openbare orde moeten handhaven. De Politiewet 1993 zal in deze zin worden aangepast teneinde de minister in staat te stellen de aanwijzingsbevoegdheid, indien nodig, daadwerkelijk én effectief in te zetten voor bewaking en beveiliging. Indien op decentraal niveau niet genoeg capaciteit of middelen beschikbaar zijn voor het uitvoeren van een aanwijzing van de minister, kan deze op grond van artikel 55 Politiewet 1993 zelf voorzien in de benodigde bijstand. In gevallen met extreme geweldsdreiging kan de BBE of KMar op basis van daarvoor geldende regelingen worden ingezet. De belangrijkste argumenten om te kiezen voor de bestaande systematiek zijn:

- Geen systeem- en politiebestelwijziging;
- Toepassing glijdende schaal van maatregelen mogelijk;
- Huidige gezagsverdeling blijft bestaan.

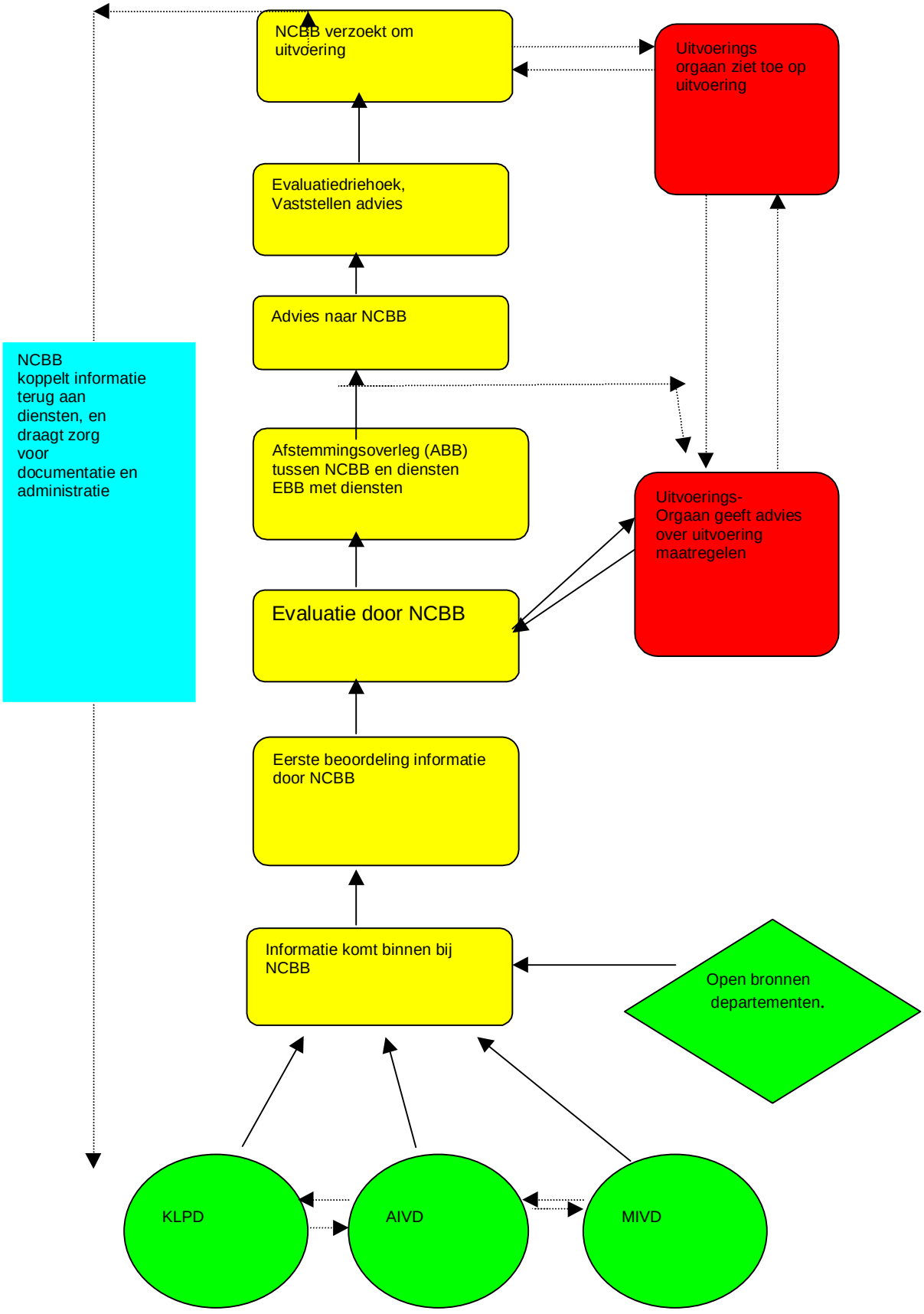
Voorwaarde hierbij is dat de politie adequaat is opgeleid, toegerust en geoefend om de bewakings- en beveiligingsstaken te kunnen uitvoeren. Hier zal door de politie nader inhoud aan moeten worden gegeven.

Uitvoeringsoverleg
Een apart in te stellen Uitvoeringsoverleg adviseert de NCBB over de uitvoering van de maatregelen. Het Uitvoeringsoverleg wordt voorgezeten door een functionaris van de NCBB, niet zijnde de NCBB zelf, en bestaat uit deskundigen van de Dienst Koninklijke en Diplomatieke Beveiliging (DKDB), de Dienst Specialistische Recherche Toepassingen (DSRT), de Koninklijke marechaussee (Kmar), de Brigade Speciale Beveiligingsopdrachten (BSB) en de regionale politiekorpsen. Het Uitvoeringsoverleg beziet enerzijds op welke wijze uitvoering wenselijk is maar kijkt anderzijds mede naar de haalbaarheid en effectiviteit. In navolging van de aanbevelingen van de Commissie van den Haak zal er sprake zijn van meer differentiatie, variatie en flexibiliteit bij de uitvoering van veiligheidsmaatregelen. Een overzicht van een glijdende schaal van maatregelen, oplopend van zeer licht tot zeer zwaar, zal worden gehanteerd als richtsnoer. Daarbij geldt dat het adviseren over maatregelen maatwerk is: elke situatie en mate van dreiging of risico vereist dikwijls andere maatregelen. Het Uitvoeringsoverleg maakt fysiek geen deel uit van de interne NCBB-organisatie. De leden zijn op afroep beschikbaar, waarbij als voorwaarde geldt dat zij uiterlijk binnen twee uur bij elkaar zijn voor overleg terzake.

Voor het Uitvoeringsoverleg is het van belang dat zo goed mogelijk wordt aangegeven wat de aard, ernst, omvang en waarschijnlijkheid van de dreiging is. Omwille van een goede uitvoering moeten de beschikbare gegevens over de bedreigde, bedreiger, locatie etcetera, zo veel mogelijk bij de leden van het Uitvoeringsoverleg bekend zijn.

Naast het adviseren over de uitvoering van maatregelen verzekert het Uitvoeringsoverleg zich ervan, namens de NCBB, dat de geadviseerde maatregelen op landelijk niveau worden uitgevoerd. In het zeer uitzonderlijke geval dat een regio weigert medewerking te verlenen kan de minister van BZK, zoals hiervoor uiteengezet, de burgemeester een aanwijzing geven, voorzover het betreft het door hem ter handhaving van de openbare orde te voeren beleid, bijvoorbeeld indien de veiligheid van de Staat in gevaar komt of de betrekkingen van Nederland met ander mogendheden dan wel zwaarwegende belangen van de samenleving kunnen worden geschaad (artikel 16, tweede lid, Politiewet 1993). Het uitvoeringsoverleg geeft een tijdige en adequate terugkoppeling over de uit te voeren en uitgevoerde maatregelen aan de NCBB. Terugkoppeling naar het onderhavig subject of object vindt plaats door de NCBB. Van belang daarbij is dat de medewerking van betrokkene essentieel is. Immers, zonder zijn of haar medewerking kan de overheid niet volledig invulling geven aan haar bijzondere verantwoordelijkheid. De NCBB draagt ten slotte zorg voor een administratieve afhandeling van de adviezen (registratie en documentatie).

Schematisch kan het proces van weging en besluitvorming voor het Rijksdomein als volgt worden weergegeven:


NCBB verzoekt om uitvoering
Uitvoerings orgaan ziet toe op uitvoering
Evaluatiedriehoek, Vaststellen advies
Advies naar NCBB
NCBB koppelt informatie terug aan diensten, en draagt zorg voor documentatie en administratie
Afstemmingsoverleg (ABB) tussen NCBB en diensten EBB met diensten
Uitvoerings- Orgaan geeft advies over uitvoering maatregelen
Evaluatie door NCBB
Eerste beoordeling informatie door NCBB
Informatie komt binnen bij NCBB
Open bronnen departementen.
KLPD
AIVD
MIVD

7 Implementatietraject nieuw samenhangend stelsel

Opgemerkt wordt dat sommige onderdelen van het implementatietraject van het nieuwe stelsel bewaken en beveiligen een langere looptijd zullen hebben dan andere en dat met het vaststellen van het nieuwe stelsel implementatie op onderdelen nog dient plaats te vinden. Aanpassing van wetgeving, organisatorische veranderingen, werven en opleiden en herinrichting van de werkprocessen vergen meer tijd. Dat geldt temeer omdat voor de uitvoering van bepaalde elementen van het nieuwe stelsel van bewaken en beveiligen aangesloten zal worden bij bredere (reeds lopende) trajecten zoals het landelijke project informatiecoördinatie en de wijzigingstrajecten van de WIV 2002 en de wet politieregisters.

8 Financiële consequenties

Het financieel beslag van dit nieuwe stelsel bewaken en beveiligen vormt onderdeel van de voorbereiding op de Rijksbegroting 2004.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
J. W. Remkes

De Minister van Justitie,
J. P. H. Donner

Lijst van afkortingen

ABB	Afstemmingsoverleg Bewaking en Beveiliging
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AT	Arrestatieteam
BBE	Bijzondere bijstandseenheid
BBRP	Besluit beheer regionale politiekorpsen
BOZ	Bureau Operationele Zaken van het directoraat-generaal Rechtshandhaving van het ministerie van Justitie
BSB	Brigade Speciale Beveiligingsopdrachten van de Koninklijke Marechaussee
BVA	Beveiligingsambtenaar
BZK	ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CIE	Criminele Inlichtingendienst Decentraal kan zowel regionaal als lokaal zijn
DGOOV	Directeur-generaal Openbare orde en Veiligheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties
DGRH	Directeur-generaal Rechtshandhaving van het ministerie van Justitie
DKDB	Dienst Koninklijke en Diplomatieke Beveiliging van het Korps landelijke politiediensten
DNP	De Nederlandse Politie in de context van het Landelijk-project informatiecoördinatie DNP
DSRT	Dienst Specialistische Recherche Toepassingen van het Korps landelijke politiediensten
EBB	Eenheid Bewaking en Beveiliging
ED	Evaluatiedriehoek die bestaat uit de Nationaal Coördinator Bewaking en Beveiliging, de directeur-generaal Rechtshandhaving van het ministerie van Justitie en de directeur-generaal Openbare orde en Veiligheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties
EO	Evaluatieoverleg
KBB	Korpsbeheerdersberaad
KLPD	Korps landelijke politiediensten
KMAR	Koninklijke Marechaussee
ME	Mobiele Eenheid
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
NBC	Nucleaire Biologische en Chemische wapens
NCBB	Nationale Coördinator Bewaking en Beveiliging
NCC	Nationaal Coördinatiecentrum
NIK	Nationaal Informatieknooppunt
NPI	Nederlands Politie Instituut
OM	Openbaar Ministerie
PG	Procureur-generaal
PW	Politiewet
RID	Regionale inlichtingendienst
RIK	Regionaal Informatieknooppunt
RvHC	Raad van Hoofdcommissarissen

TEC	Technische evaluatiecommissie
TUC	Technische uitvoeringscommissie
VIP	Very Important Person