



Adviescommissie toekomstbestendig stelsel bewaken en beveiligen

Oktober 2021



Voorwoord

‘Voorstellen doen om het stelsel bewaken en beveiligen toekomstbestendig te maken’, dit was de opdracht die de NCTV – als stelselverantwoordelijke namens de minister van Justitie en Veiligheid – aan de commissie meegaf. Het stelsel is de afgelopen jaren in rap tempo geconfronteerd met diverse ontwikkelingen in de dreiging. Bijvoorbeeld de verharding in de georganiseerde criminaliteit en de verlaging van de drempels voor het uiten van bedreigingen en het toepassen van geweld. Hierdoor moeten grotere én andere groepen personen en functionarissen worden beveiligd dan voorheen. Het stelsel in de huidige constellatie worstelt hoe hier mee om te gaan. In dat verband heeft de ministerie van Justitie en Veiligheid een onafhankelijke commissie gevraagd het huidige stelsel te beoordelen.

Het huidige stelsel is bijna twintig jaar geleden opgezet en was passend voor de dreiging in die tijd, maar is onvoldoende toegesneden op de hierboven geschetste ontwikkelingen. Het is belangrijk dat de doorontwikkeling van het stelsel krachtig ter hand wordt genomen, vooral gelet op het feit dat het stelsel al onder forse druk staat en alleszins te verwachten is dat dit de komende jaren niet zal afnemen. In dat verband wordt opgemerkt dat de aanbevelingen van de commissie aansluiten bij de knelpunten die vanuit de praktijk zijn aangedragen.

De commissie wenst allen veel wijsheid toe bij deze buitengewoon belangrijke taak.

Gertjan Bos

Voorzitter adviescommissie toekomstbestendig stelsel bewaken en beveiligen

Samenstelling van de commissie

J.G. Bos (voorzitter)
M.A. Bernds-Jansen (lid)
J.J. van Eck (lid)

Staf van de commissie

A. Jagan (secretaris)
D.W.P. van Loon

Inhoudsopgave

DEEL I - Samenvatting, conclusies en aanbevelingen	7
DEEL II - Context: de opdracht, het stelsel op papier en de verwachte dreigingsontwikkeling	14
Hoofdstuk 1. Aanleiding, opdracht en verantwoording	15
Hoofdstuk 2. Het stelsel	20
Hoofdstuk 3. Dreigingsontwikkeling	30
DEEL III - Het stelsel in de praktijk	36
Hoofdstuk 4. Uitgangspunten stelsel	38
Hoofdstuk 5. Inrichting en sturing	43
Hoofdstuk 6. Kwaliteit	48
Hoofdstuk 7. Informatiepositie	50
Hoofdstuk 8. Uitvoering	54
Hoofdstuk 9. Perspectief van een Te Beveiligen Persoon	57
DEEL IV - Bijlagen	60
Instellingsbesluit	61
Samenstelling commissie, staf en klankbordgroep	64
Lijst respondenten	65
Geraadpleegde bronnen	66
Lijst met afkortingen	67
Rapport dreigingsontwikkelingen Universiteit Leiden	69

Deel I



Samenvatting, conclusies en aanbevelingen

Inleiding

De overheid draagt zorg voor de bescherming en beveiliging van personen, objecten en diensten die worden bedreigd. Dit wordt gedaan binnen het zogenoemde Stelsel Bewaken en Beveiligen, een samenwerkingsverband van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), het Openbaar Ministerie (OM), de Politie, de Koninklijke Marechaussee (KMar), de Algemene Inlichtingen en Veiligheidsdienst (AIVD), de Militaire Inlichtingen en Veiligheidsdienst (MIVD) en burgemeesters.

Achter de afgeschermd bewakings- en beveiligingstaak ligt een omvangrijke praktijk waar impactvolle en afbreukgevoelige afwegingen en keuzes gemaakt worden. Het is daarom cruciaal dat periodiek op dit complexe systeem gereflecteerd wordt, om zo te bepalen of dit nog past bij de actuele en verwachte dreigingen en uitdagingen. De urgentie is alleen maar groter geworden door de druk die op het stelsel is komen te staan. Het aantal personen en objecten dat langdurig en intensief bewaakt en beveiligd wordt is de afgelopen jaren toegenomen en zal naar verwachting niet verminderen. De commissie is gevraagd om te reflecteren op het stelsel en voorstellen te doen om het stelsel toekomstbestendig te maken.

Opdracht en werkwijze

‘Om blijvend het hoofd te kunnen bieden aan huidige en toekomstige dreigingen in een complexer geworden samenleving laat ik een onafhankelijke commissie het stelsel bewaken en beveiligen beoordelen en voorstellen doen om het toekomstbestendig te maken. Ik zal uw Kamer informeren over de uitkomsten.’¹

Om deze brede vraag te beantwoorden, heeft de commissie gesproken met een groot aantal functionarissen (van operationeel tot en met strategisch niveau) en experts. Ook heeft er een brede documentanalyse plaatsgevonden. Ten behoeve van deze analyse hebben stelselpartners position papers aangeleverd waarin zij hun visie op een toekomstig stelsel beschrijven. Op basis hiervan is een aantal onderwerpen gedestilleerd die het fundament van het stelsel vormen en waar de commissie haar advies op richt. Het gaat dan om:

- De ontwikkelingen in de dreiging en de (verwachte) uitdagingen waar een toekomstbestendig stelsel op voorbereid moet zijn;
- De uitgangspunten, regelgeving en aannames die ten grondslag liggen aan het stelsel;
- De wijze waarop het stelsel is ingericht en wordt aangestuurd;
- De kwaliteit van de taakuitvoering binnen (processtappen van) het stelsel;
- De informatiepositie op basis waarvan dreigingsinschattingen worden gemaakt om tot de juiste beveiligingsmaatregelen te komen;
- De wijze waarop de beveiligingsmaatregelen in de praktijk worden uitgevoerd;
- De wijze waarop het perspectief van een te beveiligen persoon in een toekomstbestendig stelsel kan worden verwerkt.

Uit gesprekken met betrokken functionarissen en door stelselpartners aangeleverde documentatie is gebleken dat op dit moment de meeste – en urgente – vraagstukken zich concentreren op het gebied van beveiliging van personen. De primaire focus van het rapport is dan ook daarop gericht.

De commissie richt zich met name op de werkwijze en praktijk van het stelsel. Vanuit dat perspectief dient het rapport gezien te worden. Het stelsel vormt slechts één instrument in een breder palet om aan dreigingen tegen personen en objecten het hoofd te bieden. Daarnaast ligt er onder andere een belangrijke rol voor de verschillende aanpakken gericht op de dreiger of dader. Door een efficiënte inzet op de dreiger, kan de druk op het stelsel verminderd worden.

¹ Brief van de regering, *Voortgang aanpak ondermijnende criminaliteit*, 13 november 2020.

Hoofdboodschap

Ontwikkelingen in de dreiging volgen zich in een rap tempo op, wat grote consequenties heeft voor het stelsel. Op dit moment staat het stelsel onder hoge (operationele) druk, waarbij het geconfronteerd wordt met complexe en langdurige zaken. Het stelsel krijgt hierdoor steeds vaker te maken met vraagstukken waar het niet altijd een uniform, efficiënt en flexibel antwoord op heeft. Het stelsel is in de huidige constellatie niet in staat gebleken om zichzelf door te ontwikkelen. Het stelsel is door de urgentie van de dagelijkse operationele actualiteit steeds meer reactief gaan werken en zoekt antwoorden en oplossingen in de waan van de dag. Hierdoor blijft er zeer beperkte ruimte over om ervaren knelpunten in samenhang te bezien en te werken aan kwaliteitsverbetering en innovatie.

De overheid draagt, in aanvulling op de eigen en werkgeversverantwoordelijkheid, een verantwoordelijkheid voor het waarborgen van de fysieke veiligheid van burgers. Deze verantwoordelijkheid dient zichtbaar te zijn in de manier waarop organisaties deze taak organiseren en gezamenlijk uitvoeren. De casuïstiek toont aan dat het proces bewaken en beveiligen niet gezien kan worden als neventaak, maar als volwaardige hoofdtaak moet worden opgepakt. In dit opzicht moet het stelsel een volgende stap in de professionalisering maken. Er ligt daarnaast een belangrijke opgave om het stelsel als geheel te versterken.

Het stelsel is in zijn algemeenheid logisch en goed onderbouwd ingericht en de gedachten erachter zijn goed te volgen, maar is onvoldoende toegerust om aan de huidige en toekomstige uitdagingen het hoofd te kunnen bieden. De indeling rijksdomein – decentraal domein heeft zijn nut bewezen en de positie van de deelnemende partners kan in essentie dezelfde blijven. Vanuit het huidige fundament dient nu een transitie plaats te vinden van een reactief, vraaggericht en bestuurlijk versnipperd stelsel naar een flexibel, proactief en uniform stelsel. Hiervoor is geen grootschalige reorganisatie nodig, maar dienen gerichte versterkingen te worden aangebracht. Dit vergt scherpe keuzes. In de kern gaat het daarbij om een krachtige en robuuste aansturing, verscherping van een aantal (beleids)uitgangspunten, een sterkere informatiepositie met de inzet om meer aan de voorkant van de dreiging te komen, synergie en innovatie in de uitvoering van beveiligingsopdrachten en kwaliteitsborging.

Conclusies en aanbevelingen

Dreigingsontwikkeling

Om te kunnen adviseren over een toekomstbestendig stelsel bewaken en beveiligen, is het noodzakelijk om inzicht te krijgen in de dreigingsontwikkeling. In opdracht van de commissie is een wetenschappelijke verkenning uitgevoerd naar de dreigingsontwikkeling in de afgelopen jaren en een analyse van de verwachte ontwikkelingen de komende jaren. Het hieruit ontstane beeld werd gecompleteerd met inzichten vanuit het werkveld. Op basis van wat vanuit de wetenschappelijke studie en het werkveld is aangereikt, zijn de volgende inhoudelijke opgaven gedestilleerd waarop het stelsel een antwoord moet vinden.

Een toekomstbestendig stelsel moet de flexibiliteit bevatten om snel te kunnen inspelen op (nieuwe) dreigingsontwikkelingen. Hiervoor is het nodig dat het stelsel qua informatiepositie en analysevermogen zoveel mogelijk aan de voorkant komt van de ontwikkelingen. Daarnaast is het nodig dat in het stelsel kritische distantie en reflectievermogen is ingebouwd, om bedreigingen en de noodzakelijke respons vanuit het stelsel in proportie te zien en ontwikkelingen in hun juiste historische context te plaatsen, zodat zowel een overreactie als een onderschatting van dreigingen zoveel mogelijk wordt voorkomen.

Het is alleszins aannemelijk dat het aantal personen en objecten dat langdurig bewaakt en beveiligd moeten worden, zal toenemen. Een belangrijke oorzaak is de verharding van de georganiseerde criminaliteit. De geweldsdrempel is verlaagd en traditionele demarcatielijnen (qua doelwit-categorieën) lijken te worden doorbroken. Daarnaast is de verwachting dat de komende jaren meer grote strafprocessen zullen plaatsvinden. Dit zal een beslag leggen op het stelsel bewaken en beveiligen. Het stelsel zal verder meer moeten worden toegesneden op digitale dreigingen. Daarbij gaat het met name om de digitale dreiging als opmaat naar fysieke dreiging. Digitale activiteiten op een persoon of object horen in dat kader expliciet als indicator in een dreigingsanalyse aan de orde te komen, zodat ze integraal kunnen worden meegewogen. Hierdoor kan een completere dreigingsanalyse worden opgesteld. Daartoe zullen de capaciteiten van het stelsel, met name de expertise van analisten en uitvoerders, moeten worden versterkt. Ten slotte is de verwachting dat de dreiging vanuit statelijke actoren zal toenemen.

Aanbevelingen

- Ga uit van een toename van het aantal grote strafprocessen dat gepaard gaat met grootschalige beveiligingsoperaties en richt de capaciteit (kwalitatief en kwantitatief) daarop in.
- Versterk de capaciteiten van het stelsel zodanig dat ook de digitale opmaat naar fysieke dreiging wordt meegenomen in analyse en uitvoering.
- Bouw flexibiliteit in het stelsel opdat nieuwe ontwikkelingen in het dreigingsbeeld zo snel mogelijk kunnen worden opgevangen.

Uitgangspunten

Het huidige stelsel is voornamelijk gebouwd op de uitgangspunten en werkafspraken die in de circulaire bewaken en beveiligen zijn beschreven. Ofschoon de circulaire logisch is ingericht, is zij op sommige onderdelen te globaal geformuleerd en biedt zij onvoldoende houvast bij inhoudelijke vraagstukken. Het gaat hierbij met name over vraagstukken die samenhangen met de begrenzing van het stelsel, de verantwoordelijkheidsverdeling en de reikwijdte van de zorgplicht van de overheid. Functionarissen binnen het stelsel moeten daardoor naar eigen inzicht invulling hieraan geven. Dit gaat ten koste van consistentie van beveiligingsmaatregelen, waardoor er variatie en niet-uitlegbare verschillen ontstaan. Om tot een toekomstbestendig stelsel te komen, is het nodig dat de uitgangspunten worden gepreciseerd en verhelderd. Hiervoor is nodig dat duidelijk keuzes gemaakt worden.

Aanbevelingen

- Concretiseer de huidige uitgangspunten met betrekking tot de zorgplicht van de overheid in de circulaire. Maak daarin duidelijk:
 - dat het stelsel er in beginsel is voor iedereen;
 - dat het doel van het stelsel is het waarborgen van de fysieke veiligheid voor personen, objecten en diensten;
 - dat het stelsel uitgaat van een complementaire verantwoordelijkheidsverdeling tussen de te beveiligen persoon, de werkgever en de overheid. Neem daarin ook de rol van de betrokken brancheorganisaties op.
 - dat sprake is van risicobeheersing, niet van risico-uitsluiting.
 - dat de volledige en onbelemmerde voortzetting van particulier en zakelijk functioneren niet kan worden gewaarborgd met dien verstande:
 - dat voor een beperkt aantal functies, in ieder geval die behoren tot de kern van de democratische rechtsorde, het stelsel zoveel mogelijk het onbelemmerd uitoefenen van de functie mogelijk moet maken.
- Stel, aan de hand van dreigingsniveau's en dreigings-inschattingen, standaard (vaste) beveiligingspakketten samen voor categorieën te beveiligen personen. Neem in die pakketten op de criteria en de procedure voor het afbouwen en

beëindigen van de maatregelen. Hiermee wordt mede invulling gegeven aan de zorgplicht van de overheid.

- Zorg voor afstemming tussen de stelsels bewaken en beveiligen en getuigenbescherming. Dit dient in ieder geval te resulteren in een nadere grensmarkering tussen de stelsels.

Sturing

Om de vraagstukken die op het stelsel afkomen eenduidig en snel op te kunnen pakken, is het noodzakelijk om de governance van het stelsel op landelijk niveau zo te organiseren dat wordt voorzien in krachtige, integrale sturing. Het stelsel kent momenteel een breed scala aan overlegstructuren, maar van integrale sturing is nog geen sprake. Knelpunten worden in deze overleggen geadresseerd, maar voornamelijk vanuit monodisciplinair perspectief aangevlogen. Het ontbreekt daarnaast aan relevante sturingsinformatie waardoor er geen overzicht en inzicht is.

Aanbevelingen

- Richt een centrale aansturingsstructuur van het stelsel in. Betrek daarbij de volgende elementen:
 - Een *Vierhoek bewaken en beveiligen* voor de strategische besluitvorming en het meerjarenbeleid. In deze vierhoek nemen zitting: De portefeuillehouder Bewaken en Beveiligen in het College van procureurs-generaal, de NCTV (voorzitter), de Korpschef van de politie en de Commandant KMar.
 - Een *Uitvoeringsorgaan bewaken en beveiligen* voor de dagelijkse aansturing van het stelsel. Hierin nemen zitting alle portefeuillehouders bewaken en beveiligen van de stelselpartners, te weten OM, NCTV (voorzitter en de CBB), Politie, KMar, AIVD en MIVD.
 - Een gekwalificeerd *bestuurssecretariaat* dat beide gremia inhoudelijk voorbereidt.
 - Een *Kenniscentrum bewaken en beveiligen* dat fungeert als expertiseplatform voor het gehele stelsel. Hieraan is tevens een wetenschappelijk netwerk gekoppeld.
- Beleg de aanbevelingen van dit rapport in een strategische agenda van de Vierhoek voor de komende twee jaar.
- Zorg ervoor dat alle voor de sturing benodigde informatie geactualiseerd beschikbaar is in de vorm van een dashboard bewaken en beveiligen. In dit dashboard worden in elk geval opgenomen het landelijk dreigingsbeeld, een landelijk overzicht van de casuïstiek, een overzicht van ingezette en beschikbare capaciteit, de voortgang inzake de kwaliteitsontwikkeling en de innovatie- en ontwikkelingsagenda.
- Bestendig de bestaande opschalingsstructuur voor grote, complexe, regio-overstijgende zaken. Voorzie binnen die structuur in een coördinator uitvoering en een informatiecoördinator van de Politie en beleg daarbij het gezag weer bij het Openbaar Ministerie.

- Breng een scheiding aan tussen de operationele rol van de NCTV en zijn verantwoordelijkheid voor het stelsel als geheel. Beleg die taken bij afzonderlijke functionarissen.
- Bevorder de rolvastheid bij het Openbaar Ministerie. De hoofdofficier van Justitie dient in zijn gezagsrol te blijven, waarbij de politie verantwoordelijk is voor de uitvoering.
- Beleg de taak van bewaken en beveiligen op het niveau van de eenheidsleiding van de Politie.
- Investeer in de taak van de portefeuillehouder beleid bewaken en beveiligen van het Openbaar Ministerie en versterk zijn rol in de kwaliteitsbewaking en bevordering van uniformiteit in de taakuitvoering van de parketten.

Kwaliteit

Bewaken en beveiligen is bij een groot deel van betrokken organisaties tot op heden veelal een neventaak geweest, niet alleen op operationeel niveau, maar ook op het strategisch niveau. Mede hierdoor is het vakgebied bewaken en beveiligen niet ten volle en op alle niveaus tot ontwikkeling gekomen. Met de veranderende dreiging en de toename van het volume aan (complexe) casussen, kan een toekomstbestendig stelsel niet meer als neventaak opgepakt worden. Alle betrokken stelselpartners moeten investeren in hun eigen organisatie om het vakgebied verder te ontwikkelen. Met het thans ingezette versterkingstraject is een eerste aanzet gegeven, maar er zijn meer stappen nodig.

Aanbevelingen

- Richt bewaken en beveiligen als hoofdtaak in en borg dit binnen de eigen organisatie
- Formuleer kwaliteitsnormen voor producten en processen binnen het stelsel en stuur hierop.
- Richt een evaluatiefunctie in zodat structureel lerend vermogen in het stelsel wordt opgebouwd.
- Borg de capaciteiten en middelen die vanuit het versterkingstraject beschikbaar zijn gesteld en bewaak de besteding van die middelen voor het bestemde doel. Maak inzichtelijk hoe de middelen zijn besteed.

Informatiepositie

De informatiepositie is cruciaal binnen het stelsel. Op basis hiervan worden de dreigingsinschattingen gemaakt en wordt beoordeeld welke maatregelen nodig zijn. De huidige informatiepositie voldoet echter in toenemende mate niet meer aan de behoefte van de praktijk, waarin de dreiging complexer en ongrijpbaarder is geworden. De informatiepositie is reactief en vraaggericht. Voor een toekomstbestendig stelsel is nodig dat de informatiepositie een transitie doormaakt van voorstelbaarheid naar voorspelbaarheid. De praktijk wordt daarbij geconfronteerd met een aantal knelpunten. Zo blijkt dat de huidige wetgeving het lastig maakt om informatie te mogen verzamelen ten behoeve van bewaken en beveiligen. Daarnaast zijn er belemmeringen in de informatiedeling en samenwerking tussen organisaties, en belemmeringen in de methodieken en technieken om nieuwe typen dreigingen te kunnen duiden. Er liggen derhalve grote opgaves om deze informatiepositie te versterken.

Aanbevelingen

- Om meer aan de voorkant van de dreiging te kunnen komen is het nodig dat informatieproducten, werkwijzen, (analyse)methoden en technieken worden geïnnoveerd. Voorstelbare dreigingen moeten voorspelbaar gemaakt worden, zodat er meer proactief geacteerd kan worden.
- Richt een informatieplatform in waarin alle informatieonderdelen van de politie stelselrelevante informatie uitwisselen zodat een volledig en gestapeld beeld ontstaat.
- Zorg dat bewaken en beveiligen als proces goed is aangesloten op andere hoofdprocessen binnen de politie, zodat relevante informatie tijdig bij de juiste functionarissen terecht komt. Voeg bij (grootschalig) opsporingsonderzoeken die risico's bevatten in de sfeer van bewaken en beveiligen een analist toe aan het opsporingsteam die meekijkt vanuit de optiek van bewaken en beveiligen en die zorgt voor het doorgeleiden van relevante informatie.
- Laat met hoge prioriteit een juridisch onderzoek uitvoeren naar de vraag in hoeverre de wettelijke bevoegdheden voor informatieverzameling ten behoeve van bewaken en beveiligen moeten worden verruimd. Daarbij gaat het met name om:
 - Stelselmatig onderzoek in open bronnen (om onder andere trends eerder te duiden);
 - Informatie die ten behoeve van bewaken en beveiligen beschikbaar moet komen buiten en na afronding van het opsporingsonderzoek;
 - Betrek daarbij de aanbevelingen die zijn gedaan door de commissie van de Haak uit 2002, waaronder de mogelijkheid voor 'protective intelligence'.
- Verhelder in de Circulaire bewaken en beveiligen, en waar nodig in de Wet op de Inlichtingen- en veiligheidsdiensten, de positie van de AIVD en MIVD in het doorgeleiden van relevante informatie naar de decentrale autoriteiten.

Uitvoering

Gezien de in dit rapport geschetste ontwikkelingen, mag verwacht worden dat de druk op het stelsel de komende jaren blijft toenemen. Het is daarbij aannemelijk dat het stelsel zal worden geconfronteerd met een capaciteitsprobleem waar de recent toegekende versterking maar ten dele in voorziet. Los van dit capaciteitsprobleem, is het in ieder geval zaak om efficiënt, flexibel en innovatief gebruik te maken van het bestaande potentieel. Daarbij is aan de orde het intensiveren van de samenwerking van de stelselpartners, het actief gebruik maken van een flexibele schil van (publiek/private) partners en meer inzet van technologische middelen.

Aanbevelingen

- Intensiveer de samenwerking tussen de twee uitvoerende organisaties, politie en KMar. Die versterkte samenwerking geldt in ieder geval voor de volgende gebieden:
 - Uitvoering: ontwikkel op basis van gelijkwaardigheid en vanuit eigen unieke kwaliteiten, gezamenlijk een breed palet aan beveiligingsconcepten.
 - Opleiding: ontwikkel zoveel mogelijk gezamenlijk opleidingen en trainingen zodat functionarissen zoveel mogelijk inzetbaar zijn in alle concepten.
 - Innovatie: stel een gezamenlijke innovatieagenda op, waarin de kennis en expertise van beide organisaties worden gebundeld.
- Versterk de personele capaciteit van het stelsel door samenwerking en inschakeling van de particuliere sector. Ontwikkel daarvoor beveiligingsconcepten waarbij bepaalde taken door private organisaties kunnen worden uitgevoerd. Als voorwaarde geldt dat het geweldsmonopolie blijft berusten bij de overheid, dat de taakuitvoering valt onder het bevoegd gezag en onder regie van de politie en dat de particuliere inzet voldoet aan certificerings- en opleidingseisen.
- Maak (meer) gebruik van geavanceerde digitale en nieuwe technologische middelen bij (de ontwikkeling van) beveiligingsconcepten.
- Maak de gezamenlijk beschikbare capaciteiten en middelen inzichtelijk, om zo een landelijk overzicht te hebben op basis waarvan op capaciteit kan worden gestuurd.

Perspectief van een te beveiligen persoon

Het is van groot belang om het perspectief van een beveiligde persoon te betrekken bij het eigen beveiligingsconcept. Het ondergaan van een beveiligingsregime heeft (forse) impact op iemands leven. Zet daarom in op psychosociale zorg en het ondersteunen van weerbaarheid van de te beveiligen persoon. De communicatie met de te beveiligen persoon kan worden verbeterd. Een investering in deze elementen draagt ook bij aan het effectiever uitvoeren van het beveiligingsconcept.

Aanbevelingen

- Investeer in het (preventief) weerbaarder maken van functionarissen die te maken kunnen krijgen met bedreigingen.
- Geef de te beveiligen persoon een plaats in het beveiligingsconcept.
- Zorg ervoor dat psychosociale (na)zorg een structureel onderdeel is van het beveiligingspakket. Afhankelijk van de behoefte van de beveiligde persoon kan dit nader ingevuld worden.
- Wees zoveel mogelijk transparant in de communicatie en wijs – naar analogie van de familierechercheur bij de politie – een vast aanspreekpunt aan.

Tot slot

Een gezamenlijke opgave vanuit één stelselperspectief

Het stelsel staat voor grote uitdagingen en de noodzaak voor verbetering is urgent. De commissie stelt geen grote reorganisatie voor maar er zijn forse stappen nodig. Die kunnen worden gezet met inachtneming van het huidige fundament van het stelsel. Om het stelsel verder te brengen en het toekomstbestendig te maken, is het van groot belang dat de betrokken organisaties vanuit een gezamenlijk stelselperspectief opereren en werken aan synergie. Organisaties dienen vanuit hun eigen kracht elkaar aan te vullen. Met monodisciplinair domein-denken kan niet meer worden volstaan.

Urgentiebesef en daadkracht bij implementatie

De stelselonderdelen die de commissie heeft onderzocht zijn onlosmakelijk met elkaar verbonden. Dat betekent dat de aanbevelingen ook in samenhang moeten worden uitgevoerd. Dit leidt tot een forse opgave waarbij de uitvoering en ontwikkeling veel aandacht en intensieve inspanning zal vergen. De aanbevelingen moeten worden vertaald in een strategische ontwikkelagenda voor de komende twee jaar.

Gelet op het grote belang dat hiermee gemoeid is, ziet de commissie een verantwoordelijkheid en dragende rol voor de Vierhoek bewaken en beveiligen, waarbij de stelselverantwoordelijke namens de minister van Justitie en Veiligheid, de NCTV, het voortouw dient te nemen. Het doorvoeren van de

ontwikkelagenda vraagt daarnaast om een forse inspanning en intensieve samenwerking van de leden van het Uitvoeringsorgaan. Ten slotte is nodig om krachtige en gekwalificeerde ondersteuning te organiseren, die zich concentreert op deze doorontwikkeling.

Wat betreft het algemene kader en de uitgangspunten van het stelsel constateert de commissie dat de huidige wet- en regelgeving vooralsnog voldoende basis biedt. Wel ziet zij de noodzaak voor het verstevigen van enkele beleidskaders, die thans zijn neergelegd in de circulaire. De commissie adviseert om te onderzoeken of het op termijn nodig is om het stelsel beter wettelijk te verankeren, mede gelet op de impact van de maatregelen. Voor het versterken van de informatiepositie binnen het stelsel zijn mogelijk wetsaanpassingen nodig. Dit zal uit de aanbevolen juridisch verkenning moeten blijken.

Afsluitend

De afgelopen jaren is een groot beroep gedaan op de professionaliteit, loyaliteit en improvisatievermogen van functionarissen binnen het stelsel. De commissie heeft grote waardering voor de inzet van alle functionarissen die zijn betrokken bij de voorbereiding en uitvoering van het stelsel. De kritische observaties die in dit advies zijn gemaakt doen daar op geen enkele wijze afbreuk aan. De conclusies die de commissie trekt zijn niet gericht op deze functionarissen, maar op het systeem waarbinnen zij functioneren. En dat systeem is aan een herijking toe. Met het schetsen van een probleemanalyse, het beschrijven van verschillende oplossingsrichtingen en het formuleren van een aantal concrete aanbevelingen, hoopt de commissie de handvatten te hebben geboden om deze herijking vorm te geven.

Deel II

Context: de opdracht,
het stelsel op papier en
de verwachte dreigings-
ontwikkeling



Hoofdstuk 1

Aanleiding, opdracht en verantwoording

1.1 Inleidend

“Om blijvend het hoofd te kunnen bieden aan huidige en toekomstige dreigingen in een complexer geworden samenleving laat ik een onafhankelijke commissie het stelsel bewaken en beveiligen beoordelen en voorstellen doen om het toekomstbestendig te maken. Ik zal uw Kamer informeren over de uitkomsten.”²

De overheid draagt zorg voor de bescherming en beveiliging van personen, objecten en diensten die worden bedreigd, voor zover ze dat niet zelf kunnen doen. Dit wordt gedaan binnen het zogenoemde Stelsel bewaken en beveiligen: een samenwerkingsverband van de Nationaal Coördinator Terrorismedebijding en Veiligheid (NCTV), het Openbaar Ministerie (OM), de Politie, de Koninklijke Marechaussee (KMar), de Algemene Inlichtingen en Veiligheidsdienst (AIVD), de Militaire Inlichtingen en Veiligheidsdienst (MIVD) en bestuurlijke organisaties. Het stelsel bewaken en beveiligen is gebouwd op een verzameling van regelgeving en (werk)afspraken die gaan over het voorkomen van aanslagen op personen, objecten en diensten. In het stelsel is geregeld hoe op basis van dreiging en risico-informatie tot beveiligingsmaatregelen wordt besloten en wie verantwoordelijk is voor de uitvoering. De minister van Justitie en Veiligheid (JenV) is verantwoordelijk voor het stelsel.

Het aantal personen en objecten dat langdurig en intensief bewaakt en beveiligd wordt, is toegenomen en zal naar verwachting niet verminderen.³ Veranderingen in de dreiging en maatschappelijke ontwikkelingen leiden ertoe dat het stelsel geconfronteerd wordt met vraagstukken waar het nog niet op voorbereid was. In zijn brief stelt de minister van JenV dat door een aantal gebeurtenissen de druk op het stelsel alleen maar is toegenomen. De ‘bewaken en beveiligen-zaken’ zijn de afgelopen jaren complexer, langduriger en extremer in omvang en ernst geworden. Zo is excessief geweld tegen de dragers van onze democratische instituties vanuit criminele netwerken geen taboe meer. Steeds vaker doen zich ook zaken voor waarin statelijke actoren een dreiging voor een individu in Nederland vormen. Ten slotte komen digitale dreigingen ook steeds vaker voor.

Het kabinet heeft zich ten doel gesteld om het Stelsel bewaken en beveiligen te versterken. Dit wordt onder andere gedaan door capaciteit en middelen toe te kennen aan stelselpartners (‘versterking van de uitvoering’). Ook wordt gewerkt aan kwaliteitsverbetering (‘versterking van het stelsel’). In dat kader past ook de vraag of (de werkwijze in) het stelsel nog op de meest effectieve en efficiënte manier is georganiseerd om het hoofd te bieden aan huidige en toekomstige dreigingen en vraagstukken. De minister van JenV heeft daarop het ‘Adviescollege Toekomstbestendig Stelsel Bewaken en Beveiligen’ (hierna: de commissie) ingesteld⁴ en haar gevraagd te reflecteren op het stelsel en voorstellen te doen om het toekomstbestendig te maken.

² Brief van de regering, *Voortgang aanpak ondermijnende criminaliteit*, 13 november 2020.

³ Idem.

⁴ Instellingsbesluit in de bijlage.

1.2 Samenstelling college

De minister van JenV is verantwoordelijk voor het functioneren van het stelsel bewaken en beveiligen. Hij heeft zijn bevoegdheden gemandateerd aan de NCTV. Vanuit de rol van 'stelselverantwoordelijke' fungeert de NCTV, namens de minister, als opdrachtgever voor de commissie. Conform de richtlijnen voor adviescolleges is eerst de voorzitter van de commissie aangesteld, die vervolgens de andere leden van de commissie heeft aangezocht. De commissie bestaat daarmee uit:

- J.G. Bos (voorzitter)
- M.A. Berndsen-Jansen
- J.J. van Eck

De staf van de commissie bestaat uit A. Jagan (secretaris) en D.W.P. van Loon.

1.3 Opdracht

1.3.1 Verdieping en afbakening van de opdracht

Opdrachtformulering

De commissie heeft een brede opdracht gekregen: het beoordelen van het stelsel en voorstellen doen om het toekomstbestendig te maken. Daarbij heeft de minister geen inhoudelijke restricties gesteld en is de commissie vrij in de concrete invulling van de opdracht. De commissie richt zich op een toekomstbestendig stelsel door te kijken naar de inrichting van het stelsel als lerend geheel, dat bestand is tegen de uitdagingen in de nabije toekomst, waarbij flexibel kan worden gereageerd op nieuwe ontwikkelingen. Daarom wordt in dit advies het fundament van een toekomstbestendig stelsel beschreven, met daarbij het uitgangspunt dat het stelsel een continu lerende organisatie wordt, waarbij evaluatie leidt tot bijsturing van beleid en uitvoering.

Gezien de urgentie van het onderwerp is oorspronkelijk de wens uitgesproken uiterlijk 1 juli 2021 te rapporteren over de eerste bevindingen. Tijdens de eerste fase van het onderzoek bleek dat het onderzoek in verband met de breedte en complexiteit meer tijd vergde. De commissie verzocht de opdrachtgever om de opleverdatum uit te stellen tot oktober 2021, waarin is bewilligd.

Veldconsultatie

De opdracht van de minister is besproken in de stuurgroep bewaken en beveiligen. Dit gremium bestaat uit de strategische leiding (directeuren en portefeuillehouders) van de stelselpartners en staat onder voorzitterschap van de NCTV. De Stuurgroep heeft aangegeven wat vanuit het werkveld de belangrijkste thema's zijn en aan welke randvoorwaarden een toekomstbestendig stelsel zou moeten voldoen. Deze onderwerpen zijn aan de commissie meegegeven met het verzoek ze te betrekken bij het formuleren van haar advies:

- Het mogelijk maken om op basis van fenomenen of veronderstelde dreigingen vooraf een taxatie/inschatting te kunnen maken om op basis daarvan proactief maatregelen te kunnen treffen / strategie te bepalen.
- Binding houden met de specifieke lokale casuïstiek en tegelijkertijd in staat zijn om op te schalen bij complexe, gezag- en territorium overstijgende casussen.
- De aansturing vereenvoudigen in geval van de hiervoor genoemde opschaling.
- Ruimte bieden voor maatwerk in de uitvoering en tegelijkertijd zorgen voor uniformiteit in de kwaliteit. Het mag niet uitmaken waar een betrokkene slachtoffer is van bedreiging voor de mate van succes waarmee risicomanagement plaatsvindt;
- Een goede informatiepositie garanderen zodat het ook mogelijk wordt om strategisch en proactief te handelen;
- Een flexibele inzet garanderen, met een diversiteit aan beveiligingsconcepten zodat maatwerk mogelijk is en het gezag gerichtere strategische besluiten kan nemen.
- Gebruik maken van zowel publieke als private middelen en waar mogelijk vormen van publiek-private samenwerking aanmoedigen.
- Voorspellend en adaptief vermogen hebben om snel in te spelen op nieuwe dreigingen die nog niet goed in het Stelsel zijn geborgd (zoals digitale dreiging en spionage);
- Bevordering doelmatige inzet van capaciteit en middelen door doorontwikkeling van het stelsel.

De commissie heeft in de gesprekken met functionarissen veel waardevolle informatie en inzichten uit het veld opgehaald. Ook hechtte de commissie grote waarde aan het betrekken van de stakeholders in dit traject, om de bevindingen te valideren en inzichten te toetsen en te verrijken. Dit moet ertoe leiden dat het advies van de commissie voortvarend opgepakt kan worden en het stelsel op korte termijn kan worden versterkt.

Afbakening

In dit onderzoek wordt een afbakening gemaakt tussen het stelsel bewaken en beveiligen en het stelsel van getuigenbescherming. Hoewel er op sommige punten overlap is tussen beide stelsels, zijn de verschillen te groot om in één onderzoek te behandelen. Het stelsel van getuigenbescherming betreft het beveiligen van personen (getuigen en spijtoptanten) die gevaar lopen omdat zij medewerking verlenen aan Politie en Justitie in het kader van een strafrechtelijk onderzoek. Dit heeft een andere dynamiek en leidt tot andere type vraagstukken dan binnen het stelsel bewaken en beveiligen, dat bedoeld is om iedere burger bescherming te bieden als daar een dreiging op is.

Een andere afbakening betreft de primaire focus van het onderzoek. Het stelsel bewaken en beveiligen is een omvangrijk geheel, met daarbinnen enkele specifieke taakgebieden zoals persoonsbeveiliging, objectbeveiliging en de beveiliging van de burgerluchtvaart. Het is de commissie – uit gesprekken met betrokken functionarissen en door stelselpartners aangeleverde documentatie – vooral gebleken dat op dit moment de meeste – en urgente – vraagstukken zich concentreren op het gebied van beveiliging van personen, derhalve ligt het accent van dit advies met name hierop. De primaire focus van het rapport is dan ook daarop gericht.

1.3.2 De opdracht binnen de huidige context

De commissie verrichtte haar activiteiten in een tijd waarin het stelsel onder hoge druk staat. De moorden op de broer (2018) en de advocaat van de kroongetuige (2019) in een groot strafproces, hebben ertoe geleid dat acuut een groot aantal functionarissen uit het strafproces beveiligd moet worden. Deze onvoorziene, massieve en complexe situatie heeft een grote wissel getrokken op de betrokken organisaties. Tijdens de werkzaamheden van de commissie vond op 6 juli 2021 de moord plaats op Peter R. de Vries, vertrouwenspersoon van een kroongetuige. Dit heeft opnieuw geleid tot ongerustheid over de veiligheid van personen die op enigerlei wijze betrokken zijn bij het strafproces in kwestie.⁵

De minister van JenV heeft hierop de Onderzoeksraad voor Veiligheid gevraagd een onderzoek te starten naar aanleiding van de beveiligingssituaties van de broer, toenmalige advocaat en vertrouwenspersoon van de kroongetuige uit het strafproces. De Raad zal dit onderzoek doen, vanuit zijn onafhankelijke positie op basis van de Rijkswet Onderzoeksraad voor Veiligheid.⁶

Verder zijn de betrokken organisaties gestart met een grootschalig versterkingstraject. Het kabinet heeft in de Kamerbrieven van juni 2020⁷, november 2020⁸ en februari 2021⁹ beschreven op welke wijze het stelsel op dit moment versterkt wordt. Dit traject wordt momenteel ingezet en zit midden in de implementatie. De commissie heeft voorgaande meegewogen in haar advies.

1.3.3 Vertrekpunten en analysekader

Op basis van het voorgaande heeft de commissie haar eigen afbakening gemaakt en een kader geformuleerd waarbinnen naar het stelsel wordt gekeken. De commissie heeft gemeend in haar onderzoek met name aandacht aan de volgende onderwerpen te besteden:

- de ontwikkelingen in de dreiging en de opgaven die op het stelsel afkomen;
- de doelstelling en uitgangspunten van het stelsel;
- de vormgeving van het stelsel: inrichting, aansturing en rolinvulling;
- de kwaliteit en werking van het stelsel;
- de informatiepositie binnen het stelsel;
- de uitvoering van de beveiligingsconcepten en -maatregelen;
- het perspectief van een persoon die beveiligd wordt in het stelsel.

1.4 Werkwijze en verantwoording

1.4.1 Dataverzameling

Documentenanalyse

Voor dit onderzoek is een groot aantal documenten bestudeerd. Het gaat meer specifiek om de volgende stukken:

- Circulaires, instructies en richtlijnen waarin de (formele) inrichting en werking van het stelsel zijn beschreven.
- Onderzoekrapporten waarin andere organisaties (zoals de Commissie Van den Haak en de Inspectie Justitie en Veiligheid¹⁰) zijn ingegaan op (onderdelen van) het stelsel.
- Interne evaluatierapporten die betrokken organisaties zelf hebben opgesteld naar aanleiding van specifieke casuïstiek.
- Programma- en projectplannen die organisaties hebben opgesteld in het kader van het versterkingstraject. In deze documenten hebben organisaties vanuit hun perspectief een probleemanalyse op het stelsel gemaakt en hun gewenste verbetering geschetst.
- *Position papers* van de betrokken organisaties die al dan niet op verzoek ten behoeve van de commissie zijn opgesteld.
- Verslagen van verschillende overlegcommissies binnen het stelsel.
- Kamerbrieven.
- Mediaberichten over het stelsel, alsmede de artikelen die experts in vakbladen hebben gepubliceerd.
- Verdiepingsdocumenten die de betrokken organisaties (via de stuurgroep bewaken en beveiligen) hebben aangeleverd, waarvan zij vonden dat de commissie daar kennis van zou moeten nemen.

⁵ Ten tijde van het schrijven van dit rapport werd de achtergrond van de aanslag nog onderzocht.

⁶ Website Onderzoeksraad voor Veiligheid, <https://www.onderzoeksraad.nl/nl/page/19377/onderzoek-naar-bewaken-en-beveiligen>.

⁷ Brief van de regering, *Uitwerking breed offensief tegen georganiseerde ondermijnende criminaliteit*, 18 juni 2020.

⁸ Brief van de regering, *Voortgang aanpak ondermijnende criminaliteit*, 13 november 2020.

⁹ Brief van de regering, *Capaciteitsversterkingen Bewaken en Beveiligen* 8 februari 2021.

¹⁰ Zie lijst documenten in de bijlage.

Interviews met stakeholders en experts

Er is met een groot aantal betrokkenen gesproken. In een eerste gespreksronde werd met betrokkenen en experts uit het operationele proces gesproken. Aan hen is gevraagd om de commissie mee te nemen in de dagelijkse werkprocessen, aan te geven waar er knelpunten zitten en hoe een toekomstbestendig stelsel er vanuit hun perspectief uit zou moeten zien.

In een tweede gespreksronde is gesproken met de stuurgroep bewaken en beveiligen (plenair) en met de leden van de stuurgroep individueel. In deze ronde heeft de commissie haar bevindingen over de knelpunten gevalideerd en mogelijke oplossingsrichtingen verkend. In de laatste gespreksronde is gesproken met de strategische leiding van betrokken organisaties.

Behalve met functionarissen vanuit het stelsel, is ook gesproken met experts en andere betrokkenen die buiten het directe werkveld staan (bijvoorbeeld wetenschappers). Ten slotte hebben er enkele gesprekken plaatsgevonden met personen die beveiligd zijn (geweest) en de werking van het stelsel van binnenuit hebben ervaren.

Van alle gesprekken zijn verslagen gemaakt, die voor wederhoor zijn voorgelegd aan respondenten. Alle opmerkingen bij het verslag zijn integraal overgenomen. Om de vertrouwelijkheid van de gesprekken te waarborgen en zoveel mogelijk openheid te creëren, is tevoren aangegeven dat het verslag slechts wordt gebruikt ten behoeve van de gedachtevorming van de commissie en dat na oplevering van het rapport de verslagen worden vernietigd. Dat is ook gebeurd.

Uit de gesprekken met betrokkenen bij het stelsel blijkt dat er grote overeenstemming is over de probleemanalyse. De commissie is in de verkenning en zoektocht naar haar oordeel geen onoverbrugbare verschillen van standpunten, oplossingen en perspectieven tegengekomen.

Wetenschappelijke reflectie

Om te kunnen adviseren over de toekomstbestendigheid van het stelsel, is inzicht vergaard over trends en ontwikkelingen in het dreigingsbeeld. Hoe ontwikkelt de dreiging zich de komende jaren naar verwachting en wat betekent dit voor opgaves die op het stelsel afkomen? In dit kader is aan de Universiteit Leiden gevraagd om een wetenschappelijke reflectie hierop uit te voeren. Het onderzoek is uitgevoerd door de onderzoekers Schuurman, Van Buuren en Bakker.

Het betreft een wetenschappelijke verkenning die voornamelijk gebaseerd is op literatuuronderzoek. In de studie wordt ingegaan op relevante wetenschappelijke studies, openbare dreigingsbeelden, overheidsrapportages en andere publicaties. Een expertsessie maakte deel uit van het onderzoek. Aan wetenschappers met domeinrelevante kennis werd gevraagd inzichten te delen. De belangrijkste bevindingen uit deze rapportage zijn

verwerkt in hoofdstuk 3 - Ontwikkelingen, dreigingen en uitdagingen stelsel. Het complete rapport is in de bijlage opgenomen.

Internationale vergelijking

Ten slotte heeft de commissie gepoogd een internationale vergelijking tussen stelsels uit te voeren. De relevante informatie bleek niet of nauwelijks beschikbaar. Veelal kon die niet worden verkregen vanwege het vertrouwelijke karakter daarvan. Een betrouwbare studie van stelsels in vergelijkbare landen zou een aanzienlijk tijdsbeslag vergen, met de nodige investering in dienstreizen en individuele interviews. Dit was binnen het gegeven tijdsbestek onhaalbaar.

1.4.2 Klankbordgroep

Ten behoeve van de eigen gedachtevorming en consultatie, heeft de commissie een klankbordgroep¹¹ ingesteld, waarmee over ideeën en vraagstukken gespard kon worden. De leden van de klankbordgroep zijn op persoonlijke titel uitgenodigd en niet als vertegenwoordiger namens een organisatie. Selectie vond plaats op basis van ervaring met het stelsel en kennis van de materie. De leden vervulden recent geen actieve inhoudelijke rol in het stelsel en opereerden zonder last of ruggenspraak. Aan de groep werden eerste beelden en gedachten voorgelegd met de vraag hierop te reflecteren.

Er zijn drie bijeenkomsten met de klankbordgroep geweest. In de eerste sessie zijn de knelpunten met de klankbordgroep besproken, met als doel om de probleemanalyse te valideren en te verdiepen. In de tweede sessie zijn de mogelijke oplossingsrichtingen besproken. In de laatste sessie heeft de klankbordgroep gereflecteerd op de conceptrapportage en is gespard over de formulering van het eindadvies. Daarnaast zijn de leden van de klankbordgroep ook individueel benaderd voor een aanvullende verdieping op enkele thema's.

1.4.3 Wederhoor op feitelijke onjuistheden

In het kader van validatie van de onderzoeksbevindingen, heeft de commissie de stelselpartners gevraagd het conceptrapport te controleren op feitelijke onjuistheden. Via de stuurgroep bewaken en beveiligen zijn de hoofdstukken uit deel II en III voorgelegd aan alle betrokken organisaties. De stuurgroep heeft op 30 september 2021 een geïntegreerde reactie aangeleverd. Daar waar van toepassing zijn de teksten op feitelijke onjuistheden gecorrigeerd.'

¹¹ De samenstelling van de klankbordgroep is opgenomen in de bijlage.

1.5 Leeswijzer

Dit rapport bestaat uit drie delen. Deel I – hiervoor – is een zelfstandig leesbare samenvatting met de conclusies en aanbevelingen, in deel II en III zijn de onderzoeksbevindingen en analyses beschreven die hieraan ten grondslag liggen. Deel II biedt de noodzakelijke context voor dit onderzoek. Zo wordt in hoofdstuk 1 de opdracht van de commissie nader beschreven en wordt in hoofdstuk 2 de organisatie van het stelsel (zoals beschreven in de Circulaire bewaken en beveiligen) op hoofdlijnen toegelicht. Hoofdstuk 3 gaat in op de huidige en verwachte dreigingsontwikkelingen die relevant zijn voor het stelsel. In Deel III wordt het stelsel - op een aantal onderdelen zoals beschreven in paragraaf 1.3.3 – nader beschouwd. Per onderdeel is een probleem-analyse gegeven en worden oplossingsrichtingen geschetst.

Hoofdstuk 2

Het stelsel

2.1 Doelstelling, organisatie en wettelijk kader

Circulaire bewaken en beveiligen

Het huidige stelsel bewaken en beveiligen is in 2002 ingericht. De aanleiding hiervoor was de aanslag op Pim 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. Bij brief van 20 juni 2003 is de voorzitter van de Tweede Kamer der Staten-Generaal geïnformeerd over het 'nieuwe stelsel bewaken en beveiligen'. Twee jaar na de moord op Fortuyn zijn de procedures en de verantwoordelijkheden voor het beschermen van personen en diensten vastgelegd in de 'Circulaire met betrekking tot de bewaking en beveiliging van personen, objecten en diensten'. In dit hoofdstuk worden de voor dit onderzoek relevante onderdelen op hoofdlijnen behandeld.

Het stelsel is een gelaagd stelsel dat gebaseerd is op (een beperkte hoeveelheid) wet- en regelgeving en verder bestaat uit (werk)afspraken tussen de betrokken partners. In de circulaire worden de wet- en regelgeving, de verantwoordelijkheidsverdeling en de werking van het stelsel beschreven. Periodiek wordt de circulaire herzien. De huidige circulaire is op 1 juli 2019 in werking getreden en loopt tot 30 juni 2023. Als afgeleide van de circulaire kunnen stelselpartners hun eigen procedures vormgeven. Zo heeft het OM in de 'Instructie bewaken en beveiligen van personen, objecten en diensten' (1 mei 2016) zijn processen nader uitgewerkt en ingevuld.

Volgens de circulaire is het doel van het stelsel *“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 de circulaire worden in artikel 2.1 de volgende algemene uitgangspunten voor het stelsel geformuleerd. (letterlijk overgenomen uit de circulaire):

- 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;
- Bij het nemen van beveiligingsmaatregelen is er sprake van risicomanagement, geen risico-uitsluiting. Het al dan niet treffen van veiligheidsmaatregelen is een uitkomst van een zorgvuldige afweging door deskundigen, op dreiging, risico en het niveau van maatregelen.
- 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 ervoor 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; door het nemen van beveiligingsmaatregelen zal er altijd sprake zijn van een bepaalde mate van inperking van het privé- en/of maatschappelijk leven.

- Bij het beslissen over beveiligingsmaatregelen staat de veiligheid van de persoon, het object of de dienst centraal. De overheid biedt hierin maatwerk. Beveiligingsmaatregelen kunnen variëren van lichte maatregelen zoals extra toezicht tot zware maatregelen zoals persoonsbeveiliging en objectbeveiliging.
- Welke beveiligingsmaatregelen passend zijn en of en in hoeverre het ongestoord functioneren van een persoon gefaciliteerd kan worden, vergt een zorgvuldige afweging waarbij veiligheid en maatwerk leidend zijn. Om iemand in zijn professionele en/of sociale omgeving ongestoord te kunnen laten functioneren in een situatie van ernstige dreiging en/of risico kan er vrijwel uitsluitend een beroep gedaan worden op zware beveiligingsmaatregelen (zoals persoonsbeveiliging). Het ongestoord kunnen functioneren van een persoon binnen een situatie van dreiging en risico kan, tot op zekere hoogte, gefaciliteerd worden wanneer zwaarwegende belangen als de democratische rechtsorde of fundamentele waarden als vrijheid van meningsuiting en persvrijheid hiertoe noodzaken.

Inrichting van het stelsel

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 dreiging en risico. Het lokale gezag wordt gevormd door de burgemeester en de hoofdofficier van justitie (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 me wordt verstaan het waken over de veiligheid van personen.

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 Justitie en Veiligheid, die zijn bevoegdheden heeft gemandateerd aan de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Deze heeft deze taak intern belegd bij de Coördinator Bewaken en Beveiligen (CBB).

De Politie en de Koninklijke Marechaussee (KMar) zijn de organisaties die de beveiligingsmaatregelen uitvoeren. De informatieorganisaties van de Politie, KMar en de twee inlichtingen- en veiligheidsdiensten (AIVD en MIVD) leveren de informatie- en dreigingsproducten op basis waarvan besluitvorming over maatregelen plaatsvindt.

Hoewel het stelsel organisatorisch in twee domeinen is verdeeld, maakt dit voor de inhoud en uitvoering van de beveiligingsmaatregelen in beginsel geen verschil. Het lokaal bevoegd gezag kan dezelfde beveiligingsmaatregelen treffen als het gezag in het rijksdomein. De uitvoering van de maatregelen geschiedt eveneens door dezelfde organisaties. Voor de dreigingsinschatting en -analyse maakt het lokaal gezag gebruik van de regionale informatieorganisatie (van de Politie en KMar). Het gezag in het rijksdomein maakt gebruik van de landelijke informatieorganisatie en inlichtingen- en veiligheidsdiensten.

Relevante wet- en regelgeving

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

Aanwijzingsbevoegdheid minister van Justitie en Veiligheid

In Artikel 16 van de Politiewet 2012, lid 1 is bepaald dat de minister van JenV 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 2012. Deze artikelen zijn de basis voor het rijksdomein en de verantwoordelijkheid van de minister van Justitie en Veiligheid ten aanzien van de limitatieve lijst. De minister van Justitie en Veiligheid is op basis van deze artikelen de bevoegde autoriteit om de Politie opdracht te geven tot persoonsbeveiliging voor personen en andere beveiligingsmaatregelen. In het decentraal domein ligt het gezag over persoonsbeveiliging bij de HOvJ.

Aanvullend heeft de minister van JenV op grond van artikel 15, derde lid, van de Politiewet 2012 een aanwijzingsbevoegdheid jegens de burgemeesters. Dit kunnen algemene en bijzondere aanwijzingen zijn 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 JenV 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 JenV algemene en bijzondere aanwijzingen geven betreffende de uitoefening van de taken en bevoegdheden van het OM.

Politietaak

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 ordehandhaving 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. Volgens artikel 1, lid 2 van de Politiewet 2012 wordt in deze wet en de daarop berustende bepalingen onder strafrechtelijke handhaving van de rechtsorde mede verstaan het waken voor de veiligheid van personen.

De Politiewet 2012 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.

Politietaken KMar

In artikel 4 van de Politiewet 2012 worden, aan de Koninklijke marechaussee de volgende Politietaken opgedragen die relevant zijn voor het stelsel:

- het waken over de veiligheid van de leden van het koninklijk huis, in samenwerking met andere daartoe aangewezen organen;
- de uitvoering van de Politietaak ten behoeve van Nederlandse en andere strijdkrachten, alsmede internationale militaire hoofdkwartieren, en ten aanzien van tot die strijdkrachten en hoofdkwartieren behorende personen;
- de uitvoering van de Politietaak op de luchthaven Schiphol en op de andere door de Minister van JenV en Minister van Defensie aangewezen luchtvaartterreinen, alsmede de beveiliging van de burgerluchtvaart;
- de verlening van bijstand alsmede de samenwerking met de Politie krachtens deze wet, daaronder begrepen de assistentieverlening aan de Politie bij de bestrijding van grensoverschrijdende criminaliteit;
- De uitvoering van de Politietaak op plaatsen onder beheer van de Minister van Defensie op verboden plaatsen die krachtens de Wet bescherming staatsgeheimen ten behoeve van de landsverdediging zijn aangewezen, alsmede op het terrein van de ambtswoning van de Minister-President.
- het in opdracht van de Minister van JenV en Minister van Defensie verrichten van beveiligingswerkzaamheden ten behoeve van De Nederlandsche Bank N.V.

Daarnaast geldt de hierboven genoemde algemene bijstandstaak aan de Politie. In voorkomende gevallen kan de Politie voor haar taken op het gebied van bewaken en beveiligen bijstand vragen aan de KMar.

Informatie en inlichtingen

In de Wet op de inlichtingen- en veiligheidsdiensten (WIV, 2017) 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 8, tweede lid, onderdeel e juncto artikel 9 van de WIV 2017. Voor de MIVD is de taak in relatie tot het stelsel bewaken en beveiligen vastgelegd in artikel 10, tweede lid, onderdeel f juncto artikel 11 van de WIV 2017. 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.

2.2 Werkwijze decentraal en rijksdomein

2.2.1 Hoofdproces

In essentie is de werkwijze van het stelsel in beide domeinen gelijk. De processtappen op hoofdlijnen zijn hetzelfde, namelijk:

Intake/melding

Het proces begint bij een melding. Dit kan een aangifte zijn bij een lokaal Politiebureau, een signaal dat vanuit de informatie-organisatie en/of inlichtingen- en veiligheidsdiensten wordt afgegeven, of signalen die via andere kanalen bij de Politie en/of het gezag (HOvJ, burgemeester of NCTV) terechtkomen. Op grond van deze melding wordt beoordeeld of dit een zaak is voor het stelsel. Als dit niet zo is, dan wordt de melding door de reguliere Politiezorg afgehandeld. Wordt het wel als zaak voor het stelsel beoordeeld, dan wordt aan de informatieorganisatie gevraagd een informatieproduct (bijvoorbeeld een dreigingsinschatting) te maken.

Voor sommige functionarissen en objecten start de werkwijze niet met een intake/melding, aangezien hiervoor standaard beveiligingsmaatregelen worden getroffen. In deze gevallen wordt periodiek bekeken of er aanleiding is om het werkproces te doorlopen, te beginnen met het opvragen van (dreigings)informatie.

Dreigingsinschatting

Op decentraal niveau maakt de Dienst Regionale Informatie-organisatie (DRIO) van de Politie de dreigingsinschatting op. Voor het rijksdomein wordt dit gedaan door de Dienst Landelijke Informatieorganisatie (DLIO) van de Politie, de AIVD en de MIVD. Voor het vaststellen van het dreigingsniveau worden zowel in het decentraal als in het rijksdomein dezelfde speciaal ontwikkelde tabellen gehanteerd (zie ernst- en waarschijnlijkheidstabellen in de bijlage). Aan de hand van de tabellen wordt een inschatting gemaakt van de mate van 'ernst' en 'waarschijnlijkheid' (effect en voorstelbaarheid) van de dreiging. Deze dreigingsinschatting vormt de basis van het maatregelenadvies.

Maatregelenadvies

Op basis van een zo compleet mogelijk beeld wordt het niveau van de dreiging en het gewenste weerstandsniveau vastgesteld door het lokaal bevoegd gezag of door de CBB van de NCTV voor het rijksof domein. Het is vervolgens aan de uitvoeringsorganisatie (Politie of KMar) om op basis van een integraal inzetconcept een maatregelenadvies op te stellen. In het maatregelenadvies staat beschreven welke dreiging en risico's kunnen worden beheerst met de maatregelen. De te treffen beveiligingsmaatregelen worden vastgesteld door het bevoegd gezag. Binnen het stelsel wordt gesproken over de 'hoe' (uitvoering) en 'wat' (gezag).

Uitvoering

Voor de uitvoering van beveiligingstaken maken het decentraal domein en het rijksof domein grotendeels gebruik van dezelfde diensten. Dat zijn de regionale eenheden van de nationale Politie, de landelijke Dienst Koninklijke en Diplomatieke Beveiliging (DKDB) en de KMar (rijksof domein). De uitvoering vindt plaats onder de verantwoordelijkheid van het bevoegd gezag.

Afwegingskaders

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

Classificatie	Intentie	Potentie	Concreetheid	
	de mate waarin een dreiger voornemens is een gebeurtenis te laten plaatsvinden	de mate waarin een dreiger de kennis en middelen heeft en in de gelegenheid is om een gebeurtenis te laten plaats vinden	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	

Het stelsel: werkproces op hoofdlijnen

	Melding en intake	Dreigingsinschatting	Maatregelenadvies	Uitvoering
Proces-stappen	<p>Het proces begint bij een melding. Dit kan zijn een aangifte bij een lokaal politiebureau, een signaal dat vanuit de informatieorganisatie en/of inlichtingendiensten wordt afgegeven, of signalen die via andere kanalen bij de politie en/of het gezag (een OvJ of de NCTV) terecht komen. Deze melding wordt afgewogen of dit een zaak is voor het stelsel. Als dit niet zo is, dan wordt de melding door de reguliere politiezorg afgehandeld. Wordt het wel als zaak voor het stelsel beoordeeld, dan wordt aan de informatieorganisatie gevraagd een informatieproduct te maken.</p>	<p>Op decentraal niveau maakt de Dienst Regionale Informatieorganisatie (DRIO) van de politie de dreigingsinschatting op. Voor het rijksof domein wordt dit gedaan door de Dienst Landelijke Informatieorganisatie (DLIO), de AIVD en de MIVD. Voor het vaststellen van het dreigingsniveau worden zowel in het decentraals als in het rijksof domein 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. Deze dreigingsinschatting vormt de basis van het maatregelenadvies</p>	<p>Op basis van een zo compleet mogelijk beeld wordt het niveau van de dreiging en gewenste weerstandsniveau vastgesteld door het lokaal bevoegd gezag of door de Coördinator Bewaken en Beveiligen (CBB) voor het rijksof domein. Het is vervolgens aan de uitvoeringsorganisatie (Politie of KMar) om op basis van een integraal inzetconcept een maatregelenadvies op te stellen. In het maatregelenadvies staat beschreven welke dreiging en risico's kunnen worden beheerst met de maatregelen. De te treffen beveiligingsmaatregelen worden vastgesteld door het bevoegd gezag.</p>	<p>Voor de uitvoering van beveiligingstaken maken het decentraal domein en het rijksof domein grotendeels gebruik van dezelfde diensten. Dat zijn de regionale eenheden van de nationale politie, de landelijke Dienst Koninklijke en Diplomatieke Beveiliging (DKDB) en de KMar. De uitvoering vindt plaats onder de verantwoordelijkheid van het bevoegd gezag.</p>
Actoren	<p><i>Decentraal domein</i></p> <ul style="list-style-type: none"> • Politiefunctaris die de melding opneemt en Bureau CCB waar de melding naar toe wordt gestuurd. • Beleidsmedewerker bewaken, beveiligen en crisisbeheersing (BB&C) van het OM. Deze zorgt ervoor dat het besluitvormingsproces goed verloopt, toetst de adviezen, adviseert de hoofdofficier en onderhoudt namens de hoofdofficier de contacten met de portefeuillehouder Conflict- en Crisisbeheersing (CCB) van de politie-eenheid. <p><i>Rijksof domein</i></p> <ul style="list-style-type: none"> • Adviseur van de NCTV waar de melding binnen komt 	<p><i>Decentraal domein</i></p> <ul style="list-style-type: none"> • DRIO • Maatregelenadviseur van Bureau CCB • BB&C van het OM <p><i>Rijksof domein</i></p> <ul style="list-style-type: none"> • DLIO, AIVD en MIVD • Adviseur van de NCTV die de drie analyse weegt, een integrale beoordeling maakt en het gewenste weerstandsniveau bepaalt. 	<p><i>Decentraal domein</i></p> <ul style="list-style-type: none"> • Maatregelenadviseur Bureau CCB • BB&C • HovJ neemt het besluit <p><i>Rijksof domein</i></p> <ul style="list-style-type: none"> • Adviseur NCTV in overleg met de politie of Kmar die het weerstandsniveau vertalen in een inzetconcept. • Coördinator Bewaken en Beveiligen (CBB) neemt namens de NCTV het besluit op het maatregelenadvies. • De CBB wordt geadviseerd door het Afstemmingsoverleg (AIVD, MIVD, DLIO en NCTV) en het Uitvoeringsoverleg (DKDB, Kmar en andere uitvoerende eenheden) 	<ul style="list-style-type: none"> • Regionale politieorganisatie • Landelijke Politiediensten (DKDB) • KMar (BSB, HRB, BOB) <p>Er is geen verschil in (het niveau van) de maatregelen tussen beide domeinen. Dezelfde diensten kunnen derhalve in beide domeinen ingezet worden.</p>

2.2.2 Bijzonderheden decentraal

Criteria voor het opnemen in het stelsel

In het decentraal 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. In de Instructie bewaken en beveiligen van personen, objecten en diensten (mei 2016) heeft het OM deze criteria nader uitgewerkt. In de instructie is beschreven in welke (niet-limitatief opgesomde) gevallen deze afweging wordt gemaakt:

- a) wanneer gedreigd wordt met het (mede)plegen van geweldsdelicten (met een strafmaximum van 6 jaar of meer) alsmede;
- b) indien de dreiging valt onder artikel 285 van het Wetboek van Strafrecht, waarbij tevens sprake is van:
 - een dreiger/pleger met antecedenten met betrekking tot ernstige vormen van geweldpleging; of
 - een dreiger/pleger die beschikt of eenvoudig kan beschikken over (vuur)wapens; of
 - een dreiger/pleger die deel uitmaakt van een groepering bekend met geweld; of
 - een dreiger/pleger met een psychische stoornis; of
 - een ernstige vorm van huiselijk geweld of eengerelateerd geweld; of
 - een dreiging tegen bestuurders, sleutelfiguren in de justitiële keten, personen met een publieke taak; of
 - mediagevoeligheid of politieke gevoeligheid.

Ook die zaken waarbij de situatie naar de professionele inschatting van de Politie ernstig kan worden, dienen volgens de instructie aan het OM te worden voorgelegd.

Adviesfunctie NCTV

De Coördinator Bewaken en Beveiligen (CBB) van de NCTV speelt een signalerende en adviserende rol ten aanzien van het decentraal domein. De CBB kan zowel gevraagd als ongevraagd advies uitbrengen en daarmee het decentraal domein bij beveiligingsvraagstukken ondersteunen. Voordat de CBB ongevraagd advies uitbrengt treedt de CBB daartoe altijd in contact met het bevoegd gezag in het decentraal domein.

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 zichzelf betrekking hebben. Dit betekent overigens 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. 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 en 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.

2.2.3 Bijzonderheden rijksdomein

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 decentraal 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*.

Criteria voor het opnemen in het rijksdomein

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 Politietaken uitvoert);
 - de persoon heeft geen werkgever die kan zorgdragen voor een adequate beveiliging.

Er kan op decentraal niveau aanleiding bestaan om bepaalde personen, objecten of diensten voor te dragen voor (tijdelijke) toevoeging op de limitatieve lijst. Het lokale bevoegd gezag treedt hiertoe in overleg met de CBB. De CBB kan ook op eigen initiatief bedreigde personen voordragen. De NCTV beslist op voorstel van de CBB namens de minister van JenV of iemand (tijdelijk) wordt geplaatst op de limitatieve lijst. Zolang de NCTV geen expliciet besluit hierover heeft genomen blijft de verantwoordelijkheid decentraal belegd.

Voor wat betreft objecten en diensten in het rijksof domein, stelt de NCTV het dreigingsniveau vast. De uitvoering van de bewakings- en beveiligingsmaatregelen geschiedt vervolgens 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.

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 JenV. 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 op het gebied van bewaken en beveiligen. De NCTV is de namens de minister van JenV gezaghebbende over de beveiligingsmaatregelen met betrekking tot de aanwezige personen van de limitatieve lijst. De NCTV (CBB) 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 op deze evenementen.

2.2.4 Overlap

Het decentraal- en rijksof 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 persoon op de limitatieve lijst beveiligingsmaatregelen behoeft, betreft dit een palet aan maatregelen die beide domeinen raken. De CBB zal namens de minister van JenV opdracht verstrekken aan de uitvoerende diensten tot het beveiligen van personen. 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 rijksof domein 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 rijksof domein in contact staat met het decentraal domein om de beveiliging en relevante dreigingsinformatie uit te wisselen.

2.3 Actoren

Nationaal Coördinator Terrorismedbestrijding en Veiligheid

De NCTV heeft naast de (gezag)verantwoordelijkheid voor de limitatieve lijst, ook een bredere taak binnen het stelsel. De NCTV is onder verantwoordelijkheid van de minister van JenV belast met het opstellen, onderhouden en uitvoeren van het stelsel van bewaken en beveiligen. Daarmee heeft de NCTV de volgende formele taken:

- besluiten tot het nemen van bewakings- en beveiligingsmaatregelen voor personen en diensten in het rijksof domein.
- opstellen, onderhouden en uitvoeren van het stelsel bewaken en beveiligen (in het organisatiebesluit JenV verwoord als: het adequaat functioneren van het stelsel van bewaken en beveiligen);
- adviestaak (gevraagd en ongevraagd) omtrent casuïstiek in het decentraal domein.

Openbaar Ministerie

De HOvJ van het arrondissementsparket van het OM heeft het gezag in het kader van de strafrechtelijke handhaving, waaronder het waken over de veiligheid van personen. Het overgrote deel van de bewaken en beveiligen zaken heeft een lokaal karakter en worden derhalve onder gezag van de HOvJ uitgevoerd. De HOvJ van het arrondissement waar de bedreigde persoon woont, bepaalt de maatregelen, die voorbereid worden door de adviseur Bewaken, Beveiligen en Crisisbeheersing (BB&C). De HOvJ van één van de arrondissementen is thans belast met de (beleid)portefeuille bewaken en beveiligen.

Burgemeester

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

Politie

De Politie speelt – zoals beschreven bij het werkproces (H2.3.1) – vanuit verschillende organisatieonderdelen een grote (uitvoerende) rol in het stelsel. Het gaat dan om de aangiftebalie van de reguliere Politiezorg, bureau Conflict- en Crisisbeheersing (CCB), de regionale informatieorganisaties (DRIO's in het decentraal domein) en de landelijke informatieorganisatie (DLIO in het rijksdomein) en de uitvoeringseenheden zoals lokale eenheden en de Dienst Koninklijke en Diplomatieke Beveiliging (DKDB).

Koninklijke Marechaussee

De KMar heeft een aantal taken vanuit de Politiewet 2012 toegewezen gekregen. De KMar beschikt hiervoor over de onderdelen Hoog Risicobeveiliging (HRB), de Brigade Speciale Beveiligingsopdrachten (BSB) en de brigade Objectbeveiliging (BOB). Daarnaast levert de KMar bijstand aan de Politie bij de uitvoering haar taken, als hierom wordt verzocht. Dat kan ook op het gebied van bewaken en beveiligen zijn.

Ten behoeve van de eigen beveiligingstaken heeft de KMar een eigen informatieorganisatie, die vrijwel hetzelfde is georganiseerd als de politieorganisatie. Dreigingsinschattingen en maatregelenadviezen worden op dit moment gemaakt ter ondersteuning van KMar-taak in het kader van de bewaken en beveiligen van burgerluchtvaartterreinen, de Koninklijke woon- en werkverblijven en de persoonsbeveiliging door de BSB in het buitenland. Voor de bijstandstaak wordt gewerkt met de dreigingsinschattingen van de Politie.

AIVD/MIVD

De inlichtingen- en veiligheidsdiensten leveren dreigingsproducten aan de NCTV. Deze organisaties mogen uitsluitend inlichtingen en informatie verzamelen binnen het wettelijke kader en op de onderwerpen die aan hen zijn toegewezen.

2.4 Overlegorganen en samenwerkingsstructuren

Stuurgroep bewaken en beveiligen

Dit gremium bestaat uit de strategische leiding (directeuren en portefeuillehouders) van de stelselpartners, namelijk; NCTV (tevens voorzitter), OM, Politie, KMar, AIVD, MIVD en een vertegenwoordiger van het lokaal bestuur. Het gremium heeft volgens de circulaire als doel *'van gedachten te wisselen en sturing te geven aan verbeteringen of ontwikkelingen die het stelsel aangaan. 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.'*

Afstemmingsoverleg en uitvoeringsoverleg rijksdomein

Het proces van het komen tot adviezen en besluiten ten aanzien van operationele aangelegenheden (in het rijksdomein) vindt plaats onder de verantwoordelijkheid van de NCTV. De adviezen worden voorbereid door de adviseurs bewaken en beveiligen van de NCTV en de besluiten worden genomen door de CBB. Deze wordt hierin ondersteund door het Afstemmingsoverleg Bewaken en Beveiligen (ABB) en het Uitvoeringsoverleg (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 de NCTV. 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.

Het UO wordt voorgezeten door de NCTV en bestaat uit de vertegenwoordigers van de DKDB en de Dienst Specialistische Operaties (DSO) van de Landelijke Eenheid van de Politie, de BSB, het OM 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.

Capaciteitenoverleg

Het Capaciteitenoverleg heeft als taak alle betrokken partijen periodiek te informeren over uitstaande persoonsbeveiligingsopdrachten in relatie tot de beschikbare capaciteit, eventuele knelpunten te signaleren en in geval van schaarste te zoeken naar (structurele) operationele oplossingen.

Opschalingsstructuur grootschalig bewaken en beveiligen

Het overgrote deel van de casussen wordt lokaal binnen een regionale eenheid/arrondissement afgehandeld. Bij grote, complexe en regio-overstijgende casussen raken verschillende gezagen en organisatieonderdelen elkaar. Er is dan behoefte aan nadere afstemming en coördinatie. De circulaire kent geen structuur voor deze situaties.

In de praktijk is hiervoor de opschalingsstructuur ‘team grootschalig bewaken en beveiligen’ ingericht.¹² Dit is voor het eerst toegepast na de moord op advocaat van de kroongetuige in een groot strafproces, toen een grote groep functionarissen (verspreid over het land) tijdelijk beveiliging kreeg toegewezen. In beginsel was deze structuur bedoeld voor interregionale samenwerking in het decentraal domein. Omdat het OM in deze casus echter in een meervoudige rol terechtkwam (gezag, werkgever en deelnemer aan het strafproces), zijn verschillende te beveiligen personen (tijdelijk) aan het rijksdomein toegevoegd. Hiermee is een hybride opschalingsstructuur ontstaan waar zowel de NCTV als het OM de gezagen zijn en de verschillende arrondissementen en Politie-eenheden de maatregelen (decentraal) uitvoeren. Deze hybride opschalingsstructuur functioneert naast de ‘reguliere’ structuren en blijft in werking totdat de dreiging dusdanig afneemt (bijvoorbeeld niet meer regio-overtijgend is), dat besloten kan worden tot afschalen.

Multidisciplinair Platform Bewaken en Beveiligen

Vanuit het versterkingstraject stelsel (zie paragraaf hierna), is het zogenoemde Multidisciplinair Platform Bewaken en Beveiligen opgericht. Dit platform is een samenwerkingsverband van betrokken stelselpartners en heeft als doel gericht te werken aan kwaliteitsverbetering, innovatie en kennisborging. Het platform geeft gevraagd en ongevraagd advies aan de stuurgroep bewaken en beveiligen. Het platform is in juli 2020 gestart en verricht projecten als het (op verzoek) uitvoeren van interne evaluaties, het ontwikkelen van innovatieve beveiligingsconcepten, het uitvoeren van wetenschappelijke verkenningen en het ontwikkelen van methodieken voor scenariovorming en afschalen.

2.5 Ontwikkeling stelsel en ingezette verbeteringen

De minister van JenV heeft vanaf 2019 structureel geïnvesteerd in de versterking van de stelsels bewaken en beveiligen en getuigenbescherming. Dat is uitgewerkt langs drie sporen: versterking van de uitvoering, versterking van de stelsels en versterking van de weerbaarheid.¹³

1. Versterking uitvoering

Het stelsel wordt over de gehele linie versterkt, gericht op voldoende capaciteit, middelen en kwaliteit voor alle drie processtappen van bewaken en beveiligen.

1. Informatievoorziening: circa 30 FTE extra voor de informatieorganisatie van Bewaken en Beveiligen bij de Politie; 2 fte per eenheid (DRIO) en 9 fte landelijk DLIO.
2. Advisering over maatregelen: circa 50 FTE extra capaciteit van de (maatregelen)adviseurs bij de Politie, het OM en de NCTV.
3. De uitvoering van de beveiligingsmaatregelen:
 - a. 120 FTE extra capaciteit om in alle regionale Politie-eenheden ‘Bewaken en Beveiligen-teams’ in te stellen. Deze nieuwe teams zijn primair beschikbaar voor de uitvoering van bewakings- en beveiligingstaken in de eenheden, zoals die nu door de medewerkers uit basiseenheden worden uitgevoerd.
 - b. capaciteit bij de Politie om 24 uur per dag cameratoezicht te kunnen uitvoeren. De uitbreiding van de Monitorcentrale Bewaken en Beveiligen bij de Eenheid Den Haag met 73 FTE ten behoeve van het gehele land is gerealiseerd.
 - c. uitbreiding van minder zichtbare beveiligingsmaatregelen, zoals het onder kunnen brengen van een persoon op een veilige plaats.
 - d. om meer variatie in het aanbod aan beveiligingsconcepten te creëren, zal het eskadron Hoog Risicobeveiliging (HRB) van de Koninklijke Marechaussee (KMar) geleidelijk en aanvullend worden getraind. Door deze interne training zal de HRB in staat zijn om, in grotere mate dan thans het geval is, door middel van bijstand ook persoonsbewakingstaken uit te kunnen uitvoeren. De bovengenoemde concepten vormen een aanvulling op de uitvoering van persoonsbeveiliging in het hoogste dreigingsniveau door de Dienst Koninklijke en Diplomatieke Beveiliging (DKDB), die deze al dan niet met bijstand van de Brigade Speciale Beveiligingsopdrachten (BSB) van de KMar uitvoert. De HRB wordt uitgebreid met 21 fte, de BSB met 12 fte en de intell-organisatie met 3 fte.
 - e. vanaf 2022 worden daarnaast financiële middelen beschikbaar gesteld voor de ontwikkeling en uitvoering van aanvullende alternatieve en innovatieve beveiligingsconcepten ten behoeve van het creëren van meer gradaties daarin. Hierbij wordt onder andere gekeken naar de inzet van (slimme en innovatieve) technieken. De periode tot aan 2022 wordt gebruikt om deze concepten (verder) te ontwikkelen en uit te proberen in de praktijk.

¹² Raamregeling Team Grootschalig Bewaken & Beveiligen (TGBB).

¹³ Brief van de regering, Capaciteitsversterkingen Bewaken en Beveiligen 8 februari 2021.

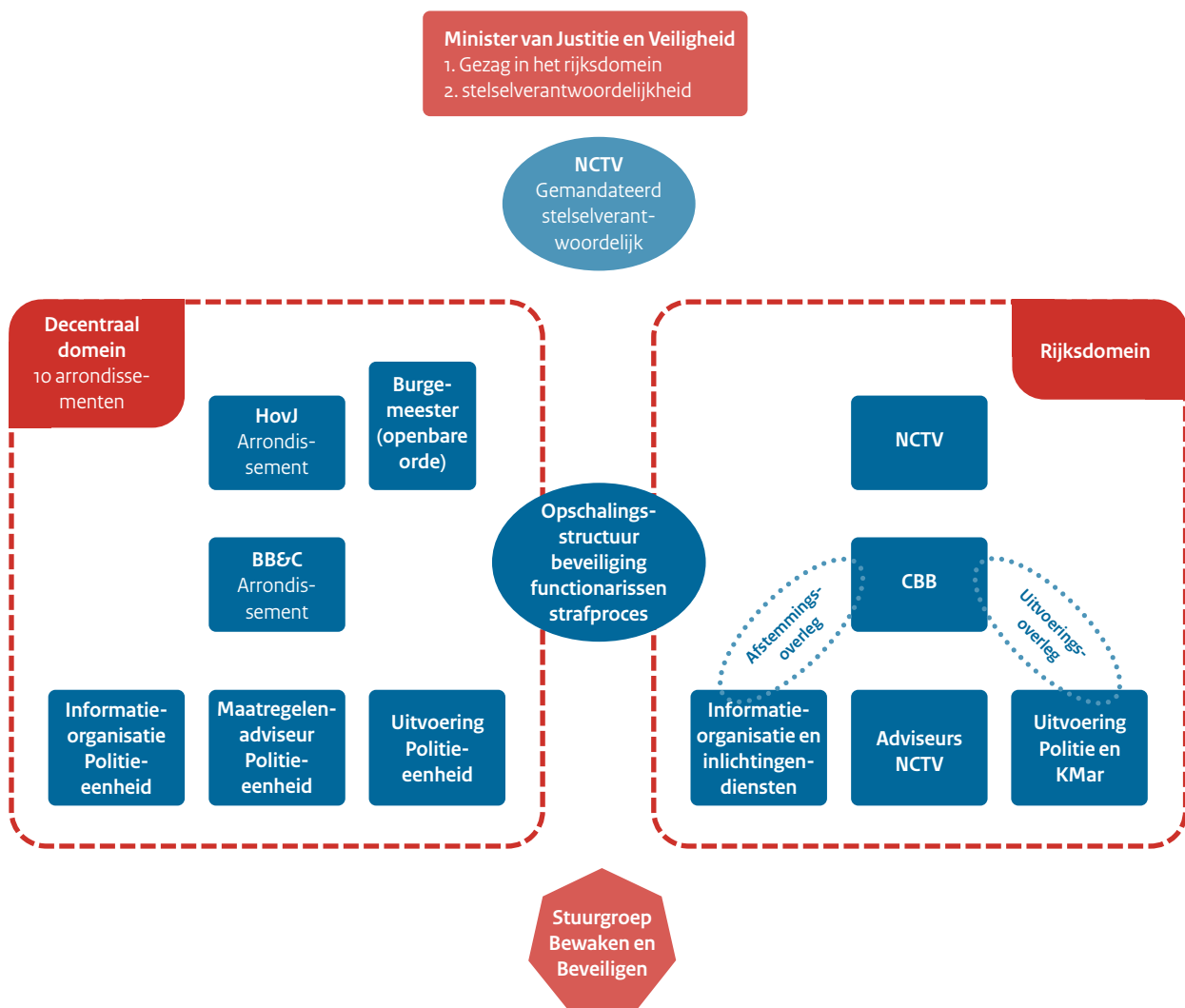
2. Versterking stelsel

Om met alle partners binnen het stelsel kennisdeling, innovatie en kwaliteitsverbetering te realiseren is het hiervoor vermelde multidisciplinair platform ingericht. Het platform fungeert daarnaast ook als vraagbaak voor de operationele stelselpartners. Voor het platform is structureel budget toegekend uit deze versterkingsgelden, zodat projecten en trajecten voortvarend opgepakt kunnen worden, met input vanuit de wetenschap, particuliere sector en bestaande innovatietrajecten.

3. Versterking weerbaarheid

Er is voor 2021 € 3,5 miljoen en vanaf 2022 € 1 miljoen beschikbaar gesteld voor maatregelen, capaciteit en initiatieven om de weerbaarheid van rechters, officieren van justitie, advocaten en journalisten te versterken. Inmiddels zijn door de aangetrokken kwartiermakers onderling best practices en ervaringen gedeeld en zijn er in 2020 verschillende initiatieven van de betrokken beroepsgroepen gefinancierd om de weerbaarheid te intensiveren. Zo zijn onder andere weerbaarheidstrainingen aangeboden en is aan de Nederlandse Orde van Advocaten subsidie verstrekt om scans aan advocaten te kunnen aanbieden waarmee kantoor, woonhuis of digitale voetprint vanuit veiligheidsoogpunt gecontroleerd kunnen worden op kwetsbaarheden.

Inrichting stelsel



Stuurgroep bestaat uit vertegenwoordiging van partners en staat los van de operationele processen. Het heeft als doel om van gedachten te wisselen en sturing te geven aan verbeteringen of ontwikkelingen die het stelsel aangaan.

Hoofdstuk 3

Dreigingsontwikkeling

3.1 Inleidend

Om te kunnen adviseren over een toekomstbestendig stelsel bewaken en beveiligen, is het noodzakelijk om inzicht te krijgen in de ontwikkelingen in de dreiging: wat zijn de uitdagingen waar het stelsel mee geconfronteerd kan worden? Een dreigingsbeeld specifiek gericht op het domein bewaken en beveiligen is tot op heden nooit uitgevoerd. Wel worden in andere (nationale) dreigingsbeelden en –verkenningen trends en ontwikkelingen geschetst die direct of indirect het stelsel van bewaken en beveiligen raken.

De commissie heeft een wetenschappelijke verkenning laten verrichten naar de dreigingsontwikkeling in de afgelopen jaren en een analyse naar de verwachte ontwikkelingen de komende jaren (paragraaf 3.2). Het hieruit ontstane beeld werd gecompleteerd met informatie uit de gesprekken met de functionarissen uit het veld. Zij zijn onder meer bevraagd over de ontwikkelingen die zij in de praktijk zien en op basis van hun kennis en ervaring (paragraaf 3.3). Op basis van deze twee bronnen heeft de commissie geschetst met welke ontwikkelingen een toekomstbestendig stelsel te maken kan krijgen en aan welke voorwaarden het bestel zou moeten voldoen om het hoofd te bieden aan de uitdagingen.

3.2 Ontwikkelingen gezien vanuit de wetenschap

3.2.1 Onderzoek dreigingsontwikkelingen stelsel

De wetenschappelijke verkenning is uitgevoerd door de Universiteit Leiden. Dit heeft geleid tot de rapportage *'Dreigingsontwikkelingen relevant voor het stelsel bewaken en beveiligen: een blik op verleden en mogelijke toekomst'* (Schuurman, Van Buuren en Bakker; 2021). Deze rapportage is in de bijlage opgenomen.

In dit onderzoek is op basis van relevante wetenschappelijke studies, overheidsrapportages (dreigingsbeelden) en andere publicaties geschetst hoe de dreigingen waarmee het stelsel is geconfronteerd, zich sinds de eeuwwisseling hebben ontwikkeld. Dit feitelijke overzicht is aangevuld met de beschikbare cijfers over (ernstige) dreigingen in Nederland. Ten slotte is een expertsessie gehouden met wetenschappers waarin is gereflecteerd op de bevindingen en waarin naar hun inschattingen over de dreigingsontwikkeling is gevraagd. Op basis van deze informatiebronnen hebben de onderzoekers een beschouwing gegeven op de ontwikkeling van stelselrelevante dreigingen en de vraag welke dreigingen de komende jaren als bijzonder relevant kunnen worden geacht.

3.2.2 Verwachte ontwikkelingen en de valkuilen van voorspellen

Initieel had de commissie de behoefte aan een wetenschappelijk onderbouwde voorspelling van de dreigingen die de komende jaren op het stelsel zullen afkomen. De onderzoekers hebben echter op voorhand meegegeven dat dit niet mogelijk is. Zoals zij in hun rapportage stellen: *'de geschiedenis van het vooruitblikken op toekomstige ontwikkelingen qua dreigingen is er één vol missers'*. Volgens de onderzoekers is terughoudendheid geboden, net als een mate van acceptatie van het gegeven dat de onvoorspelbaarheid van dreigingen betekent dat niet ieder geweldsincident kan worden voorkomen.

De onderzoekers hebben niettemin kans gezien een voorzichtige beschouwing te geven over de te verwachten trends en ontwikkelingen. Daarbij is het volgens onderzoekers zaak om zoveel mogelijk los te komen uit de tunnelvisie rond de meest recente dreiging. Ideeën over toekomstige dreigingen vloeien in belangrijke mate voort uit de percepties van wat op dit moment de meest prangende dreigingen zijn. Het is dus belangrijk om breder te kijken dan de meest recente crisis.

De onderzoekers hebben in hun rapport een aantal ontwikkelingen genoemd die zij relevant achten voor het stelsel. Deze zijn in de tabel op de volgende pagina weergegeven.

Ontwikkeling stelselrelevante dreigingen

Ontwikkeling stelselrelevante dreigingen.

In hoeverre laten zich patronen herkennen die zicht bieden op de uitdagingen waar het stelsel zich de komende jaren mee geconfronteerd kan zien? Hieronder wordt op deze vraag puntsgewijs ingegaan.

1. Fluctuatie en nuancering

Dreigingen volgen geen vast patroon en fluctueren in aard en omvang. Het stelsel moet derhalve in staat zijn om snel en flexibel te reageren op deze fluctuaties.

2. De actie-reactie cyclus

De ernst en omvang van dreigingen tegen bepaalde groepen personen of functionarissen (met name lokale bestuurders, officieren van justitie en journalisten) lijkt onderhevig aan een actie-reactie cyclus. Vanuit dat gegeven is het waarschijnlijk dat, met de strijd tegen ondermijning en de lopende strafzaken tegen criminele organisaties, deze cyclus ook de komende jaren tot bedreigingen en geweld zal leiden.

3. Verruwing en een lagere geweldsdrempel

Voor burgers is de drempel tot het uiten van bedreigingen verlaagd. Enerzijds is het waarschijnlijk dat (lokale) bestuurders, ambtenaren en politici in toenemende mate en vooral via sociale media bedreigd zullen worden. Anderzijds lijkt er met name in het criminele milieu sprake van een lagere drempel om dodelijk geweld toe te passen tegen rivalen in de onderwereld, maar ook tegen vermeende tegenstander in de bovenwereld. Het is waarschijnlijk dat het stelsel in de nabije toekomst rekening moet blijven houden met (zeer) ernstige dreigingen vanuit de georganiseerde misdaad.

4. Aanhoudende terroristische dreiging

De terroristische dreiging is sterk gedreven door internationale ontwikkelingen. Het jihadisme is momenteel nog altijd de voornaamste terroristische dreiging, maar het is voorstelbaar dat in de toekomst ook in Nederland andere vormen van extremisme dan het jihadisme tot aanslagen zullen leiden.

5. (On)voorstelbare dreigingen

Terroristen zijn steeds op zoek naar aanslagen die qua vorm of doelwitten opnieuw weten te shockeren. Bij het inschatten van mogelijke toekomstige dreigingen blijft het belangrijk om niet alleen terug te kijken op bekende bronnen van dreiging en geweld, maar vooral ook uiteenlopende en (vooralsnog) fictieve scenario's de revue te laten passeren.

6. Dreigers met mentale gezondheid gerelateerde problematiek

Zowel in Nederland als daarbuiten lijken personen met problemen op het vlak van mentale gezondheid verantwoordelijk voor een aanzienlijk deel van de geuite bedreigingen. Naar verwachting vormt de potentieel gewelddadige eenling ook in de toekomst een dreiging.

7. Internet, complotdenken en de dreiging van statelijke actoren

Het internet is bijzonder relevant geworden voor de ontwikkeling van stelselrelevante dreigingen. Het biedt zeer laagdrempelige mogelijkheden om met een grote mate van anonimiteit bedreigingen te uiten. Daarnaast geeft het toegang tot radicale en extremistische ideeën en de digitale gemeenschappen waarin deze wereldbeelden gedeeld worden. Complotdenken is in sterke mate door het internet aangewakkerd. Het internet is ook een steeds belangrijker domein voor statelijke actoren met vijandelijke intenties. Het lijkt waarschijnlijk dat de verspreiding van desinformatie door burgers en door staten in toenemende mate een bron van frictie en afkalvend vertrouwen in instituties en gezaghebbers zal worden en zal bijdragen aan de vorming van nieuwe dreigingen die onder het stelsel vallen.

8. Dreigingen van binnenuit

Het merendeel van de behandelde literatuur ziet dreigingen richting politici, bestuurders, ambtenaren en journalisten als iets waarvan de bron buiten het directe leef- of werkveld van de slachtoffers ligt. Er bestaat echter ook een risico op ondermijning van binnenuit. Zie de dreiging voor rechts-extremistische militairen waar in landen als Duitsland en de VS toenemend aandacht voor is. Een directe vergelijking op deze thema's met Nederland gaat gelukkig niet op. Deze voorbeelden dienen vooral ter herinnering dat dreigingen uit onverwachte hoek kunnen komen, zelfs in ogenschijnlijk stabiele staten. Het lijkt verstandig om de komende jaren expliciet rekening te houden met zowel externe als interne dreigingen voor de Nederlandse staat en zijn instituties en zicht te houden op buitenlandse ontwikkelingen.

9. De grote invloed van (internationale) incidenten en ontwikkelingen

Incidenten en onvoorziene ontwikkelingen, zowel in Nederland als internationaal, hebben het stelsel regelmatig voor uitdagingen gesteld. Het kunnen inspelen op plotselinge gebeurtenissen met dreiging-verhogend effect en over de grenzen kijken om op de invloed van internationale gebeurtenissen te anticiperen, is ook de komende jaren van groot belang voor het stelsel.

10. Een brede groep bedreigden

Stelselrelevante bedreigingen treffen inmiddels een brede groep individuen, functionarissen en organisaties. Afhankelijk van een bepaald type maatschappelijke crisis kunnen andere doelgroepen dan de huidige in beeld komen. Het stelsel moet snel kunnen schakelen tussen personen en instituties die bescherming nodig hebben.

3.2.3 Conclusies vanuit wetenschappelijk onderzoek

Op basis van het voorgaande trekken de onderzoekers conclusies die relevant zijn voor het stelsel. Onderstaande tekst komt vrijwel letterlijk uit het hoofdstuk conclusies uit het rapport (zie ook bijlage).

Flexibiliteit

Uit het onderzoek komt naar voren dat er plotselinge veranderingen kunnen optreden in wie er beveiligd moet worden. Zo zijn er de laatste jaren toenemende zorgen over bedreiging en intimidatie van journalisten en heeft de coronacrisis opeens wetenschappers en experts van organisaties als het RIVM blootgesteld aan bedreiging van onder andere complotdenkers. De moord op de scholiere Hümeyra illustreert bovendien dat zeer ernstige dreigingen ook ‘gewone burgers’ kunnen treffen. Tot slot kunnen ook statelijke actoren een dreiging vormen voor in Nederland aanwezige diaspora gemeenschappen, zoals de moorden op twee mannen van Iraanse komaf in 2015 en 2017 aantoonde.

De veranderlijkheid van zowel de omvang als de ernst van stelselrelevante dreigingen en de invloed van het actie-reactie mechanisme zullen ook de komende jaren beeldbepalend zijn. Voor de toekomstbestendigheid van het stelsel lijkt de flexibiliteit om snel te kunnen inspelen op (een wellicht tijdelijke) toenemende vraag naar persoonsbeveiliging of objectbewaking een belangrijke voorwaarde. Dat geldt ook voor het blijven investeren in methoden en technieken waarmee zo goed mogelijk een onderscheid kan worden gemaakt tussen ernstige en minder ernstige bedreigingen om op die manier de beschikbare capaciteit van het stelsel optimaal te benutten.

Onvermijdelijkheid van gewelddadige verrassingen

De coronacrisis is illustratief voor een andere belangrijke conclusie, namelijk de grote invloed van onverwachte incidenten en ontwikkelingen. De Nederlandse jihadistische beweging werd bijvoorbeeld tussen 2005 en 2011 getekend door inactiviteit en gebrek aan leiders. Dat veranderde haast plotsklaps toen de Syrische burgeroorlog het land veranderde tot spil in een heroplevende internationale jihad die in 2014 zou uitmonden in het kalifaat van IS. Dergelijke ontwikkelingen laten zich niet of nauwelijks voorspellen, temeer omdat ze vaak internationaal van aard zijn. Dit probleem wordt versterkt doordat nieuwe dreigingen vaak voorheen onvoorstelbare vormen aannemen, zoals de aanslag op het Koninklijk Huis met een auto in 2009 en de moorden op een onschuldige broer van een kroongetuige, op de advocaat en op de vertrouwenspersoon door criminelen. Deze tendensen zullen ook in de toekomst ervoor zorgen dat onze maatschappij verrast wordt door geweldsincidenten die we in vorm of omvang nog niet kennen. Dit is in veel opzichten onvermijdelijk en moet niet per definitie worden gezien als het falen van het stelsel.

Afbakening stelsel

Het brede perspectief dat in het rapport gehanteerd is, vestigt de aandacht op zowel directe fysieke bedreiging en intimidatie van personen als dreigingen voor het ongestoord functioneren van politici, bestuurders en de Nederlandse rechtsstaat in bredere zin. De toekomstbestendigheid van het stelsel is op de eerste plaats afhankelijk van een heldere afbakening. Wordt bijvoorbeeld ook het bewaken en beveiligen van *digitale* objecten en diensten hiertoe gerekend, dan staat het stelsel uiteraard qua capaciteit en middelen voor een grotere uitdaging dan wanneer de nadruk op het fysieke domein blijft liggen. Het scheppen van heldere kaders wat betreft de reikwijdte van het stelsel lijkt dus een belangrijke voorwaarde om überhaupt toekomstbestendig te kunnen opereren.

Kritische distantie

Op meerdere punten maant het rapport tot nuance en kritische distantie. Niet om de reële dreigingen waarmee het stelsel te maken heeft te bagatelliseren, maar om met gepaste afstandelijkheid dreigingen, hun ontwikkeling qua aard en omvang en ook de meest effectieve respons in de juiste proporties te blijven zien. Verschillende publicaties wijten toenemende bedreigingen onder andere aan maatschappelijke verzuivering. Ook is sprake van een tendens vanuit burgers en overheid om ieder risico te willen uitsluiten en ieder geweldsincident of terroristische aanslag te zien als representatief voor fundamentele tekortkomingen van de het stelsel betrokken diensten als Politie en AIVD. Totale veiligheid bestaat niet en het nastreven ervan is niet te verenigen met een open en democratische samenleving. Dat is geen vrijbrief om tekortkomingen van het stelsel weg te wuiven of om betrokkenen niet ter verantwoording te roepen. Het is slechts de nuchtere gevolgtrekking uit een recente geschiedenis waarin de meest invloedrijke geweldsincidenten en dreigingsontwikkelingen zich van tevoren moeilijk lieten voorspellen.

Afsluitend

De toekomst zal het stelsel voor legio uitdagingen plaatsen, van voortdurende ondermijning door (drugs)criminaliteit tot de invloeden van toenemende geopolitieke instabiliteit en afkalvend vertrouwen in de overheid, experts en objectieve nieuwsvergaring. Tegelijkertijd is er ook de noodzaak tot enige relativisering. Ten eerste blijft het belangrijk om te benadrukken dat het in de meeste gevallen van bedreiging van personen daarbij blijft. Hoe onsmakelijk en onwenselijk de bedreiging ook is, tot daadwerkelijk geweld wordt nog altijd relatief zelden overgegaan. Ten tweede is het erg moeilijk om met het heden op het netvlies de toekomst te voorspellen; schokkende gebeurtenissen zoals de moord op Fortuyn of op advocaat Derk Wiersum zijn niet noodzakelijkerwijs tekenen van een nieuwe trend van soortgelijk geweldgebruik. Er lijkt eerder sprake te zijn van contextgebonden toenames in aantal en ernst van stelselrelevante dreigingen. De flexibiliteit om hier snel en daadkrachtig op in te kunnen spelen lijkt een belangrijke vereiste voor de toekomst van het stelsel. Maar een breed en kritisch perspectief op dreigingsontwikkelingen wordt in het rapport eveneens aanbevolen om zo het stelsel op gebalanceerde en proportionele wijze waar nodig te kunnen aanpassen.

3.3 Ontwikkelingen gezien vanuit het werkveld

Stelselpartners hebben in hun *position papers* en gesprekken met de commissie hun visie gegeven op de uitdagingen die op het stelsel afkomen. Op verzoek van de commissie hebben stelselpartners op onderdelen nog aanvullende informatie aangeleverd. Op basis daarvan worden op dit moment vier grote ontwikkelingen gezien.

Toename volume casussen voor het stelsel

Het overgrote deel van de casussen binnen het stelsel vindt volgens respondenten plaats in het decentraal domein. Zaken als bedreiging, stalking, eerwraak, huiselijk geweld, afpersing zijn al jaren aanleiding om personen in het stelsel op te nemen. De verwachting is dat deze casussen ook in de toekomst substantieel onderdeel van het stelsel zullen blijven. Ook op centraal niveau blijven de bekende dreigingen bestaan. Zo wordt structureel in het Dreigingsbeeld Terrorisme Nederland (DTN) gesteld dat een aanslag in Nederland is voorstelbaar is. Het aantal personen en objecten dat langdurig en intensief bewaakt en beveiligd wordt, is toegenomen en zal naar verwachting niet verminderen.

Verwachting toename zware rechtszaken

Nooit eerder was er de noodzaak om voor meerdere advocaten, officieren van justitie en rechters tegelijkertijd (langdurig) veiligheidsmaatregelen te treffen, zoals thans in de praktijk inmiddels gebeurt. De verwachting van professionals is dat dit geen incident is maar een nieuwe realiteit waar rekening mee moet worden gehouden. Respondenten geven aan te zijn geschrokken van de escalatie en drempelverlaging die blijkt uit recente zaken waarin de Politie het versleutelde berichtenverkeer van criminele samenwerkingsverbanden heeft weten te kraken. Bovendien voorziet men dat met het verkrijgen van meer opsporingsinformatie, de komende jaren het aantal zware rechtszaken tegen criminele samenwerkingsverbanden alleen maar zal toenemen. Dit zal onmiskenbaar druk opleveren voor het stelsel.

Vermenging digitale en fysieke veiligheid

Alle stelselpartners hebben aandacht gevraagd voor de digitale dreiging dat zijn weerslag heeft op het domein van bewaken en beveiligen. Van origine is het stelsel gericht op de fysieke veiligheid van een persoon, object of dienst. Maar in de praktijk is volgens functionarissen een vermenging tussen digitale en fysieke veiligheid zichtbaar. De toegenomen digitalisering van de samenleving heeft ervoor gezorgd dat digitale dreiging in toenemende mate van invloed is op het veilig en ongestoord functioneren van de in het kader van het stelsel te beschermen personen, objecten en diensten.

Digitale activiteiten vormen voornamelijk een dreiging voor de fysieke veiligheid als daarmee de vindbaarheid en/of de voorspelbaarheid van een persoon wordt vergroot (op welke locaties en tijdstippen bevinden een persoon en diens naasten zich). Dit kan doordat de dreiger de digitale systemen van een persoon hackt en de benodigde informatie tot zich neemt, maar kan ook doordat de persoon (en/of diens naasten) zelf gevoelige informatie op sociale media plaatst en zich daardoor kwetsbaar opstelt.

De AIVD duidt dat de digitale dreiging zich voordoet in twee verschijningsvormen. Enerzijds vormen digitale activiteiten soms een voorloper van fysiek geweld. Als wordt 'terug-gerechercheerd', komen soms digitale sporen naar voren (bijvoorbeeld een hack op systemen om informatie op te halen ter voorbereiding van een aanslag). Anderzijds worden digitale middelen ingezet om het functioneren van een individu of organisatie te belemmeren. Met de inzet van digitale middelen kan het leven van een persoon ernstig geschaad worden (bijvoorbeeld door identiteitsdiefstal), zonder dat het (fysiek) levensbedreigend is. Volgens de AIVD heeft een te beveiligen persoon ook een cyberidentiteit die beschermd moet worden.

Statelijke dreigingen

De AIVD vraagt daarnaast aandacht voor de dreiging vanuit statelijke actoren voor het veilig en ongestoord functioneren van te beschermen personen, objecten en diensten.¹⁴ Deze dreiging betreft zowel spionage als ongewenste beïnvloeding, zowel fysiek als digitaal. Statelijke dreiging is op zichzelf geen nieuw verschijnsel, maar verandert volgens de AIVD qua modus operandi. Aanleiding voor deze evolutie zijn geopolitieke verschuivingen, nieuwe of hernieuwde assertiviteit van gevestigde en opkomende machten en het ontstaan van nieuwe kwetsbaarheden in de samenleving. Tegelijkertijd nemen de (technologische) mogelijkheden en middelen om een dreiging te vormen toe, evenals de behendigheid van staten om daadwerkelijk een dreiging te vormen voor specifieke doelwitten. Vanwege het gebruik van *proxies* (tussenpersonen) is het bovendien lastig om een dreiging aan specifieke staten toe te schrijven. Complicerende factor hierbij is dat de kennis over statelijke dreigingen vooral bij de inlichtingen- en veiligheidsdiensten AIVD en MIVD aanwezig is. Deze dreigingen manifesteren zich echter steeds vaker in het decentraal domein, waar de kennis, expertise en informatielijnen op dit gebied minder ontwikkeld zijn.

14 Jaarverslag AIVD (2020) en rapport 'Dreigingsbeeld statelijke actoren' (2021).

3.4 Opgaven en uitdagingen voor een toekomstbestendig stelsel

Op basis van hetgeen vanuit de wetenschappelijke studie (paragraaf 3.2) en het werkveld (paragraaf 3.3) is aangereikt, distilleert de commissie de volgende inhoudelijke opgaven waarop het stelsel een antwoord moet vinden.

Toename aantal zware beveiligingsopdrachten

De verwachting is dat het aantal personen en objecten dat langdurig bewaakt en beveiligd moeten worden, zal toenemen. Zorgwekkend, ook naar het oordeel van de commissie, is de verharding in de georganiseerde criminaliteit. De geweldsdrempel is verlaagd en traditionele demarcatielijnen (qua doelwit-categorieën) lijken te worden doorbroken. Ook het eerste beeld dat oprijst uit de onderzoeken die volgen uit de onderschepte versleutelde berichten is er één van zeer ernstig te nemen verharding.

Daarnaast is de verwachting dat deze opsporingsuccessen ertoe zullen leiden dat de komende jaren meer grote strafprocessen zullen plaatsvinden die gepaard gaan met serieuze risico's voor procesdeelnemers en hun omgeving. De commissie acht het derhalve alleszins aannemelijk dat grootschalige beveiligingszaken vanwege dreiging vanuit de georganiseerde criminaliteit geen incident zullen zijn. De kring van beveiligde personen zal als gevolg daarvan toenemen hetgeen een fors beslag zal leggen op het stelsel bewaken en beveiligen. Dit leidt tot vraagstukken als 'voorstelbare dreigingen'¹⁵, gelijkheid van maatregelen en reikwijdte van de zorgplicht. Zaken die nu al spelen, maar in omvang en complexiteit zullen toenemen. Hier zal in het volgende hoofdstuk nader op worden ingegaan.

Blijvend meebewegen nieuwe dreigingen

Een toekomstbestendig stelsel moet de flexibiliteit bevatten om snel te kunnen inspelen op (nieuwe) dreigingsontwikkelingen. Het stelsel dient de eigenschappen te bevatten om hier adequaat op in te spelen. Hiervoor is het nodig dat het stelsel qua informatiepositie en analysevermogen zoveel mogelijk aan de voorkant komt van de ontwikkelingen. Proactieve dreigingsanalyses en scenarioverkenningen kunnen daarbij behulpzaam zijn.

Dreiging in perspectief beschouwen

Daarnaast is het nodig dat in het stelsel kritische distantie en reflectievermogen is ingebouwd, om bedreigingen en de noodzakelijke respons vanuit het stelsel in proportie te zien en ontwikkelingen in hun juiste historische context te plaatsen, zodat zowel een overreactie als een onderschatting van dreigingen zoveel mogelijk wordt voorkomen. Daarvoor moet worden geïnvesteerd in (nieuwe) methoden en technieken waarmee zo goed mogelijk een dreiging kan worden geduid. Dit maakt het ook mogelijk om tijdig beveiligingsmaatregelen op- of af te schalen.

Digitale dreiging als uitdaging

Het stelsel zal meer moeten worden toegesneden op digitale dreigingen. Daarbij heeft de commissie met name de digitale dreiging als opmaat naar fysieke dreiging voor ogen. Verdachte digitale activiteiten gericht op een persoon of object horen in dat kader expliciet als indicator in een dreigingsinschatting aan de orde te komen, zodat ze integraal kunnen worden meegewogen. Hierdoor wordt een completere dreigingsanalyse opgesteld in het kader van bewaken en beveiligen. Daartoe zullen de capaciteiten van het stelsel, met name de expertise van analisten en uitvoerders, moeten worden versterkt.

Waar het gaat om digitale verstoringen van iemands particulier of beroepsmatig functioneren ziet de commissie in de eerste plaats een taak voor de betrokkene zelf en diens werkgever, bijvoorbeeld door het beschikbaar stellen van systemen met adequate securitymaatregelen en gecertificeerde software, met actuele updates en technische ondersteuning en zorgvuldige (terughoudende) uitingen op openbare bronnen als sociale media.

Ten slotte heeft de overheid in bredere zin een taak waar het gaat om (het veilig gebruik van) het digitale netwerk. Bijvoorbeeld het ministerie van Economische Zaken en Klimaat (EZK) via de Telecommunicatiewet, het Nationaal Cyber Security Centrum (NCSC) van het ministerie van JenV of de digitale recherche bij Politie in geval van cybercrime.

Statelijke dreiging

Ten aanzien van de dreiging vanuit statelijke actoren, is het van belang dat in een toekomstbestendig stelsel het decentrale gezag voldoende toegerust is met kennis, handelingsperspectieven en een goede informatievoorziening. In zeer complexe gevallen of gevallen met een groot (internationaal) afbreukrisico kan tijdelijke opname op limitatieve lijst worden overwogen.

Ten slotte

De hierboven geschetste uitdagingen voor het stelsel zijn direct gerelateerd aan de specifieke toekomstige ontwikkelingen en opgaven zoals geschetst door de wetenschappers en door de professionals in het werkveld. Daarnaast komt de commissie tot een aantal algemene bevindingen die leiden tot de noodzaak van vernieuwing op substantiële onderdelen.

¹⁵ Over het begrip 'voorstelbare dreiging' zal later in het rapport ingegaan worden (hoofdstuk 7).

Deel III

Het stelsel in de praktijk



Inleidend

In de voorgaande hoofdstukken is ingegaan op de organisatie en werkwijze van het stelsel (hoofdstuk 2) en op ontwikkelingen en uitdagingen waar het stelsel mee geconfronteerd wordt (hoofdstuk 3). In de komende hoofdstukken gaat de commissie in op de (dagelijkse) praktijk ervan. Het stelsel heeft continu te maken met complexe en diffuse vraagstukken waarop, vaak onder tijdsdruk, een antwoord gevonden dient te worden. Dit heeft zijn weerslag op de huidige invulling van de werkwijze en uitvoering. In dit deel van het rapport wordt bezien of de verschillende onderdelen binnen het stelsel zo zijn ingericht dat blijvend een antwoord kan worden gegeven op de toegenomen complexiteiten en of het stelsel als geheel voldoende geëquipeerd is om de uitdagingen het hoofd te bieden.

Gedeeld beeld

Op basis van documentstudie en gesprekken met een groot aantal respondenten heeft de commissie de volgende onderwerpen geïdentificeerd, waar verschillende vraagstukken en uitdagingen uit voortkomen:

- uitgangspunten stelsel;
- inrichting en aansturing;
- kwaliteit;
- informatiepositie;
- uitvoering;
- het perspectief van de te beveiligen persoon.

Per onderdeel geeft de commissie weer hoe zij de bevindingen analyseert (**rood kopje**) en welke oplossingsrichtingen zij ziet om tot een toekomstbestendig stelsel te komen (**blauw kopje**). Daarbij geeft de commissie aan dat sommige onderwerpen uitgebreid zijn beschreven en tot hele concrete oplossingsrichtingen en aanbevelingen leiden. Andere onderwerpen behoeven vanwege hun complexiteit echter nader onderzoek met specifieke kennis en expertises. In die gevallen heeft de commissie op een abstracter niveau haar aanbevelingen geformuleerd.

Het algemene beeld is dat betrokkenen goeddeels op dezelfde lijn zitten voor wat betreft probleemanalyse en mogelijke oplossingsrichtingen. Het verschil zit vooral in de nuancering van formuleringen en/of de kwalificatie van de ernst van een knelpunt.

Om het overzicht te behouden, is hierna aangegeven welke onderwerpen en vraagstukken in welke paragraaf worden behandeld:

Onderwerpen deel II	
<p>Hoofdstuk 4. Uitgangspunten (p. 45)</p>	<p>In dit hoofdstuk wordt ingegaan op de uitgangspunten die ten grondslag liggen aan het stelsel en tot welke complexe dilemma's dit in de praktijk leidt. Thema's die behandeld worden zijn: reikwijdte stelsel, verantwoordelijkheidsverdeling, zorgplicht, afzien van beveiliging en overlap met het stelsel getuigenbescherming.</p>
<p>Hoofdstuk 5. Inrichting en sturing (p. 54)</p>	<p>Is er een effectieve structuur van waaruit flexibel en daadkrachtig complexe problematiek kan worden opgepakt? Thema's die behandeld worden zijn: strategische sturing op het stelsel als geheel, operationele aansturing van casussen, onderscheid rijksofstedelijk/decentraal domein, rolinvulling van de verschillende vertegenwoordigers van het gezag.</p>
<p>Hoofdstuk 6. Kwaliteit (p. 64)</p>	<p>In dit hoofdstuk wordt de werking van en kwaliteit binnen het stelsel beschouwd. Wat is het kwaliteitsniveau binnen (de verschillende processtappen) het stelsel en hoe werkt de kwaliteitsborging? Thema's die behandeld worden zijn: kwaliteit en uniformiteit, lerend vermogen van het stelsel, het ingezette verbetertraject.</p>
<p>Hoofdstuk 7. Informatiepositie (p. 66)</p>	<p>In dit hoofdstuk wordt ingegaan op de organisatie van de informatiefunctie binnen het stelsel. Hoe is de informatiepositie en voldoet deze voor huidige en verwachte dreigingen? Thema's die behandeld worden zijn: informatiestructuur, informatievergaring, -deling en analyse, wettelijke bevoegdheden en belemmeringen, nieuwe analysemethoden en werkwijzen.</p>
<p>Hoofdstuk 8. Uitvoering (p. 75)</p>	<p>In dit hoofdstuk wordt gekeken naar de uitvoering van de beveiligingsopdrachten. Thema's die behandeld worden zijn: schaarste in capaciteit, inzet van private partijen, gebruik van technologische middelen, samenwerking uitvoerende partners (Politie en KMar).</p>
<p>Hoofdstuk 9. Perspectief van een TBP (p. 80)</p>	<p>In dit hoofdstuk wordt ingegaan op het perspectief van de te beveiligen persoon. Is er in een complexe en dynamische praktijk voldoende oog voor de persoon waar het stelsel uiteindelijk voor is ingericht? Thema's die behandeld worden zijn: impact van beveiliging, weerbaarheid, informatievoorziening en communicatie.</p>

Hoofdstuk 4

Uitgangspunten stelsel

Centrale boodschap

Doordat de Circulaire op enkele cruciale punten te algemeen is geformuleerd, ontstaat variatie en niet uitlegbare verschillen in bewaking en beveiliging. Aanbevolen wordt om op (de belangrijkste) punten helderheid aan te brengen.

4.1 Inleidend: complexe dilemma's

De commissie constateert op basis van de beschrijving in de Circulaire (hoofdstuk 2) dat het stelsel in zijn algemeenheid logisch en goed onderbouwd is ingericht en dat de gedachten erachter goed te volgen zijn. Tegelijkertijd wordt geconstateerd dat er al vele jaren vraagstukken spelen over de uitgangspunten die ten grondslag liggen aan het stelsel. Het gaat hierbij met name over vraagstukken die samenhangen met de begrenzing van het stelsel, de verantwoordelijkheidsverdeling en de reikwijdte van de zorgplicht van de overheid. Die onduidelijkheid leidt in de praktijk tot complexe dilemma's en discussies. Het ontbreken van een heldere afbakening en richting resulteert daarnaast in variatie en niet uitlegbare verschillen in de dagelijkse toepassing. Deze dilemma's worden momenteel extra zichtbaar door de toename van het aantal casussen en de veranderende aard van de dreiging en ontwikkelingen in de samenleving. Uit de position papers die de commissie van stelselpartners heeft ontvangen, alsmede uit gesprekken met functionarissen, blijkt dat er grote behoefte is aan verduidelijking en concretisering op genoemde punten.

De commissie Van den Haak concludeerde in 2003 eveneens dat 'het gebrek aan duidelijke criteria' een zwak punt binnen het toenmalige stelsel was. Het was daardoor voor burgers en voor (particuliere) organisaties onduidelijk wat het stelsel inhield en wat ze van het stelsel mochten verwachten. Met de aanpassing van de Circulaire Bewaken en beveiligen is geprobeerd meer helderheid te verschaffen. Dit is maar ten dele gelukt. Het is nodig om de uitgangspunten te verduidelijken en te herijken.

Bij deze herijking spelen meerdere fundamentele, juridische en staatsrechtelijke vraagstukken, die aanvullend specialistisch onderzoek behoeven. De commissie stelt vast dat dit complexe afwegingen zijn, waaruit vele dilemma's en afwegingen voortkomen, waar soms politieke besluitvorming over nodig is. Tegelijkertijd ziet de commissie de worsteling in het werkveld en heeft zij het signaal opgepakt om meer duidelijkheid in deze vraagstukken te krijgen. Om die reden zal de commissie ingaan op een aantal dilemma's en daarbij richting schetsen. Hierna zal de commissie ingaan op de vraagstukken reikwijdte, verantwoordelijkheid en zorgplicht van het stelsel.

4.2 Reikwijdte, verantwoordelijkheid en zorgplicht

Reikwijdte van de zorgplicht van de overheid

De zorgplicht wordt in de juridische literatuur gedefinieerd als 'een plicht tot handelen of nalaten ten behoeve van één of meerdere belangen van een persoon of object'¹⁶. De zorgplicht van de overheid in het kader van bewaken en beveiligen vloeit voort uit artikel 2 van het Europees Verdrag van de Rechten van de Mens¹⁷ (EVRM) waarin het recht op leven is opgenomen. De staat heeft de positieve verplichting om dit belang actief te beschermen. Met het inrichten van een adequaat functionerend stelsel en het bieden van de mogelijkheid tot bescherming aan alle burgers, wordt invulling gegeven aan die verplichting. Die verplichting is uitgewerkt in de circulaire. Die is echter op enkele punten abstract opgesteld en biedt in de praktijk onvoldoende houvast. Hiermee blijft te veel onduidelijkheid bestaan voor zowel functionarissen als de te beveiligen personen wat verwacht mag worden van de beveiligingsmaatregelen. Deze onduidelijk spijst zicht voornamelijk op de punten ongestoord functioneren en de verantwoordelijkheidsverdeling.

¹⁶ Korten, M.C.P., *Getuigenbescherming in Nederland*, (2015).

¹⁷ Artikel 2, eerste lid EVRM: 'Het recht van een ieder op leven wordt beschermd door de wet. Niemand mag opzettelijk van het leven worden beroofd, behoudens voor de tenuitvoerlegging van een gerechtelijk vonnis wegens een misdrijf waarvoor de wet in de doodstraf voorziet.'

Ongestoord functioneren

In de circulaire wordt als de centrale boodschap van het stelsel gemarkeerd dat ‘[...] personen, objecten en diensten, ondanks dreiging en risico, zo veilig en zo ongestoord mogelijk kunnen functioneren’. Bij de actualisatie van de circulaire in 2019 is dit uitgangspunt nader ingevuld door toevoeging van de volgende passage: *‘het ongestoord functioneren van een persoon kan, tot op zekere hoogte, worden gefaciliteerd wanneer zwaarwegende belangen als de democratische rechtsorde of fundamentele waarden als vrijheid van meningsuiting en persvrijheid hiertoe noodzakelijk zijn.’* Hiervoor zijn echter geen normen, criteria en randvoorwaarden geformuleerd. Daardoor blijft in vele gevallen onduidelijk hoe ver dit ongestoord functioneren dient te reiken en welke personen in welke gevallen hierop aanspraak kunnen maken.

Verantwoordelijkheidsverdeling

In de circulaire staat de gelaagde verantwoordelijkheidsverdeling beschreven (tevens hoofdstuk 2 van dit rapport). Het begint bij de eigen verantwoordelijkheid van de bedreigde persoon. Daarna komt de werkgeversverantwoordelijkheid in beeld. Als deze partijen niet in staat blijken voldoende weerstand te bieden tegen de dreiging en het risico, dan neemt de overheid aanvullende maatregelen. Het is echter niet uitgewerkt wat deze verantwoordelijkheden concreet inhouden en waar de ene verantwoordelijkheid ophoudt en de andere begint. De commissie merkt daarbij wel op dat in de huidige invulling van de verantwoordelijkheidsverdeling er veelal eerst naar de overheid wordt gekeken, waarmee het stelsel al snel als beginpunt wordt gezien in plaats van als aanvulling op eigen verantwoordelijkheden. Uit de verschillende praktijkvoorbeelden die respondenten hebben gegeven, blijkt dat de nadere invulling per casus kan divergeren. Dit kan gaan om fysieke beveiligingsmaatregelen die getroffen worden, maar ook om financiële maatregelen (bijvoorbeeld compensatie van verlies aan inkomen of tegemoetkoming in gemaakte kosten). In het stelsel zijn hiervoor geen richtlijnen opgenomen.

4.3 Aanscherping, verduidelijking en transparantie

Hoewel de normen niet zodanig kunnen worden uitgewerkt dat zij tot in detail houvast bieden voor elk individueel geval, geeft de commissie hier wel richting in. Daarbij focust de commissie op drie aspecten: concretisering van uitgangspunten, het creëren van uitvoeringskaders door middel van vaste beveiligingspakketten en sturing op deze punten.

Concretisering (algemene) uitgangspunten

Om zorg te dragen voor proportionaliteit, uniformiteit en transparantie heeft het stelsel in de eerste plaats concretisering van de uitgangspunten. De commissie adviseert om deze concretisering op te nemen in de circulaire, waardoor er meer duidelijkheid komt wat er wel en niet van het stelsel verwacht mag worden.

Stelsel is er voor iedereen

Geadviseerd wordt om primair te expliciteren dat het stelsel voor iedereen in Nederland beschikbaar is wanneer de dreiging en risico daar aanleiding toe geven. Wanneer iemand door (ernstige) dreiging bescherming behoeft, kan elke inwoner op de overheid rekenen. Daarmee wordt in beginsel voldaan aan de minimale zorgplicht van de overheid op het gebied van veiligheid. Het dilemma daarbij is hoe ver de beveiligingsmaatregelen reiken. Moet iemand die beveiligd wordt, te allen tijde ongestoord zijn zakelijke en persoonlijke leven kunnen voortzetten?

Ongestoord functioneren

De thans in de circulaire neergelegde doelstelling ‘zo veilig en zo ongestoord mogelijk kunnen functioneren’ bevat een onheldere norm en wekt daardoor bepaalde verwachtingen. Beveiligingsmaatregelen binnen het stelsel gaan altijd ten koste van de persoonlijke vrijheid. De term ‘ongestoord’ wekt de suggestie dat de overheid ervoor moet zorgen dat iemand zijn zakelijk en privéleven kan voortzetten. Het is goed om expliciet te markeren dat dit niet het geval is. Het doel van bewaken en beveiligen is het waarborgen van de fysieke veiligheid. Daarbij kan – als nevendoelelstelling en tot op een aanvaardbaar niveau - worden gestreefd naar een “zoveel mogelijk onbelemmerd functioneren” maar ook niet meer dan dat. De commissie acht het daarbij noodzakelijk een expliciet onderscheid te maken tussen het zoveel mogelijk onbelemmerd functioneren in de privésfeer en het zoveel mogelijk onbelemmerd functioneren in de beroepssfeer (uitoefening van de functie).

In de privésfeer zal een te beveiligen persoon concessies moeten doen. Volledige en onbelemmerde voorzetting van alle activiteiten kan in de praktijk onmogelijk worden verlangd en gewaarborgd. Dit zou tot een onaanvaardbare belasting van het stelsel leiden en te veel beslag leggen op schaarse capaciteiten. Het “u vraagt, wij draaien” kan niet als uitgangspunt gelden, met name waar het gaat om activiteiten die niet direct behoren tot de primaire levensbehoeften.

De commissie ziet het zoveel mogelijk onbelemmerd functioneren in de beroepssfeer als een bredere verantwoordelijkheid waarbij, wanneer de dreiging werkgerelateerd is, nadrukkelijk de werkgever in beeld komt. In dat laatste geval moeten ook de brancheorganisaties hun verantwoordelijkheid nemen. Het stelsel kan een faciliterende rol spelen door te voorzien in adviezen en handelingsperspectieven. Daarmee krijgt de verantwoordelijkheidsverdeling een complementair in plaats van lineair karakter.

Een uitzondering op dat laatste uitgangspunt acht de commissie gerechtvaardigd ten aanzien van functionarissen die een wezenlijke rol vervullen in het functioneren van de democratische rechtsorde. Het gaat hier in ieder geval – zoals de Circulaire ook omschrijft – om ‘personen ten aanzien van wie door de aard en/of herkomst van de dreiging en de functie van de persoon 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.’ Hierbij komt de overheidsverantwoordelijkheid nadrukkelijker in beeld. De overheid heeft immers

een belangrijke rol om te waarborgen dat deze functies zoveel mogelijk onbelemmerd uitgeoefend kunnen worden.

Beveiligingspakketten

Vaste pakketten per dreigingsniveau

De commissie meent dat er een meer uniform en helder uitvoeringskader nodig is om zo veel mogelijk duidelijkheid en gelijkheid te creëren voor een te beveiligen persoon. Het instellen van standaardpakketten levert hier een belangrijke bijdrage aan. Deze pakketten worden samengesteld aan de hand van de beoordeling van de dreiging (ernst en waarschijnlijkheid, zie matrix op pagina 23) én het te beschermen belang dat voortkomt uit (bepaalde aspecten van) de functie. In deze pakketten wordt allereerst het beveiligingsconcept en de in te zetten maatregelen beschreven. Daarnaast acht de commissie het verstandig om in deze pakketten ook modules op te nemen in het kader van psychosociale zorg. Zie in dat kader ook hoofdstuk 9 waarin het perspectief van een te beveiligen persoon wordt geschetst. Ten slotte dient in deze pakketten – indien dat aan de orde is – te worden ingegaan op eventuele financiële tegemoetkoming.

Door vooraf een beperkt aantal standaardpakketten vast te leggen, de criteria voor toedeling van een pakket te beschrijven en de spelregels tussen de betrokken persoon en de overheid te expliciteren, wordt de besluitvorming (voor zowel op- als afschalen van maatregelen) en het vervolgtraject transparant en beter uitlegbaar. In de pakketten wordt geëxpliciteerd wat onder eigen verantwoordelijkheid en werkgeversverantwoordelijkheid valt. Door het vaststellen van dergelijke pakketten krijgt ook de zorgplicht van de overheid nader vorm.

Daarnaast wordt met deze pakketten voorkomen dat het gezag in elk concreet geval moet onderhandelen met de te beveiligen persoon over het niveau van de beveiliging. Ook wordt hiermee tegengegaan dat politieke en publicitaire druk wordt aangewend om te komen tot meer of andere beveiligingsmaatregelen dan door de dreigingsinschatting wordt onderbouwd. Pakketten zijn aan de voorkant vastgesteld en de besluitvorming is gebaseerd op objectieve criteria. Daarmee helpen de standaardpakketten om de besluitvorming ten aanzien van beveiligingsmaatregelen transparanter te maken en te depolitiseren. Ook wordt op deze wijze de schaarse capaciteit zo doelmatig mogelijk ingezet.

Een standaardpakket betekent overigens niet dat daarbinnen maatwerk geheel onmogelijk is. Tot op zekere hoogte en binnen een aanvaardbare bandbreedte kan hierin worden voorzien voor zover de specifieke situatie van een te beveiligen persoon hierom vraagt.

Om het werken in standaardpakketten mogelijk te maken, is het nodig dat de verschillende betrokken overheidspartijen hun kennis, creativiteit en capaciteiten bijeenbrengen en gezamenlijk een breed gedifferentieerd palet aan (integrale) beveiligingsconcepten ontwikkelen. De commissie adviseert de pakketten te

laten uitwerken onder verantwoordelijkheid van de NCTV in een gezamenlijk project met OM, Politie en KMar en daarbij ook de private sector te betrekken. De pakketten moeten vervolgens formeel vastgesteld worden in het hoogste sturingsorgaan van het stelsel. In hoofdstuk 5 van dit rapport doet de commissie een voorstel voor een nieuwe aansturingsstructuur en introduceert het hiervoor de zogenoemde Vierhoek bewaken en beveiligen.

Het is van belang dat afspraken voor alle partijen eenduidig en zorgvuldig vastgelegd worden. Geadviseerd wordt de afspraken in een document vast te leggen en dit te laten ondertekenen door de te beveiligen persoon.

Tot slot

Overigens merkt de commissie op dat voor een aantal functionarissen standaard maatregelen worden getroffen. Dit zijn specifieke functies of openbare ambten die op zichzelf een zodanig afbreukrisico hebben dat bepaalde veiligheidsmaatregelen zonder nadere dreigingsinschatting permanent nodig zijn. Ook voor deze beperkte groep functionarissen gelden dezelfde basisregels ten aanzien van de eigen verantwoordelijkheid en acceptatie van de maatregelen.

De commissie is zich ervan bewust dat niet alles in regels en standaardpakketten is te vangen. Er zullen altijd gevallen overblijven waarover specifieke besluitvorming nodig is. Wanneer er keuzes gemaakt dienen te worden bij precieze zaken kan dit vraagstuk op hoger strategisch niveau behandeld worden. Daarnaast bestaat altijd nog de weg – indien een te beveiligen persoon het in de praktijk niet eens is met (de invulling van) het pakket dat hem is toegewezen – om een oordeel van de rechter te vragen. Zo ontstaat jurisprudentie en wordt de zorgplicht ook nader ingevuld.

4.3 Gerelateerde vraagstukken en spanningsvelden

Risico-uitsluiting

Vrijwel alle functionarissen hebben in hun gesprekken met de commissie gewezen op het knelpunt van risico-acceptatie. In de circulaire is opgenomen: *'bij het nemen van beveiligingsmaatregelen is er sprake van risicomangement, geen risico-uitsluiting'*. Ondanks deze heldere beschrijving, geven respondenten aan dit in de praktijk niet zo te ervaren. Zij zien dat bij de politiek en in de samenleving geen of een zeer beperkt niveau van risico-acceptatie is. Men verwacht risico-uitsluiting en houdt de autoriteiten verantwoordelijk voor incidenten. Het stelsel kan echter nooit zo ingericht worden dat volledig alle risico's worden weggenomen. Volledige risico-uitsluiting is gezien de draconische aard van de maatregelen en de impact op het leven van een te beveiligen persoon, in een open samenleving als de onze niet mogelijk.

Verwachtingenmanagement

In dit kader is het goed om bij alle betrokken partijen aan verwachtingsmanagement te doen. Daarbij is het stelsel niet de oplossing, maar slechts één instrument in een breder palet om dreigingen het hoofd te bieden. Strikt beschouwd is bewaking en beveiliging het sluitstuk van dit palet. Dreigingen moeten primair worden weggenomen door preventie, opsporing, interventie en vervolging. Het stelsel geldt daarbij als tijdelijke voorziening totdat die dreiging weg is. Voor een toekomstbestendig stelsel is het daarom cruciaal dat de veiligheidsketen in de volle breedte goed functioneert. Hoe eerder een dreiging wordt afgewend, hoe minder druk er op het stelsel komt.

Niet meewerken aan of afzien van beveiliging

In de circulaire is opgenomen dat *'het niet invullen van de eigen verantwoordelijkheid, de weigering of beperkte medewerking ertoe leidt dat de overheid niet of minder goed haar verantwoordelijkheid (ten aanzien van de persoon voor wie beveiligingsmaatregelen noodzakelijk zijn) kan nemen.'* Wanneer een persoon geheel of gedeeltelijk afziet van beveiliging die wordt aangeboden door de overheid, ontstaat een problematische situatie. De actieve verplichting van de staat om bescherming te bieden, is gebonden aan grondrechten. In dat kader is bijvoorbeeld artikel 5 van het EVRM aan de orde: *'een ieder heeft recht op vrijheid en veiligheid van zijn persoon. Niemand mag zijn vrijheid worden ontnomen, behalve in de navolgende gevallen en overeenkomstig wettelijk voorgeschreven procedure.'* Het Nederlandse staatsrecht kent eenzelfde systematiek waarin (negatief) overheidsingrijpen alleen wordt toegestaan bij of krachtens de formele wet. Dit betekent dat de overheid geen beveiligingsmaatregelen dwingend kan opleggen aan een persoon die dat niet wil. De inzet van alternatieve methoden – zoals het plaatsen van camera's of intensieve Politie surveillance langs de woning – staat al snel op gespannen voet met andere regelgeving, waaronder de privacyregels.

Mede aanleiding van de moord op Peter R. De Vries is het vraagstuk van al dan niet meewerken aan beveiligingsmaatregelen in de publieke discussie actueel. De commissie gaat niet in op deze specifieke casus. De minister van Justitie en Veiligheid heeft de Onderzoeksraad voor de Veiligheid (OvV) gevraagd hier nader onderzoek naar te doen. Wel merkt de commissie in zijn algemeenheid het volgende op.

Los van de juridische beperkingen om beveiliging dwingend op te leggen, deelt de commissie de mening van functionarissen dat dit in de operationele praktijk ook niet goed uitvoerbaar is. Om effectieve beveiligingsmaatregelen te kunnen treffen, is het nodig dat de te beveiligen persoon tijdig alle relevante informatie deelt met de Politie, bijvoorbeeld zijn agenda van verplaatsingen en activiteiten buitenhuis. Zonder dit inzicht is het niet mogelijk om een integraal beveiligingsconcept te ontwerpen en de beproefde werkwijzen in te zetten. Dit kan leiden tot een ineffectief optreden en tot extra veiligheidsrisico's voor de persoon, de omgeving én de beveiligers.

Invulling overheidsverantwoordelijkheid na afzien beveiliging

In gesprekken met functionarissen is aan de orde gekomen dat zij worstelen met het vraagstuk hoe de zorgplicht moet worden ingevuld als een persoon afziet van beveiliging. De commissie realiseert zich dat de Onderzoeksraad op dit onderwerp zal ingaan en is daarom in haar rapport terughoudend hierover. Met dit voorbehoud volstaat de commissie met de volgende opmerkingen.

Als een persoon beveiliging weigert, is er – binnen de gegeven juridische kaders – enig handelingsperspectief. Zo is vanzelfsprekend dat de verantwoordelijke autoriteiten strafvorderlijk blijven acteren op de verdachte, waarmee op termijn de bron van de dreiging onschadelijk kan worden gemaakt. Daarnaast kunnen andere middelen (zoals bijvoorbeeld Politie surveillance en camera's) op de openbare weg ingezet worden, voor zover wettelijk toegestaan en operationeel uitvoerbaar. Ten slotte is het zaak dat de verantwoordelijke autoriteiten contact onderhouden met de persoon in kwestie om deze regelmatig te informeren over (ontwikkelingen in) diens dreigingsbeeld waarbij adviezen kunnen worden gegeven om de eigen (en/of werkgevers) verantwoordelijkheid op dit punt in te vullen. Daarbij moet worden bedacht dat een overheid die niet conform haar eigen kaders vorm kan geven aan de beveiliging, omdat de betrokkene niet meewerkt, daardoor in een kwetsbare positie komt. Ook om deze reden is het van belang om afspraken vast te leggen.

Grensvlak met stelsel getuigenbescherming

Uit gesprekken met betrokken functionarissen is gebleken dat zij binnen het stelsel bewaken en beveiligen knelpunten ervaren die voortvloeien uit het Stelsel Getuigenbescherming (GTB). Zoals in hoofdstuk 1 staat beschreven valt het stelsel GTB buiten de onderzoeksopdracht van de commissie. Beide stelsels hebben namelijk hun eigen zelfstandige uitgangspunten en kennen een eigen dynamiek. Dit vertaalt zich ook door in de vraagstukken over reikwijdte, verantwoordelijkheidsverdeling en zorgplicht. In geval van getuigenbescherming loopt een individu gevaar vanwege medewerking aan een opsporingsonderzoek en strafrechtelijke vervolging door de overheid. Dit brengt een bijzondere verantwoordelijkheid van de overheid met zich mee voor de veiligheid van de getuige en zijn omgeving.

In de praktijk blijkt dat het stelsel bewaken en beveiligen geconfronteerd wordt met casussen die voortkomen uit het stelsel GTB. Personen die onder het stelsel GTB vallen, kunnen om hun moverende redenen besluiten om af te zien van de getuigenbescherming. Deze personen vallen dan automatisch onder het stelsel bewaken en beveiligen wanneer de dreiging en het risico blijven bestaan. Het is hierbij niet duidelijk welk beleid de overheid in dit soort casussen hanteert.

Nader onderzoek afstemming stelsels

De commissie beveelt aan de stelsels bewaken en beveiligen en GTB nader op elkaar af te stemmen. Dit dient in ieder geval te resulteren in een nadere grensmarkering tussen de stelsels. Zoals in hoofdstuk 3 is gesteld is de verwachting dat het aantal zware strafzaken zal toenemen en dat de kring van personen (de strafprocesdeelnemers en eventueel hun omgeving) die in dit kader beveiligd moet worden, ook groter wordt. Het is alleszins aannemelijk dat dit ook voor de kring van (kroon)getuigen (en naasten) zal gelden.

Hoofdstuk 5

Inrichting en sturing

Centrale boodschap

Een toekomstbestendig stelsel moet in staat zijn flexibel in te spelen op ontwikkelingen in de dreiging en opkomende vraagstukken. Daarvoor is nodig: wendbaarheid, krachtige aansturing en intensieve samenwerking van ketenpartners.

- veelal wisselende vertegenwoordigers vanuit organisaties, omdat andere overleggen (op andere beleidsterreinen) voorrang krijgen;
- onvoldoende mandaat van de vertegenwoordigers in het overleg om de gemaakte afspraken door te voeren in de eigen organisatie;
- het perspectief van de vertegenwoordigers dat zich voornamelijk richt op de (belangen van de) eigen organisatie en niet daarnaast ook op het stelsel als geheel.

5.1 Landelijke aansturing stelsel

Meer centrale sturing nodig

De commissie constateert dat de operationele aansturing van casussen op lokaal niveau op dit moment helder is belegd. Het stelsel sluit aan bij de bestuurlijke inrichting en de decentrale gezagsstructuur in Nederland. De operationele aansturing van bovenregionale casussen wordt – middels de opschalingstructuur – thans in de praktijk ontwikkeld. Hier wordt in de volgende paragraaf nader op ingegaan.

Het ontbreekt op dit moment echter aan sturing op het stelsel als geheel. Er is geen landelijk overzicht en inzicht op basis waarvan gezamenlijke beleidskaders worden geformuleerd en/of inhoudelijke knopen worden doorgehakt. Hierdoor is er veel ruimte voor eigen invulling bij verschillende inhoudelijke en operationele kwesties en kunnen verschillen per regio ontstaan. Daarbij merkt de commissie op dat eenheden veelal op zichzelf werken zonder goede afstemming onderling, wat ten koste gaat van de uniformiteit. Het ontbreken van landelijke sturing leidt er tevens toe dat strategieontwikkeling en kwaliteitsverbetering onvoldoende plaatsvindt.

Nadruk op afstemming

In de verschillende gremia die zijn ingericht (zoals genoemd in hoofdstuk 2) worden de inhoudelijke vraagstukken en de noodzaak tot verbetering wel geadresseerd, zo blijkt uit interviews en de verslagen van deze overleggen. Het uiteindelijk vormgeven én borgen van de verbeteringen stopt echter al snel. Respondenten signaleren dit knelpunt en geven daar een aantal verklaringen voor:

Hierdoor wordt geen basis gelegd om te werken aan de gezamenlijke opgaven voor het stelsel. De overleggremia richten zich primair op adresseren en afstemmen, maar in onvoldoende mate op inhoudelijk sturen. Dit knelt met name bij de stuurgroep bewaken en beveiligen die – conform de circulaire – een belangrijke rol heeft in het blijven doorontwikkelen van het stelsel. Respondenten geven aan de strategische discussies op stelsel-niveau in deze stuurgroep te missen. De focus is vooral gericht op (operationele) incidenten en (politieke) actualiteiten. Dit beeld wordt bevestigd als gekeken wordt naar de verslagen van dit overleg. In de afgelopen jaren kwam daarbij de discussie over verdeling van (financiële) middelen vanuit het versterkingstraject, die veel tijd en energie vergde. Het sturen op lange-termijn-scenario's, gezamenlijke capaciteiten en de kwaliteit van de verschillende stelselonderdelen lijkt de afgelopen jaren ondergeschoven te zijn geraakt.

Ontbreken van sturingsinformatie

Voor adequate sturing is een volledig en actueel beeld van de stand van zaken nodig. Het ontbreekt echter op dit moment aan overzicht van en inzicht in het aantal (lopende) casussen, de ingezette en beschikbare capaciteit en het verloop van de ontwikkeltrajecten. Hierdoor is het maar beperkt mogelijk om ontwikkelingen te signaleren en knelpunten tijdig te detecteren. Naast kwantitatieve gegevens ontbreekt het ook aan sturingsinformatie over de kwaliteit en effectiviteit van (de werkprocessen binnen) het stelsel. Hier wordt verder in dit rapport nader op ingegaan. Door het ontbreken van overzicht kan niet structureel getoetst worden of het stelsel doelmatig is georganiseerd en voldoende voorbereid is op nieuwe opgaves, of dat (bij)sturing nodig is.

Invoering landelijke aansturing stelsel

De commissie ziet het als noodzakelijke stap om de governance van het stelsel op landelijk niveau zo te organiseren dat wordt voorzien in krachtige, integrale sturing. Hiermee wordt het mogelijk om de knelpunten op stelselniveau – zoals beschreven in dit rapport – aan te pakken. Daarvoor is nodig:

- een orgaan dat strategische besluiten neemt ten aanzien van het stelsel als geheel en de randvoorwaarden creëert waarbinnen het stelsel optimaal kan functioneren.
- een orgaan dat deze besluiten uitvoert en zich bezighoudt met de dagelijkse aansturing en coördinatie van het stelsel.
- beschikbaarheid van ‘dedicated’ hooggekwalificeerde ondersteuning die zich bezighoudt met de strategisch-inhoudelijke voorbereiding van de overleggen en de doorontwikkeling van het stelsel (los van de dagelijkse hectiek);
- ruimte en commitment van betrokken functionarissen om hun rol volwaardig in te vullen en niet als neventaak.

Het bovenstaande helpt ook om de stelselverantwoordelijkheid van de NCTV beter tot zijn recht te laten komen. De commissie benadrukt dat bij de door haar voorgestelde aansturingsstructuur de gezagsverantwoordelijkheid in de individuele casus en de gebruikelijke beheerslijnen intact blijven. Beslissingen die consequenties hebben voor gezagsuitoefening en beheer in de betrokken organisaties lopen via de gebruikelijke lijnen waarbij het collegiale oordeel van de gremia zwaar moet wegen.

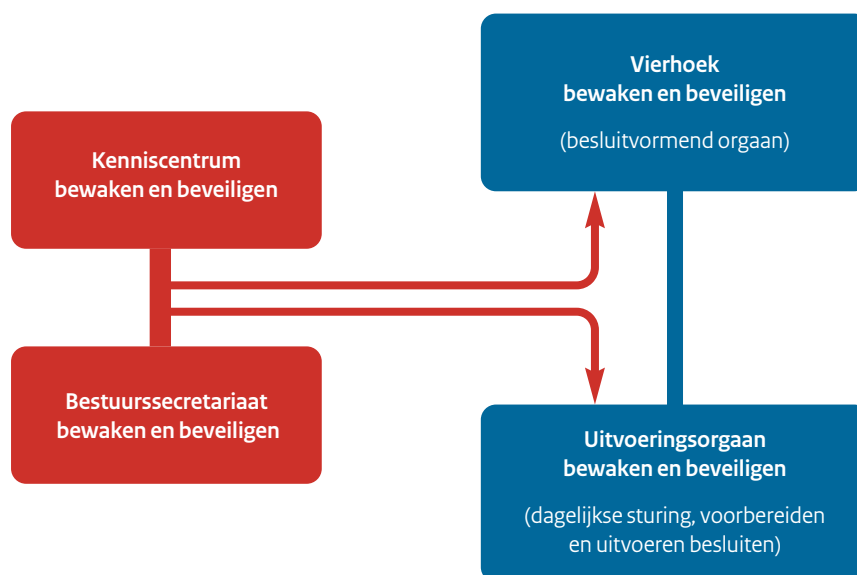
De commissie stelt aldus voor om op landelijk niveau de volgende organen in te richten:

Vierhoek bewaken en beveiligen

De Vierhoek bewaken en beveiligen is het centrale sturingsorgaan voor besluitvorming op het hoogste niveau. In dit orgaan participeren de hoogste leidinggevenden van vier stelselpartners: de NCTV, de portefeuillehouder Bewaken en Beveiligen in het college van Procureurs-Generaal, de Korpschef van de Politie en de Commandant KMar. Hiermee zijn beide gezagen en uitvoeringsorganisaties vertegenwoordigd. De vierhoek stelt de beleidskaders vast (meerjarenbeleid) en neemt de strategische besluiten over het stelsel als geheel. Het voorzitterschap wordt belegd bij de NCTV (als stelselverantwoordelijke en vertegenwoordiger van de minister van JenV). Besluiten van dit centrale sturingsorgaan worden zoveel mogelijk voorbereid door het in te stellen uitvoeringsorgaan (zie hieronder).

Uitvoeringsorgaan bewaken en beveiligen¹⁸

De dagelijkse coördinatie en aansturing van het stelsel komt te liggen bij een orgaan waarin alle stelselpartners (NCTV, OM, Politie, KMar, AIVD en MIVD) zijn vertegenwoordigd. Ook hier berust het voorzitterschap bij de NCTV. Dit overleg opereert binnen de door de vierhoek vastgestelde kaders. Op basis van actuele en volledige informatie wordt het totaal aan activiteiten gemonitord en worden met inachtneming van de verantwoordelijkheden van de (de)centrale autoriteiten, acties uitgezet naar de verschillende onderdelen binnen het stelsel. Het uitvoeringsoverleg bereidt besluiten voor van de vierhoek en is verantwoordelijk voor het uitvoeren van de strategische agenda. Daarnaast heeft dit overleg als taak de operationele afstemming, de kwaliteitsborging en doorontwikkeling van het stelsel.



¹⁸ Ter voorkoming van misverstanden; de commissie stelt een hier nieuw orgaan voor. Niet te verwarren met het in hoofdstuk 2 vermelde uitvoeringsoverleg.

Gezien de druk op het stelsel, de uitdagingen waar het voor staat en het grote belang van adequate sturing, is het belangrijk dat in dit orgaan vertegenwoordigers plaatsnemen met het vereiste mandaat en doorzettingskracht binnen de eigen organisaties en dat zij voldoende tijd vrij maken om deze rol volwaardig in te vullen.

Het is wenselijk dat de relevante informatie beschikbaar komt in de vorm van een dashboard waarin alle voor de aansturing en besluitvorming noodzakelijke gegevens actueel beschikbaar zijn. In dat dashboard horen de hierna genoemde de elementen in ieder geval in terug te komen:

- **Landelijk casusoverzicht**
Om (proactief) verbanden, bijzonderheden en knelpunten te identificeren, wordt in het Uitvoeringsorgaan structureel een actueel landelijk casusoverzicht besproken. Dit maakt het onder andere mogelijk om vanuit landelijk en multidisciplinair perspectief inhoudelijke en operationele afstemmingsvraagstukken te bespreken en – waar nodig – expertise en capaciteit (tijdelijk) te herverdelen om bij piekmomenten of bijzondere casussen elkaar te helpen.
- **Landelijk dreigingsbeeld bewaken en beveiligen**
Dit beeld is mede gebaseerd op de geaggregeerde informatiebeelden uit de regio's (zie ook paragraaf Informatiepositie), aangevuld met wetenschappelijke inzichten. Op basis van dit landelijke dreigingsbeeld, kan het uitvoeringsorgaan proactief scenario's (doen) opstellen en ontwikkelingen agenderen. Het Uitvoeringsorgaan is daarmee in staat zich te prepareren op nieuwe ontwikkelingen in de dreiging – zoals in hoofdstuk 3 geschetst.
- **Innovatie- en doorontwikkelingsagenda**
Het realiseren en implementeren van innovatie en doorontwikkeling is een belangrijke taak van het uitvoeringsoverleg. De werkwijze, analysemethodieken, beveiligingsconcepten en andere producten en processen binnen het stelsel moeten immers meebewegen met de veranderingen in de dreigingsbeelden en ontwikkelingen in de samenleving.
- **Landelijk kwaliteitsbeeld stelsel.**
In het Uitvoeringsorgaan wordt structureel de kwaliteit en effectiviteit van het stelsel beoordeeld op basis van een landelijk kwaliteitsbeeld stelsel. Hiertoe dient een kwaliteitssysteem en een evaluatiefunctie opgezet te worden (zie paragraaf kwaliteit).

Gekwalificeerde ondersteuning

Het goed functioneren van de Vierhoek en het Uitvoeringsorgaan vraagt om goede en zorgvuldige voorbereiding. Het is daarbij van belang dat er hooggekwalificeerde ondersteuning beschikbaar is ten behoeve van deze overleggen. Het is wenselijk dat de NCTV – vanuit zijn rol als stelselverantwoordelijke – de ondersteuning coördineert

en in samenwerking met stelselpartners stuurt op de totstandkoming van de sturingsinformatie in het dashboard. Alle stelselpartners leveren hiervoor de benodigde informatie aan.

Kenniscentrum bewaken en beveiligen

Gezien de aard van de vraagstukken, en de grote ontwikkelopgave, is het tevens van belang om vraagstukken te kunnen adresseren bij een groep van deskundigen. In opdracht van de overleggremia – maar ook eigenstandig – kan deze groep voorstellen en projecten ontwikkelen ten behoeve van kwaliteitsverbetering en kennisborging. De commissie adviseert om hiervoor voort te bouwen op het – in het versterkingstraject ingerichte – Multidisciplinair Platform Bewaken en Beveiligen. Ze adviseert om dit orgaan te verbreden naar een kenniscentrum.

Aan dit kenniscentrum kunnen inhoudelijke opdrachten worden verstrekt en vragen worden voorgelegd op het vlak van verkenning en analyse van nieuwe dreigingen, ontwikkeling van beveiligingsconcepten, instrumenten en methodieken, opzet en onderhoud van een kwaliteitsstelsel, internationale kennisuitwisseling en het uitvoeren van evaluaties om het lerend vermogen van het stelsel te vergroten. Het is wenselijk om aan dit centrum een wetenschappelijk netwerk te koppelen, zodat tevens een blik van buiten naar binnen wordt gehaald en er vanuit een breed perspectief naar het stelsel wordt gekeken. Om dit kenniscentrum het gewenste – en noodzakelijke – effect te geven is het nodig om het centrum goed te positioneren binnen het stelsel en te zorgen voor geborgde capaciteit vanuit de verschillende stelselpartners.

Strategische ontwikkelagenda, mijlpalen en tastbare producten

Met het inrichten van een krachtige aansturingsstructuur, wordt het mogelijk om de noodzakelijke stappen te zetten in het meer toekomstbestendig maken van het stelsel. Om snel voortgang te boeken, beveelt de commissie de vierhoek aan om de aanbevelingen van de commissie in een (tweejarig) strategische agenda om te zetten, met concrete mijlpalen en deliverables, die door het Uitvoeringsorgaan wordt uitgevoerd.

5.2 Lokale aansturing casuïstiek

Decentraal domein, rijksdomein en opschalingsstructuur

Het stelsel is ingericht volgens het uitgangspunt 'decentraal, tenzij'. Alle stelselpartners hebben aangegeven dat ook een toekomstbestendig stelsel lokaal verankerd moet zijn. Het leeuwendeel van de zaken speelt zich ook af in het decentrale domein, de relevante informatie is lokaal aanwezig en de capaciteit om maatregelen te treffen komt primair vanuit de regionale Politie-eenheden. Ook over het bestaan van het rijksdomein is geen discussie. Er zal altijd een groep functionarissen en objecten zijn die vanwege de specifieke belangen en karakteristieken op de limitatieve lijst staan en waar het centrale gezag verantwoordelijkheid voor moet dragen.

Steeds vaker doen zich echter casussen voor, die qua omvang en complexiteit deze ‘klassieke’ geografische en organisatorische grenzen overschrijden. Zo kan er bijvoorbeeld sprake zijn van een grote groep bedreigde personen die verspreid over een aantal arrondissementen woont. Of er kan sprake zijn van een dreiging afkomstig van een statelijke actor, gericht op verschillende inwoners in het decentrale domein (bijvoorbeeld politieke tegenstanders en dissidenten) die op verschillende plekken verblijven in het land.

Dergelijke casussen, waarbij meerdere personen moeten worden beveiligd die in meerdere regio’s wonen en samenhang met elkaar hebben, leiden tot sturingsvraagstukken waarop het stelsel nog niet goed was ingericht. Er was, zoals een respondent het noemde, een ‘ontbrekende dakpan’ in het stelsel. In dergelijke situaties zijn meerdere gezagen en Politie-eenheden betrokken bij de beveiliging van een groep personen inzake dezelfde dreiging. Dit betekent dat de besluitvorming over het beveiligingsniveau, het opbouwen van de informatiepositie en de uitvoering van de maatregelen gecoördineerd moet verlopen.

Werkende weg is inmiddels een werkwijze voor het opschalen van casussen ontstaan. De Politie heeft de opschalingsstructuur Team Grootchalig Bewaken en Beveiligen (TGBB) ontwikkeld. Een TGBB functioneert als een structuur voor de aanpak van omvangrijke complexe en/of bovenregionale stelselzaken. Het OM hanteert daarnaast de werkwijze dat bij interregionale casussen het College van procureurs-generaal een coördinerend HOvJ aanwijst die het gezag uitoefent over die casus (en waar de andere HOvJ’s zich naar voegen).

Bestendinging opschalingsstructuur

De commissie ziet geen aanleiding om het uitgangspunt ‘decentraal, tenzij’ te wijzigen. Als op centraal niveau de beleidskaders en kwaliteitseisen zijn vastgesteld, zijn de randvoorwaarden gecreëerd om op lokaal niveau – binnen één regio – de uitvoering eenduidig te laten verlopen. In de volgende gevallen kan worden afgeweken van de decentrale structuur:

- Vanwege zwaarwegende belangen wordt een persoon – conform de huidige uitgangspunten – al dan niet tijdelijk toegevoegd aan de limitatieve lijst. Het gezag wordt dan uitgeoefend door de NCTV;
- Een zaak speelt over verschillende regio’s waarbij er bovenregionaal wordt opgeschaald - conform de TGBB structuur – onder gezag van het OM.

Gegeven wat in de vorige paragraaf is beschreven, adviseert de commissie om de opschalingsstructuur in de circulaire vast te leggen en daarmee de ‘ontbrekende dakpan’ te formaliseren. Daarnaast dient, gezien de ervaringen dusver, de huidige opschalingsstructuur op enkele punten nader gespecificeerd te worden. De commissie adviseert om daarin de volgende elementen te borgen:

- één gezag vanuit het OM, zodat er geen verschillen ontstaan in de besluitvorming over de beveiligingsmaatregelen in de casussen (zie hieronder bij paragraaf rolinvulling van de gezagen);
- één coördinator uitvoering vanuit de Politie die doorzettingsmacht heeft om eenheid-overstijgend zorg te dragen voor een goede uitvoering van de beveiligingsmaatregelen.
- één informatiecoördinator vanuit de Politie die de regie heeft bij het opzetten en onderhouden van de – voor de casus benodigde – informatiepositie en zorg draagt voor eenduidige dreigingsinschattingen.

De NCTV kan in een dergelijke structuur vanuit de adviesrol aansluiten. Indien er sprake is van één of meerdere te beveiligen personen die op de limitatieve lijst staan, dan zal de NCTV ook vanuit zijn gezagsrol deelnemen aan de opschaling. Het is noodzakelijk dat de informatieorganisatie ook inhoudelijk voldoende mee kan gaan in de opschaling. In hoofdstuk Informatiepositie wordt hierop nader ingegaan. Met de koppeling tussen deze opschalingsstructuur en de voorgestelde landelijke aansturingstructuur kan het stelsel flexibeler functioneren waardoor meer focus kan worden ontwikkeld op de aard en complexiteit van de casus en de competenties en capaciteiten die daarvoor nodig zijn.

5.3 Rolinvulling van de gezagen

In hoofdstuk 2 is beschreven wat de taken en rollen zijn van de actoren binnen het stelsel. De commissie constateert dat die rollen – met name bij de beide gezagen (OM en NCTV) – niet altijd zuiver worden ingevuld en door elkaar heen lopen. Gezag, uitvoering en strategievorming zijn te veel vermengd geraakt. Door respondenten uit de uitvoering wordt aangegeven dat het gezag te veel op hun stoel is komen te zitten. Vanuit het gezag wordt aangegeven dat dit gebeurt omdat er lacunes zijn in (kwaliteit van) de uitvoering. Om de aansturingstructuur zoals hierboven geschetst effectief te laten werken, is het nodig dat de actoren vanuit hun eigen rol elkaar versterken. Dit vergt om te beginnen rolvastheid bij alle actoren.

Verschillende rollen belegd bij de NCTV

De NCTV oefent namens de minister van JenV het gezag uit op het rijksof domein en is daarnaast verantwoordelijk voor het onderhouden en ontwikkelen van het stelsel (‘stelselverantwoordelijk’). Het beleggen van de verschillende rollen - uitvoering en stelselontwikkeling - bij één functionaris – de facto bij de CBB en zijn team – is te plaatsen in een tijd waarin het volume aan casussen, zeker in het rijksof domein, nog overzichtelijk was. De commissie meent echter dat, met name gezien de huidige drukte in de dagelijkse operationele uitvoering in combinatie met de politieke, parlementaire en beleidsmatige taken die hieruit voortvloeien, de twee taken niet meer bij één functionaris belegd

kunnen worden. Ook volgens de NCTV zelf komt de rol van stelselverantwoordelijke in de verdrinking door de grote operationele druk in de uitvoering. Die druk is nog meer toegenomen toen op verzoek van het OM aan de NCTV in oktober 2019 (tijdelijk) de verantwoordelijkheid over de beveiliging van een grote groep functionarissen – betrokken bij een groot strafproces – werd overgedragen.

Scheiding operationele rol en stelselverantwoordelijkheid NCTV

Om beide taken – operationele uitvoering en stelselontwikkeling – goed tot hun recht te laten komen adviseert de commissie binnen de NCTV de rol van stelselverantwoordelijke te scheiden van de operationele werkzaamheden. De rol van de Coördinator Bewaking en Beveiliging moet vanuit dat perspectief worden herbezien. Deze dient belast te worden met de uitvoeringen van taken die voortvloeien uit de limitatieve lijst en het adviseren bij decentrale casuïstiek. Een ander, af te scheiden onderdeel binnen de NCTV dient zich bezig te houden met al hetgeen te maken heeft met de doorontwikkeling van het stelsel.

Rolvermenging Openbaar Ministerie

Ook bij het OM constateert de commissie dat gezag en uitvoering door elkaar lopen. De HOvJ staat doorgaans op grote afstand van de casuïstiek en wordt grotendeels in beslag genomen door andere (hoofd)taken. De adviseur Bewaken, Beveiligen en Crisisbeheersing (BB&C) die hem ondersteunt, heeft daardoor veelal een verzelfstandigde en geïsoleerde positie met veel discretionaire ruimte. Hij staat daarnaast zelfstandig in contact met de Politie en de te beveiligen persoon. Uit de gesprekken blijkt dat er verschillen zijn waarop de BB&C'ers hun rol invullen. Een aantal van hen blijkt in de casussen een meer uitvoerende rol te vervullen, die eerder bij de Politie past. Doordat bij de Politie de bewaken en beveiligen-taak nog onvoldoende is ontwikkeld, geven sommige BB&C'ers een sterk operationele invulling aan die functie. Door gezag en uitvoering zo sterk te vermengen, komt de BB&C'er in een kwetsbare positie en er ontstaat spanning met de vereiste checks and balances in het systeem.

Een ander knelpunt is dat het OM in een toenemend aantal casussen wordt geconfronteerd met overlappende, soms conflictueuze verantwoordelijkheden. Als bijvoorbeeld een officier van justitie wordt bedreigd, dan is het OM tegelijkertijd de werkgever van de bedreigde functionaris, het gezag over de beveiliging en soms ook deelnemer in de strafzaak tegen partijen van waaruit de dreiging komt (bijvoorbeeld een crimineel samenwerkingsverband). Daarnaast kan het OM ook verantwoordelijk zijn voor de beveiliging van de rechters en advocaten in datzelfde strafproces.

In dat kader speelt het punt dat de gezagsrol voor de beveiliging van een grote groep strafprocesdeelnemers tijdelijk is overgenomen door de NCTV. Na de moord op de advocaat van de kroongetuige in een groot strafproces, was sprake van grote politiek-maatschappelijk druk en was er weinig tijd om een

adequate oplossing voor het vraagstuk van de vermenging van verantwoordelijkheden te vinden. De NCTV heeft toen op verzoek van het OM de gezagsrol tijdelijk op zich genomen. Als tijdelijke oplossing in een urgente situatie is dit begrijpelijk en te billijken, maar daarmee is de NCTV in een oneigenlijke positie gekomen die hem te veel in de dagelijkse operationele actualiteit heeft getrokken.

Scheiding gezag en uitvoering OM

De commissie benadrukt in de eerste plaats rolvastheid. De BB&C'er is primair ondersteuner van de hoofdofficier in diens gezagsrol. Daarvoor moet er meer afstand komen tot de uitvoeringstaak van de Politie. Dat kan ook in toenemende mate omdat de Politie die taak professionaliseert.

Vanwege het feit dat niet alle parketten in gelijke mate te maken hebben met bewaken en beveiligen, ontstaan ervaringsverschillen en kan de uitvoering van het stelsel per parket verschillen. Dit is risicovol. Om het probleem aan te pakken is nodig dat het OM verder investeert in het versterken van de coördinatie-taak. Het is belangrijk dat alle arrondissementen op hetzelfde kwaliteitsniveau worden gebracht ten aanzien van de invulling van de gezagsrol. De portefeuillehouder beleid bij het OM heeft de beschikking over twee landelijke BB&C-ers die hem specifiek kunnen ondersteunen in zijn coördinerende rol. De coördinatiefunctie van de portefeuillehouder zal zich gaandeweg moeten ontwikkelen tot een expertisefunctie die ten dienste staat van alle parketten. Daarvoor is wel nodig dat ook de landelijke BB&C-ers niet de uitvoering in worden getrokken.

Naar het oordeel van de commissie moet het OM ook in opschalingsstructuur weer structureel de gezagsrol vervullen. Bij arrondissement-overstijgende zaken waarbij het om andere redenen (werkgeversverantwoordelijkheid of specifieke gevoeligheden) dienstig wordt geacht dat een andere dan de reguliere HOvJ de gezagsrol vervult, wijst het college van procureurs-generaal een andere hoofdofficier aan die tijdelijk deze taak op zich neemt. Deze hoofdofficier heeft geen rechtstreekse binding met de regio, de casus en het betrokken personeel. Deze rol zou bij voorkeur niet moeten worden vervuld door de hoofdofficier/landelijke portefeuillehouder bewaken en beveiligen van het OM. Deze moet zich immers, naast zijn taken in het arrondissement, kunnen blijven toelagen op algemene beleidsmatige coördinatie-taken.

De commissie is zich ervan bewust dat niet alle problemen worden opgelost in dit model. Ook een hoofdofficier op afstand die belast wordt met het gezag kan door sommige procesdeelnemers worden gezien als partijdig. Dit vloeit echter voort uit het wettelijke stelsel waarbij het gezag is belegd bij de HOvJ. Het geschetste model is te verkiezen boven de tijdelijke oplossing die thans (incidenteel) is gekozen, zeker nu te verwachten is dat de opschalingsstructuur vaker wordt geactiveerd.

Hoofdstuk 6

Kwaliteit

Centrale boodschap

Vanwege de zwaarte en het belang, verdient het vakgebied bewaken en beveiligen het om bij alle stelselpartners (NCTV, OM, Politie, KMar en AIVD en MIVD) als hoofdtaak ingericht en organisatorisch verankerd te worden, zodat aspecten als uniformiteit, kwaliteit en continu verbeteren worden geborgd.

Kwaliteitsverschillen, geen uniformiteit

Bewaken en beveiligen is bij een groot deel van betrokken organisaties tot op heden veelal een neventaak geweest, niet alleen op operationeel niveau, maar ook op het strategisch niveau. Met uitzondering van de KMar en de NCTV, hebben slechts kleine onderdelen van betrokken organisaties het vakgebied bewaken en beveiligen als hoofdtaak ingericht¹⁹. Mede door de variatie in aanbod en werklust is het vakgebied bewaken en beveiligen daardoor niet ten volle en op alle niveaus tot ontwikkeling gekomen. Ook is daardoor de taak van bewaken en beveiligen niet altijd aangesloten bij andere werkprocessen binnen de eigen organisatie.

Respondenten geven aan dat er bijvoorbeeld grote verschillen zitten in processtappen, zoals: de afweging om in het stelsel te komen, het opstellen van het dreigingsproduct, de besluitvorming om tot een maatregelenpakket te komen en de wijze waarop de maatregelen worden uitgevoerd. Omdat er geen objectieve criteria, kwaliteit- en prestatie-eisen zijn beschreven waaraan het stelsel moet voldoen, is het ook moeilijk sturen op (het uniformeren en verhogen van de) kwaliteit.

Het gevolg van de kwaliteitsverschillen en gebrek aan uniformiteit is tweeledig. Allereerst raakt dit de burger: gelijke gevallen kunnen verschillend opgepakt worden. Hoe een burger wordt bewaakt en beveiligd hangt deels af van de plaats waar hij wordt bedreigd of waar hij aangifte doet. Een ander gevolg is dat bij regio- of domeinoverstijgende samenwerking, organisaties geconfronteerd worden met werkwijzen en producten die niet op elkaar aansluiten en daardoor een effectieve samenwerking belemmeren.

De commissie constateert dat thans al de nodige stappen worden gezet om hier verbeteringen in aan te brengen. Vanuit het versterkingstraject (zoals beschreven in hoofdstuk 2) wordt ingezet op het verhogen van het kwaliteitsniveau. Met de versterking van capaciteit en competenties krijgt het stelsel over de gehele linie een kwaliteitsimpuls en wordt de basis gelegd om van bewaken en beveiligen een volwaardige taak te maken.

Tegelijkertijd constateert de commissie dat de verbeterprogramma's veelal monodisciplinair zijn opgesteld en ook zo worden uitgevoerd. Er is geen sprake van een integraal verbetertraject. Politie, KMar, OM en NCTV organiseren elk, los van elkaar, hun eigen programma's. Daarnaast, met het uitvoeren van deze verbeterprogramma's alleen staat er geen toekomstbestendig stelsel. De verbeterprogramma's leveren (monodisciplinair) de randvoorwaarden om de basis op orde te krijgen, maar worden uitgevoerd binnen bestaande kaders en grondslagen van het stelsel. Het maximale wat hiermee bereikt kan worden, is optimalisatie van het oude stelsel.

Richt bewaken en beveiligen in als volwaardige hoofdtaak

Een toekomstbestendig stelsel dient een stevig fundament te hebben. Het is daarom van belang om bewaken en beveiligen als hoofdtaak in te richten en dit op het niveau van de eenheidsleiding stevig te verankeren. In dat kader is het cruciaal om de ingezette versterkingstrajecten – vanuit een gemeenschappelijke visie en in multidisciplinair verband - voortvarend door te zetten en daarbij de beschikbare financiële middelen expliciet geoormerkt te houden voor bewaken en beveiligen en hierover voortdurend verantwoording af te leggen. Met het inrichten van de teams bewaken en beveiligen bij de Politie in de eenheden en het creëren van de functies van landelijk BB&C'er, zijn de essentiële randvoorwaarden geschapen om de kwaliteit te uniformeren en naar een hoger niveau te brengen. Belangrijk daarbij is dat de verantwoordelijke functionarissen tijd vrij maken om de noodzakelijke veranderingen door te voeren en daarin niet opgeslokt worden door de dagelijkse operationele hectiek.

¹⁹ Zoals DLIO en DKDB bij de Politie en individuele BB&C'ers bij het OM.

Verder is het van belang om kwaliteitseisen voor producten, processen en andere activiteiten in het stelsel te formuleren, waar vervolgens op gestuurd kan worden. Vanwege de stelselverantwoordelijkheid ligt het voor de hand dat de NCTV hier het voortouw in neemt en erop toeziet dat overal uniforme eisen gelden en dat de processen overeenkomstig die eisen zijn ingericht. In dat kader adviseert de commissie om een kwaliteitstraject op te zetten, waarin kwaliteits-, certificerings- en opleidingsnormen worden ontwikkeld in gezamenlijk overleg met alle partners. Door daarnaast een evaluatie- en auditfunctie in te richten, kan structureel lerend vermogen worden opgebouwd. Aldus opgedane kennis kan worden aangewend voor verbeteringen. De resultaten uit dit kwaliteitstraject worden periodiek als sturingsinformatie in het Uitvoeringsorgaan bewaken en beveiligen geagendeerd, zodat een goed overzicht ontstaat over (de kwaliteit van) het stelsel waarbij zo nodig kan worden bijgestuurd.

Hoofdstuk 7

Informatiepositie

Centrale boodschap

De informatiefunctie binnen het stelsel moet worden versterkt. De huidige informatiepositie is voornamelijk reactief en vraaggericht. Het is belangrijk om meer aan de voorkant te komen van de dreiging. Daarmee kunnen voorstelbare dreigingen meer voorspelbaar worden. In dat verband wordt ook geadviseerd een nadere studie te verrichten naar verruiming van de wettelijke grondslag voor informatie-inwinning in het kader van het stelsel.

7.1 Verbetering en doorontwikkeling informatiepositie nodig

Het stelsel staat of valt met een optimale informatiepositie. Op basis daarvan moet met de juiste analysemethoden en technieken een professionele dreigingsinschatting worden gemaakt. De huidige informatiepositie binnen het stelsel is vooral reactief en vraaggericht. Pas als er een concrete dreigingsmelding is, wordt op basis van de beschikbare informatie in de systemen een dreigingsinschatting gemaakt. Dit systeem functioneert afdoende in standaardzaken. Bij complexe en meer diffuse dreigingsbeelden bestaat echter de noodzaak de informatieorganisatie meer proactief te organiseren, zodat zoveel mogelijk aan de voorkant van de dreiging kan worden gekomen. In de huidige structuur en werkwijze zitten echter belemmeringen voor deze wijze van informatievergarig. Ook los van deze exercitie zijn verbeteringen nodig in de informatie-organisatie. In de volgende paragrafen wordt hier nader op ingegaan.

7.2 Doorontwikkeling informatiepositie en -producten

Reactief en voorstelbaar

Steeds vaker wordt het stelsel geconfronteerd met complexe situaties, waarin er geen concrete dreigingsinformatie is en in een context van grote onzekerheid besluiten genomen moeten worden. Bestaande instrumenten en afwegingsmatrices (zoals

weergegeven op pagina 23 in hoofdstuk 2), voldoen dan niet meer. Het begrip 'voorstelbaarheid' is gaandeweg prominenter geworden: hoewel er geen concrete informatie is over een dreiging op een persoon of object, kunnen er situaties ontstaan waarin die dreiging wel voorstelbaar is. Ook op basis van weinig informatie, wordt dan de noodzaak gevoeld maatregelen te treffen omdat ook zonder concrete indicaties aanzienlijke risico's aanwezig worden geacht. Het stelsel komt daarmee steeds meer onder druk. Schaarste capaciteiten worden mogelijk onnodig ingezet en een traject om beveiligingsmaatregelen af te bouwen ontbreekt veelal. Want als op basis van weinig concrete informatie beveiligingsmaatregelen zijn getroffen, wanneer kunnen deze maatregelen dan weer worden afgeschaald? De voorstelbaarheid blijft immers. Respondenten geven aan dat vooral het ontbreken van een afbouwroute het stelsel zwaar belast. Partijen geven verder aan dat de informatieorganisatie moet kunnen voorzien in deze veranderde informatiebehoefte, zodat het stelsel ook bij complexe, meer diffuse dreigingsbeelden zoveel mogelijk informatiegestuurd kan functioneren.

Van reactief naar proactief, van voorstelbaarheid naar voorspelbaarheid

Om meer aan de voorkant van de dreiging te kunnen komen is het nodig dat informatieproducten, werkwijzen, (analyse)methoden en technieken worden geïnnoveerd. Voorstelbare dreigingen moeten voorspelbaar gemaakt worden, zodat er meer proactief geacteerd kan worden. De commissie beseft tegelijkertijd dat dit een flinke opgave is. Er zullen situaties blijven die ook met verbeterde analyseproducten niet voldoende zijn te duiden. De informatiepositie en dreigingsanalyse zullen altijd een bepaalde mate van 'voorstelbaarheid' bevatten. De opgave is om die factor zo klein mogelijk te houden. Hiervoor is nodig dat de informatie-organisatie wordt versterkt, dat de belemmeringen die partners in het informatieproces ervaren zoveel mogelijk worden opgeheven en dat waar mogelijk nieuwe informatiekanalen worden geopend.

7.3 Noodzaak versterking informatiefunctie van de Politie

De Politie is een belangrijke informatieverancier. De tien regionale informatieorganisaties van de eenheden (DRIO) en de landelijke informatieorganisatie (DLIO) zijn de primaire leveranciers van de dreigingsinschattingen op basis waarvan op decentraal niveau en in het rijksdomein maatregelen worden bepaald. De informatie die deze organisaties voor de dreigingsinschattingen vergaren, komen vanuit de hele Politieorganisatie. In dit proces wordt een aantal knelpunten ervaren.

Interregionale informatie-uitwisseling en landelijk overzicht

Alle functionarissen benadrukken dat de informatiepositie lokaal verankerd moet blijven. Het overgrote deel van de casussen heeft volgens hen namelijk een lokaal karakter of is mede afhankelijk van lokaal aanwezige informatie. De Politie geeft aan dat het daarom onwenselijk zou zijn om de informatiepositie weg te trekken uit het lokale domein en dit bij een aparte centrale organisatie te beleggen, omdat hiermee een wij-zij denken kan ontstaan en belangrijke informatielijnen worden afgesneden.

Deze opvatting wordt gedeeld door de commissie. Lokale verankering van informatie-inwinning en lokaal commitment is onontbeerlijk. Tegelijkertijd constateert de commissie dat de eenheden primair hun focus op lokale casuïstiek hebben en weinig zicht hebben op de casussen in andere eenheden, mede als gevolg van het ontbreken van een landelijk totaalbeeld. Zo kunnen twee verschillende eenheden, in twee verschillende casussen te maken hebben met een dreiging, zonder meteen op te merken dat deze verband met elkaar (kunnen) hebben. Doordat relevante informatie niet wordt gedeeld, kan het daarnaast zijn dat de dreigingsinschatting in de ene casus anders uitvalt dan in de andere casus.

Dit knelpunt wordt versterkt wanneer een te beveiligen persoon een landelijke uitstraling heeft en voor zijn of haar werk veelvuldig door Nederland beweegt. Meerdere regionale informatieorganisaties zijn dan betrokken en hebben informatie die relevant is voor bewaken en beveiligen. Er ontbreekt echter een landelijk beeld waarin de informatie gestructureerd bij elkaar komt en wordt verrijkt.

Er is dus geen totaaloverzicht in de informatiepositie op het gebied van bewaken en beveiligen en er wordt onvoldoende (proactief) relevante informatie tussen eenheden (horizontaal tussen de DRIO's en verticaal met DLIO) gedeeld. De informatieorganisaties worden pas in stelling gebracht als er formeel (door het gezag) om een dreigingsanalyse wordt gevraagd. Het proactief opstellen van dreigingsanalyses – om eerder een potentiële dreiging te signaleren en te duiden – is op dit moment geen onderdeel van het proces. Dit is een belangrijke lacune.

Opzetten informatiestructuur bewaken en beveiligen

Het stelsel verdient een eigen, meer op dit taakgebied toegesneden informatiefunctie. Er is een informatiestructuur bewaken en beveiligen nodig die zich niet losmaakt van de bestaande informatieorganisatie, maar waarbij wel alle voor bewaken en beveiligen relevante informatie overzichtelijk beschikbaar is voor alle eenheden en waarin alle beschikbare informatie kan worden ontsloten en gestapeld, zodat een compleet beeld voor het stelsel als geheel, of specifieke casus in het bijzonder, ontstaat.

Vastgesteld wordt dat vanuit het versterkingstraject de regionale informatieorganisaties en de landelijke informatieorganisatie worden toegerust met extra analysecapaciteit ten behoeve van bewaken en beveiligen. De commissie benadrukt het belang van deze investering. Vanuit deze geormerkte versterkingscapaciteit bij DLIO en de tien DRIO's kan een informatieplatform ontstaan, zoals hierboven beschreven. Een samenwerkingsverband als ware het één informatieplatform. Het ligt in de rede dat een dergelijk informatieplatform wordt ondersteund door DLIO.

Dit informatieplatform werkt naast het (proactief) delen van informatie, ook aan het (door)ontwikkelen van de discipline 'informatieanalyse bewaken en beveiligen' en het ontwikkelen van nieuwe analysemethodieken en instrumenten. Daarmee wordt uiteindelijk de kwaliteit van de informatieproducten verhoogd. Op basis van de regionale dreigingsproducten wordt een landelijk dreigingsbeeld opgesteld, om trends en ontwikkelingen in de dreiging te onderkennen. Dit landelijke beeld wordt als sturingsinformatie in de landelijke aansturingsstructuur (vierhoek en uitvoeringsorgaan) geagendeerd.

Met een stevige informatiestructuur kunnen tevens de banden met de KMar, AIVD en MIVD en andere informatieveranciers worden versterkt. Het platform is het aanspreekpunt voor andere partijen op het gebied van bewaken en beveiligen. Er ontstaat zo een vertrouwd, multidisciplinair en geprofessionaliseerd netwerk waarin sneller informatie gedeeld wordt. Deze structuur kan ook behulpzaam zijn bij casussen waarin een opschalingsstructuur wordt opgezet waarbij in een specifieke informatiefunctie moet worden voorzien.

Noodzaak eigenstandige informatiestroom bewaken en beveiligen

Respondenten hebben aangegeven dat de primaire focus van de recherche-onderdelen (begrijpelijk) gericht is op de hoofdtak opsporing en niet op het inschatten van risico's op basis waarvan voor bepaalde personen beveiligingsmaatregelen dienen te worden getroffen. Hierdoor kan het zijn dat relevante veiligheidsinformatie uit de opsporingskolom niet – of niet tijdig – bij de functionarissen verantwoordelijk voor bewaken en beveiligen terecht komt en daardoor relevante veiligheidsinformatie ontbreekt. Een factor die hierbij ook meespeelt is de afscherming van precaire informatie die bij uitlekken het opsporingsonderzoek kan bemoeilijken.

Daarnaast speelt het knelpunt dat als een opsporingsonderzoek – naar de persoon of organisatie vanwaar de dreiging komt – wordt afgerond, ook de informatiestroom vanuit de opsporing opdroogt. Strafvorderlijke middelen waarmee zicht wordt verkregen op bewegingen van dreigers zijn afgebouwd en de betreffende persoon zit bijvoorbeeld in detentie of is daaruit ontslagen. Daarmee hoeft de dreiging echter niet weg te zijn, maar beschikt de Politie niet meer over een actuele informatiepositie. Respondenten hebben aangegeven de behoefte te hebben om na een afgesloten zaak het lopende onderzoek (tijdelijk) voort te zetten om informatie ten behoeve van bewaken en beveiligen te kunnen blijven verzamelen.

Koppelen van perspectief bewaken en beveiligen aan andere processen

Het is belangrijk dat gedurende opsporing en vervolging ook het bewaken en beveiligen perspectief aan bod komt om tijdig essentiële veiligheidsinformatie te detecteren en doorgeleiden. Aanbevolen wordt om een analist aan grote opsporingsonderzoeken toe te voegen die specifiek de taak krijgt om vanuit verschillende disciplines binnen de politieorganisatie de – voor bewaken en beveiligen relevante - informatie bij elkaar te brengen en te analyseren, om deze vervolgens beschikbaar te stellen aan de juiste functionarissen, zonder het opsporingsonderzoek daarbij in gevaar te brengen.

Grens van bevoegdheden bereikt

Informatieverzameling door de Politie, ook op het terrein van bewaken en beveiligen, moet gebeuren op basis van wettelijke bevoegdheden en heldere kaders. De Politie geeft aan dat zij in het kader van bewaken en beveiligen al snel tegen de grenzen van haar bevoegdheden aanloopt en dat zij daarmee belemmerd wordt om de juiste informatie te verzamelen om proactief een dreiging te signaleren en te duiden. Deze belemmering wordt op twee niveaus ervaren:

- als er vanuit het perspectief van de dreiger (persoon of groepering) informatie moet worden verzameld om de concrete dreiging en de modus operandi te detecteren;
- als er vanuit het perspectief van de bedreigde persoon informatie moet worden verzameld om de (potentiele) dreigingen te detecteren en analyseren.

Op het moment dat de strafrechtelijke middelen ophouden is het voor de Politie in het kader van bewaken en beveiligen van belang om een goede informatiepositie te behouden. De mogelijkheden daartoe zijn echter zeer beperkt. Als er geen algemene strafrechtelijke titel is of een grondslag uit bijzondere wetten, kan daarbij tot op heden alleen gesteund worden op de algemene taakstelling van de Politie, zoals omschreven in artikel 3 Politiewet (hierna: artikel 3 PW)²⁰. Op grond van dit artikel kan en mag de Politie publiek toegankelijke bronnen bekijken en gegevens verzamelen ter uitvoering van haar taken. Maar daaraan zitten, vanwege het algemene taakstellende karakter van deze bepaling (en het ontbreken van een specifieke grondslag), grenzen en beperkingen.

De belangrijkste beperking is dat de inbreuk die gemaakt kan worden op de persoonlijke levenssfeer nooit meer mag zijn dan 'een geringe inbreuk'. Wordt deze grens overschreden dan kan het zoeken en verzamelen van gegevens in openbare bronnen met het oog op bewaken en beveiligen niet op artikel 3 PW worden gebaseerd. De Politie wordt daarmee beperkt in haar bevoegdheden om onderzoek te doen naar dreigingen, wanneer er nog geen verdenking van een strafbaar feit is. En als die verdenking er wel is of het strafbare feit manifesteert (een gerichte bedreiging bijvoorbeeld), dan zit men al in de fase waarin de dreiging dusdanig hoog is, dat daardoor ook meteen zwaardere beveiligingsmaatregelen moeten worden getroffen.

Ter concretisering geeft de Politie verder aan dat zij niet gericht en stelselmatig in open bronnen onderzoek mag doen naar een persoon of groep, die zich intimiderend en/of dreigend uit naar een of meer personen, zolang er althans geen strafbare handelingen zijn verricht of een strafforderlijke verdenking bestaat. De Politie is niet bevoegd om deze subjecten (structureel) te volgen (op bijvoorbeeld social media) om te kijken hoe de dreiging zich ontwikkelt, terwijl iedere burger privé dit wel mag doen. Dit zet de Politie op achterstand waardoor men achter de feiten aan loopt. Grootste zorg op dit moment is dat er concrete dreigingen zijn op personen, objecten en diensten die met de huidige informatiepositie niet worden opgemerkt. Early warning signals worden dan niet of onvoldoende opgemerkt met de daaraan verbonden risico's.

²⁰ Artikel 3 Politiewet 2021: 'De Politie heeft tot taak in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.'

Tot welke praktische problemen leidt dit in de praktijk? (voorbeelden)

- Bij een te beveiligen persoon wordt een verdachte auto opgemerkt die blijkt toe te behoren aan een leasebedrijf. De Politie heeft geen mogelijkheid om dit leasebedrijf te gelasten de gegevens van de leaser vrij te geven.
- Een activistische groepering richt zich op publieke personen. Op social media doet deze groep intimiderende uitspraken en roept op tot actie. Maar er is nog geen strafbaar feit gepleegd en er kan geen strafvorderlijke verdenking worden onderbouwd. De Politie mag dan niet stelselmatig deze groepering op openbare media volgen – wat een burger wel mag doen – of in de besloten groepen meekijken, om de dreiging op de publieke personen te kunnen duiden.
- Potentieel gewelddadige eenlingen onttrekken zich aan het zicht van de autoriteiten. Het is niet te voorspellen tot welke acties zij in staat zijn en wanneer het gaat gebeuren. De Politie mag deze personen niet structureel monitoren, waardoor deze dreiging een black box blijft.

Noodzaak verkenning verruiming wettelijke grondslag

De commissie neemt de hierboven weergegeven signalen van de Politie serieus en meent dat er voor het domein bewaken en beveiligen aanzienlijke risico's zijn verbonden aan de geschatte informatielacunes. Er is een (gebruikelijk) spanningsveld tussen de wens van de Politie om te beschikken over een zo ruim mogelijk wettelijk kader voor opsporings- en beveiligingsactiviteiten enerzijds en andere te beschermen belangen anderzijds, zoals de privacy van burgers en het recht om niet te worden onderworpen aan vergaande inbreuken op de persoonlijke levenssfeer zonder dat sprake is van een strafrechtelijke verdenking. Gezien de complexiteit van het probleem was het voor de commissie, binnen het bestek van deze opdracht en de daarvoor beschikbare tijd, niet mogelijk dit vraagstuk voldoende uit te diepen en te voorzien van een onderbouwd advies. Het vraagstuk verdient echter nadere studie.

De minister van JenV wordt dan ook geadviseerd een juridisch onderzoek te laten uitvoeren naar de vraag in hoeverre de bevoegdheden ten aanzien van informatieverzameling in het kader van bewaken en beveiligen (zowel vanuit perspectief 'dreiger' als 'bedreigde'), binnen de grenzen van de rechtstaat, kunnen worden verruimd. In dit kader heeft de commissie Van den Haak in 2002 aanbevelingen gedaan om voor enkele specifieke functionarissen het mogelijk te maken om gericht informatie te verzamelen (protective intelligence).²¹ Deze aanbevelingen dienen bij het juridisch onderzoek betrokken te worden.

Mocht het tot een verruiming komen van wettelijke mogelijkheden, dan zouden bevoegdheden in deze sfeer uitsluitend moeten toekomen aan ambtenaren die reeds met de opsporing van strafbare feiten zijn belast. De commissie heeft geen taakuitbreiding op dit vlak bij de inlichtingen- en

veiligheidsdiensten voor ogen. Voor bepaalde activiteiten zal daarnaast de toestemming van de te beveiligen persoon noodzakelijk zijn.

7.4 Belemmeringen in informatiepositie inlichtingen- en veiligheidsdiensten

Naast de Politie leveren de inlichtingen- en veiligheidsdiensten AIVD en MIVD dreigingsproducten aan. Deze doen dit alleen binnen het hun toegewezen taakgebied. Ook op dit vlak doet zich een aantal knelpunten voor.

Inlichtingen delen met decentraal domein niet formeel geregeld

De AIVD geeft aan dat er knelpunten bestaan bij het delen van inlichtingen met het decentrale domein. De AIVD is er primair voor het centrale domein, maar heeft regelmatig informatie die relevant is voor het decentrale domein, bijvoorbeeld een dreiging vanuit een statelijke actor tegen een burger die binnen het decentrale bereik valt. De AIVD geeft aan dat zij deze informatie echter niet kan delen. In de Circulaire bewaken en beveiligen is dit ook niet (expliciet) geregeld.

De Circulaire Bewaken en Beveiligen maakt ten aanzien van het aanleveren van informatie geen onderscheid tussen decentraal en rijksdomein. De Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017) maakt dat onderscheid ook niet. In de Circulaire staat wel dat de inlichtingen- en veiligheidsdiensten informatie aanleveren aan de NCTV. Dat impliceert volgens de AIVD dat de dienst in het kader van het stelsel deze informatie uitsluitend via de tussenkomst van de NCTV kan delen met het lokaal bevoegd gezag.

Op dit moment gebruikt de AIVD daarom de NCTV als tussenpersoon om die informatie naar het decentrale domein te vertalen. Het gevolg hiervan is dat functionarissen in het decentrale domein beveiligingsmaatregelen moeten treffen op basis van onvolledige en gefilterde informatie. Dit levert ook op dat niveau een knelpunt op, omdat men vaak meer informatie nodig heeft om tot afgewogen maatregelen te komen.

Aanpassing kaders voor de AIVD

De commissie onderschrijft de wens en noodzaak om de lokale autoriteiten meer direct en ook breder te informeren over dreigingen die in kaart zijn gebracht door de AIVD, maar meent dat het hier geen fundamenteel knelpunt betreft. Waarschijnlijk kan worden volstaan met een aanpassing van de circulaire. Mogelijk is daarnaast sprake van een wettelijke lacune die kan worden meegenomen bij een eerstvolgende aanpassing van de Wiv.

²¹ De commissie stelde toen voor om voor een kleine kring van personen die reeds het voorwerp uitmaken van een gericht beveiligingsbeleid (uitsluitend de limitatieve lijst) een systeem van *protective intelligence* op te zetten. Een dergelijk systeem zou het mogelijk maken om – voor die selecte groep functionarissen – 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.

Hoofdstuk 8

Uitvoering

Centrale boodschap

Gezien de in dit rapport geschetste ontwikkelingen, mag verwacht worden dat de druk op het stelsel de komende jaren blijft toenemen. Het is daarbij aannemelijk dat het stelsel zal worden geconfronteerd met een capaciteitsprobleem waar de recent toegekende versterking maar ten dele in voorziet. Los van dit capaciteitsprobleem, is het in ieder geval zaak om efficiënt, flexibel en innovatief gebruik te maken van het bestaande potentieel. Daarbij is aan de orde het intensiveren van de samenwerking van de stelselpartners, het actief gebruik maken van een flexibele schil van (publiek/private) partners en meer inzet van technologische middelen.

8.1 Capaciteit

Structureel capaciteitstekort in de uitvoering

Op dit moment is de druk op de capaciteit in het stelsel hoog. De toename van het aantal casussen vraagt volgens betrokkenen veel van de betrokken organisaties. De afgelopen jaren is daar een aantal grootschalige en complexe casussen bijgekomen, die leiden tot een forse belasting op de capaciteit. De Politie heeft (tijdelijk) capaciteit vanuit wijkteams uit heel het land onttrokken om deze casussen te kunnen bemensen en de KMar heeft taken moeten herprioriteren. Respondenten geven aan dat deze constructie onwenselijk is en geen duurzame borging biedt voor een toekomstbestendig stelsel. Ook bij het OM, waarop een groot deel van de gezagsverantwoordelijkheid rust, is de druk groot.

De versterkingsgelden die recent beschikbaar zijn gesteld, bieden volgens respondenten in beperkte mate een oplossing. Zo worden bij de Politie de versterkingsgelden onder andere ingezet om per eenheid een Team Bewaken en Beveiligen in te richten (12 fte per eenheid, 120 fte totaal). Deze teams zijn volgens de Politie in beginsel bedoeld voor lokale zaken op het terrein van bewaken en beveiligen waarbij sprake is van een lage dreiging, en bieden geen uitkomst voor bemensing van de zware gevallen en voor de opschalingsstructuur.

Gelet op de analyse van de dreigingsontwikkeling in hoofdstuk 2, schat de commissie in dat de druk op de capaciteit de komende jaren alleen maar zal toenemen. Dit is niet alleen een kwantitatief probleem (voldoende fte en middelen) maar vormt ook een kwalitatieve opgave (beschikbare competenties, samenwerkingsvormen en flexibiliteit). Met enerzijds een toename aan (complexe en grootschalige) casussen en anderzijds een grote uitstroom van personeel door de vergrijzing (in de periode van 2020 tot en met 2025 verlaat ruim 14.000 fte de Politie) wordt die druk alleen maar groter. Daarbij is men afhankelijk van de ontwikkelingen op de arbeidsmarkt waarbij het de vraag is of tijdig voldoende gekwalificeerd personeel kan worden aangetrokken en opgeleid. Het is gezien deze ontwikkelingen aannemelijk dat het stelsel wordt geconfronteerd met een capaciteitsprobleem waarin de recente versterking maar ten dele voorziet. Naast uitbreiding van capaciteit en middelen is het in ieder geval zaak om efficiënt, flexibel en innovatief om te gaan met het bestaande potentieel. Daarbij is aan de orde het intensiveren van de samenwerking van de stelselpartners, het actief gebruik maken van een flexibele schil van (publiek/private) partners en meer inzet van technologische middelen.

Inzichtelijk maken en borgen van capaciteit

Efficiënte inzet van mensen en middelen vergt overzicht van de bestaande casuïstiek en de daarvoor ingezette capaciteit. De commissie verwijst hiervoor naar de in eerdere hoofdstukken beschreven noodzaak tot een actueel landelijk overzicht. Door het ontbreken van die informatie is het voor de commissie niet inzichtelijk of de huidige inzet van capaciteit op de meest effectieve en doelmatige manier plaatsvindt en kan zij derhalve geen onderbouwde uitspraken doen over capaciteitsvraagstukken. Een gegeven is echter dat binnen het stelsel altijd sprake zal zijn van schaarse capaciteit. In dat kader wijst de commissie op de noodzaak om landelijk te denken. De (versterkings)capaciteit is verdeeld over alle regio's/eenheden, maar dat laat onverlet dat capaciteit tijdelijk kan worden ingezet in een andere regio waar extra druk bestaat. Het dashboard – zie hoofdstuk 5 – kan helpen voor het overzicht van capaciteit.

Vervolgens is de vraag of met een andere wijze van werken en/of inzet van andere partijen winst, synergie en schaalvoordelen kunnen worden bereikt. Hieronder schetst de commissie verschillende mogelijkheden daartoe.

Inzet private organisaties

Om capaciteitsproblemen beter het hoofd te kunnen bieden, kunnen, meer dan thans het geval is, de capaciteiten van private bedrijven worden benut. Deels kan dit structureel, deels biedt de inzet van andere partijen de mogelijkheid fluctuaties in werklast op te vangen. Tijdens grote incidenten en op piekmomenten is soms acuut capaciteit en/of specifieke expertise nodig, die later weer afgeschaald worden.

De commissie adviseert daarom om te werken met een flexibele schil aan (publieke en private) partners, die op hun specifieke expertise ingezet kunnen worden op bepaalde taken binnen een beveiligingsconcept. Hiervoor kan gebruik gemaakt worden van een ring aan bedrijven, die zijn gecertificeerd aan de hand van door de overheid vastgestelde normen. De Nederlandse veiligheidsbranche kent bijvoorbeeld een breed palet aan capaciteiten die met name op taken als statische beveiliging, toezicht, observatie, voorverkenningen, bemensing van wachtposten en het volgen en uitlezen van camera-beelden ingezet kunnen worden.

De vrijgespeelde capaciteit van de Politie en/of KMar kan op andere plekken of in een andere rol ingezet worden, waar de specifieke kwaliteit beter tot haar recht komt. Wijkagenten die thans worden inzet in het stelsel kunnen dan weer terug naar hun eigenlijke taak. Dit levert niet alleen maar capaciteitswinst op, maar verhoogt ook de kwaliteit van het beveiligingsconcept. Met het betrekken van de expertise vanuit de private sector, worden de mogelijkheden om een breed palet aan beveiligingsconcepten te ontwikkelen ook groter.

Hoewel functionarissen aangeven in beginsel open te staan voor inzet van private partijen, blijkt in de praktijk sprake te zijn van terughoudendheid. Het probleem is echter urgent en op dit punt moeten nu de nodige stappen gezet worden.

Bij de inzet van private organisaties gelden naar opvatting van de commissie wel drie principiële uitgangspunten:

1. het geweldsmonopolie blijft bij de overheid; de private partijen verrichten ongewapend hun taken;
2. de uitvoering van hun taken valt te allen tijde onder het bevoegde gezag en onder regie van de Politie of KMar;
3. de particuliere beveiliging voldoet aan certificerings- en opleidingseisen die worden vastgesteld door het bevoegde gezag.

Als voorbeeld kan de constructie op Schiphol worden genoemd waarbij de beveiliging van de burgerluchtvaart (ongewapend) door private bedrijven wordt uitgevoerd, onder toezicht van de KMar en onder politieke verantwoordelijkheid van de minister van JenV.

Inzet technologische middelen

Functionarissen geven aan dat naast inzet van private partijen er ook veel kwaliteits- en capaciteitswinst is te halen met het gebruik van (geavanceerde) digitale en technologische middelen. Hiermee zijn de statische taken in een beveiligingsconcept in te vullen. Door het inzetten van sensoren als slimme camera's en technologieën als *artificial intelligence* (AI), is het niet meer nodig om fysieke capaciteit in te zetten op statische taken als toezicht, observaties en het uitkijken van camerabeelden. De vrijgespeelde capaciteit kan ingezet worden om een effectieve respons op meldingen te organiseren. Daarmee is schaarse capaciteit alleen ter plaatse wanneer dat nodig is. De commissie beveelt daarom aan om nieuwe beveiligingsconcepten te ontwikkelen, waarin nieuwe technologieën zijn verwerkt en deze in pilotvorm in de praktijk te testen. Ook kunnen private partijen worden ingeschakeld die veelal al gebruik maken van dit soort technieken. Daarbij is het zaak innovatiekracht te bundelen in plaats van het zelfstandig en versnipperd ontwikkelen van trajecten door elk organisatieonderdeel.

8.2 Samenwerking uitvoerende partners

Noodzaak aanbrengen van meer synergie in de samenwerking binnen het stelsel

Bewaken en beveiligen behoren tot de algemene Politietaken. De KMar verricht, naast de in de Politiewet genoemde taken (waaronder bewaken en beveiligen van objecten, Koningshuis en speciale beveiligingsopdrachten) vanuit de algemene bijstandstaak aan de Politie, werkzaamheden op het terrein van bewaken en beveiligen. In de bijstandsconstructie opereert de KMar onder regie en leiding van de Politie. De Politie heeft de bewaken en beveiligen taak tot op heden grotendeels als neventaak ingericht, waarbij elke Politie-eenheid bovendien eigen ruimte heeft gehad voor invulling.

De Politie en KMar hebben hun eigen afzonderlijke wettelijke taken op het gebied van bewaken en beveiligen. Beide organisaties hebben hun eigen unieke expertises en capaciteiten. Daarmee zijn ze complementair aan elkaar. Tegelijkertijd constateert de commissie dat er een gebied is waarin de Politie en de KMar vergelijkbare taken verrichten in het stelsel, maar grotendeels apart van elkaar werken. Ook in het verbetertraject investeren beide organisaties in de eigen informatiepositie, in eigen opleidingen, in eigen middelen en eigen inzet. Er wordt versnipperd geïnvesteerd in de toepassing van nieuwe technologieën, zoals slim cameratoezicht. Ondanks bestaande vormen van samenwerking wordt er nog veel langs elkaar heen gewerkt. Dat levert energieverlies op, hetgeen disfunctioneel is en het stelsel onnodig

belast. Daarbij wordt het werkveld complexer en is er toenemende schaarste aan personeel, capaciteiten en middelen. Het gescheiden opereren van de partners wordt dan steeds problematischer en is daarmee niet uit te leggen.

Intensieve samenwerking op basis van gelijkwaardigheid

De commissie ziet geen reden om de formele taakverdeling tussen Politie en KMar en de wettelijke basis van de inzet van beide Politieorganisaties te wijzigen. De bijstandsconstructie mag echter geen barrière vormen voor het zoveel mogelijk samen optrekken van de beide organisaties. Het vakgebied bewaken en beveiligen moet gezamenlijk worden (door)ontwikkeld. Zeker nu de casussen complexer worden en de bijstand van de KMar aan de Politie steeds vaker een langdurig karakter krijgt, is de noodzaak van goede samenwerking en afstemming evident. De commissie ziet een versterkte samenwerking in ieder geval op de volgende gebieden:

- *samenwerking in de uitvoering*
Spreek in de uitvoering duidelijk af wie waarvoor aan de lat staat en bepaal op basis daarvan waarin gezamenlijk opgetrokken kan worden. Inzetconcepten kunnen dan gezamenlijk worden ontwikkeld en waar mogelijk wordt ook in de uitvoering gewerkt in gezamenlijke teams. Hiermee moet een breed palet aan concepten ontstaan die aansluiten bij de pakketten per risiconiveau, zodat het stelsel flexibel kan inspelen op de uitdagingen.
- *samenwerking in de opleidingen*
Opleidingen en trainingen worden zoveel mogelijk gezamenlijk ontwikkeld en gevolgd. Dit lijdt slechts uitzondering waar het kennis en vaardigheden betreft die zijn gekoppeld aan een inzet die specifiek wordt uitgevoerd door een van de twee organisaties. Eindtermen en certificeringen zijn gelijk of worden op elkaar afgestemd. Dit maakt dat functionarissen moeiteloos en complementair aan elkaar in verschillende concepten zijn in te zetten. Met aanvullende modules en/of opleidingen kan daarbij de eigen unieke expertise geborgd worden.
- *samenwerking op het gebied van innovatie*
Bij de ontwikkeling van beveiligingsconcepten speelt inzet van slimme technologie een belangrijke rol. Er is een innovatieagenda bewaken en beveiligen nodig die kennis bundelt en de slagkracht vergroot. De innovatieagenda wordt gezamenlijk ontwikkeld, waarbij een team van Politie en KMar de uitwerking ter hand neemt.

Van de leiding van beide organisaties mag worden verwacht dat zij de noodzaak tot intensieve samenwerking actief uitdraagt en bevordert. Niet zozeer de eigenheid van de organisatie moet worden benadrukt maar de gezamenlijke opdracht en de opgave om samen op te trekken op dit precaire terrein. Hier ligt een belangrijke taak voor de leiding van de betrokken organisaties die deel uit gaan maken van de geadviseerde Vierhoek bewaken en beveiligen.

Hoofdstuk 9

Perspectief van een te beveiligen persoon

Centrale boodschap

Een toekomstbestendig stelsel stelt de beveiligde persoon meer centraal, investeert in diens weerbaarheid en heeft oog voor de implicaties die de maatregelen met zich meebrengen.

9.1 Inleidend

In dit rapport wordt het stelsel vanuit een sterk organisatorisch en bestuurskundig perspectief beschreven. Daarbij moet niet uit het oog worden verloren dat het uiteindelijk gaat om de veiligheid van een persoon en zijn of haar omgeving. De commissie achtte het van groot belang om het perspectief van een beveiligde persoon te betrekken in de gedachtevorming over een toekomstbestendig stelsel en heeft daartoe met enkele (voormalig) beveiligde personen gesproken. Ook heeft de commissie gebruik gemaakt van het 'Onderzoek psychosociale effecten van bedreiging en beveiliging'²² dat in opdracht van de NCTV door het Nationaal Psychotrauma Centrum is uitgevoerd.

9.2 Belangrijkste lessen

Impact op het dagelijkse leven

De impact van beveiligingsmaatregelen mag niet onderschat worden. Op verschillende manieren heeft het ingrijpende gevolgen voor het dagelijkse leven van een persoon en diens gezin. In een zwaar beveiligingsconcept moet een persoon zijn of haar leven zoveel mogelijk vooruit plannen en steeds een agenda aan de autoriteiten overhandigen, zodat daarop de fysieke beveiliging georganiseerd kan worden. Dit betekent in de praktijk dat vrijheid en flexibiliteit ingeperkt wordt. In extreme situaties kan het voorkomen dat een persoon 24 uur per dag beveiligers om zich heen heeft of dat deze het eigen huis moet verlaten om elders in een *safehouse* te verblijven. Al deze maatregelen hebben ingrijpende gevolgen in een situatie die toch al leidt tot stress en onveiligheidsgevoelens.

Investeren in weerbaarheid en psychosociale (na)zorg

In een toekomstbestendig stelsel moet het welbevinden van een te beveiligen persoon een goede plaats krijgen. Psychosociale (na)zorg behoort een vast onderdeel te zijn van de standaardpakketten. Afhankelijk van de behoefte van de te beveiligen persoon kan de invulling in overleg bepaald worden. Belangrijk daarbij is de overgangsfase waarin de beveiligingsmaatregelen worden afgebouwd en betrokkene weer naar de normale situatie gaat.

Investeren in weerbaarheid functionarissen

Daarnaast wordt aanbevolen om te investeren in het (preventief) weerbaarder maken van functionarissen die in de uitoefening van hun taak te maken krijgen met ernstige dreiging, zodat zij daarmee beter kunnen leren omgaan. En als de dreiging vervolgens zo hoog wordt dat er (mogelijk) maatregelen moeten worden getroffen, dat zij leren om te gaan met het leven met beveiligingsmaatregelen en de onzekerheid die daarmee gepaard gaat. Hier ligt primair een taak voor de werkgevers en de brancheorganisaties, waarbij de NCTV als stelselverantwoordelijke een faciliterende rol kan spelen door het delen van *good practices* en het in kaart brengen van adequate trainingen en opleidingen.

Informatie, communicatie en uitvoering

Hoewel er verschillen zijn en zeker ook goede voorbeelden, geven beveiligde personen in het onderzoek van IVP aan dat de informatievoorziening vanuit de overheid gebrekkig is. Dit kan de aard en herkomst van de dreiging betreffen, maar ook de communicatie over de beveiligingsmaatregelen zelf laat soms te wensen over. In een situatie waarin een persoon zich al onveilig voelt en daardoor alerter en wantrouwend is, kan de opstelling van de overheid die geen informatie deelt – hoe begrijpelijk dat soms ook is – dat gevoel verergeren.

²² Rapport Onderzoek Psychosociale effecten van bedreiging en beveiliging (2020), ARQ Kenniscentrum Impact van Rampen en crisis en ARQ IVP.

In dit verband wordt het gemis ervaren van een vast aanspreekpunt. Zo kan het zijn dat een persoon contact heeft met zowel functionarissen van het gezag (OM/NCTV) als de uitvoering (Politie/KMar). Ook binnen de uitvoering heeft men vaak te maken met verschillende contactpersonen. Deze onduidelijkheid wordt mede veroorzaakt door de versnipperde inrichting van het stelsel – zoals beschreven in hoofdstuk 5 – en de rolvermenging van partners, waardoor het voor een persoon niet helder is wie nu waar over gaat.

Transparantie en het gevoel van regie

Door een te beveiligen persoon het gevoel te geven ‘in control’ te zijn, wordt diens veiligheidsgevoel vergroot en groeit het vertrouwen in het stelsel. Dit heeft niet alleen effect op de beleving van de te beveiligen persoon maar verhoogt ook de effectiviteit van het beveiligingsconcept als geheel.

Communicatie en transparantie binnen de gegeven kaders en beperkingen is belangrijk. De commissie beseft dat niet zonder meer vertrouwelijke dreigingsinformatie gedeeld kan worden, maar er is wellicht een tussenweg te vinden waarbij niet te snel moet worden gewezen op louter juridische kaders.

Daarnaast is het belangrijk om de te beveiligen persoon te betrekken bij de uitvoering van het beveiligingspakket, door goed uit te leggen waarvoor bepaalde maatregelen noodzakelijk zijn en vervolgens gezamenlijk te kijken hoe dit pragmatisch ingevuld kan worden. Daarbij benadrukt de commissie dat deze ‘invulruimte’ sterk afhankelijk is van de dreigingsinschatting op dat moment. Uiteindelijk gaat het bieden van bescherming (de primaire doelstelling van het stelsel) altijd voor op het bieden van comfort.

Ten slotte adviseert de commissie aan een te beveiligen persoon een vast contactpersoon toe te wijzen met een vaste vervanger (bij ziekte en verlof), bij wie deze met alle vragen terecht kan, naar analogie van de ‘familiechercheur’ bij de politie. Deze functionaris fungeert als het aanspreekpunt namens de overheid en verzamelt bij betrokken organisaties de antwoorden op vragen van de beveiligde persoon.

Deel IV

Bijlagen



STAATSCOURANT

Nr. 25135

20 mei

2021

Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.

Regeling van de Minister van Justitie en Veiligheid van 3 mei 2021, nr. 3291895, houdende instelling van het adviescollege toekomstbestendig stelsel bewaken en beveiligen

De Minister van Justitie en Veiligheid en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties;

Handelende in overeenstemming met het gevoelen van de ministerraad;

Gelet op artikel 6, eerste lid, van de Kaderwet adviescolleges;

Besluiten:

Artikel 1

Er is een adviescollege toekomstbestendig stelsel bewaken en beveiligen.

Artikel 2

Het adviescollege heeft tot taak het stelsel bewaken en beveiligen te beoordelen en voorstellen te doen om het toekomstbestendig te maken, zodat zij het hoofd kan blijven bieden aan huidige en toekomstige dreigingen in een steeds complexer wordende samenleving.

Artikel 3

Het adviescollege bestaat uit een voorzitter en twee andere leden.

Artikel 4

1. Het adviescollege brengt zijn advies uit voor 1 juli 2021 aan de minister van Justitie en Veiligheid.
2. Na het uitbrengen van het advies is wordt het adviescollege opgeheven.
3. De voorzitter kan tot 1 juni 2021 aan de Minister van Justitie en Veiligheid om uitstel verzoeken voor wat betreft het uitbrengen van het eindrapport.
4. Een verzoek tot uitstel van het eindrapport is met redenen omkleed en vermeldt een nieuwe einddatum die redelijk is ten opzichte van de in lid 1 genoemde datum.

Artikel 5

De archiefbescheiden van het adviescollege worden na zijn opheffing of, zo de omstandigheden daartoe eerder aanleiding geven, zoveel eerder, overgebracht naar het archief van de NCTV van het ministerie van Justitie en Veiligheid.

Artikel 6

Deze regeling treedt in werking met ingang van de dag na uitgifte van de Staatscourant waarin zij wordt geplaatst en vervalt met ingang van het uitbrengen van het eindrapport van het adviescollege.

Artikel 7

Deze regeling wordt aangehaald als: Regeling instelling adviescollege toekomstbestendig stelsel bewaken en beveiligen.



Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

*De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus*

*De Staatssecretaris van Binnenlands Zaken en Koninkrijksrelaties,
R.W. Knops*



TOELICHTING

Het huidige stelsel bewaken en beveiligen (hierna: stelsel) is in 2002 ingericht. Het doel van het stelsel is het voorkomen van (terroristische) aanslagen op personen, objecten en diensten. In het stelsel is geregeld hoe op basis van informatie over dreiging en risico tot beveiligingsmaatregelen wordt besloten. Bij bewaken en beveiligen zijn veel partijen betrokken: politie, OM, lokale besturen, inlichtingen- en veiligheidsdiensten, ministeries en de NCTV. De verantwoordelijkheid voor het stelsel is namens de Minister van Justitie en Veiligheid belegd bij de NCTV.

In het kader van het brede offensief tegen ondermijnende criminaliteit investeert het kabinet de komende jaren structureel in de versterking van het stelsel. Het goed functioneren van het stelsel vraagt echter niet alleen om voldoende capaciteit, maar ook om kwaliteitsontwikkeling en kennisborging. Daarbij is het van belang om, in lijn met de ingezette kwaliteitsverbeteringen binnen het stelsel, ook naar het functioneren van het stelsel als geheel en de wijze waarop deze is ingericht te kijken. In de Kamerbrief d.d. 13 nov. 2020¹ heeft de Minister van Justitie en Veiligheid toegezegd een externe commissie, vanuit een afstandelijk perspectief, naar het stelsel te laten kijken en voorstellen te laten doen op welke wijze het stelsel toekomstbestendig gemaakt kan worden om blijvend het hoofd te bieden aan huidige en toekomstige dreigingen.

Het is van belang dat dit door een onafhankelijk adviescollege gebeurt, om te voorkomen dat de belangen van de bij het stelsel betrokken partners het kijken naar het functioneren van het stelsel te veel kleurt. Om duurzame verbeteringen door te kunnen voeren is een onafhankelijke, kritische blik op het stelsel nodig, te meer er de afgelopen jaren verschillende terugkerende knelpunten en vraagstukken zijn geconstateerd.

Het instellen van een eenmalig adviescollege is nodig, omdat dit vraagstuk niet ondergebracht kan worden bij een reeds bestaand adviescollege. Er is geen bestaand adviescollege met expertise over het beleidsterrein van bewaken en beveiligen.

Voor de samenstelling van het adviescollege is gekeken naar personen die kennis hebben van en/of affiniteit hebben met het domein of de betrokken organisaties, maar deze niet representeren.

Het college is verzocht om advies uit te brengen middels een eindrapport op uiterlijk 1 juli 2021. Het adviescollege wordt met terugwerkende kracht vanaf 10 februari 2021 ingesteld, aangezien de collegeleden al op dat moment met hun werkzaamheden zijn begonnen. Na het uitbrengen van het advies wordt dit adviescollege opgeheven en het instellingsbesluit worden ingetrokken.

¹ Kst. 29911-292

Samenstelling commissie, staf en klankbordgroep

Commissie

J.G. (Gertjan) Bos (voorzitter)

Ambtelijke loopbaan bij verschillende ministeries. Diverse leidinggevende functies in beleid, uitvoering en toezicht. Laatstelijk als Inspecteur-Generaal van de Inspectie Justitie en Veiligheid.

M.A. (Magda) Berndsen

Toezichthouder, actief in diverse adviescommissies. Voormalig burgemeester, korpschef en Tweede Kamerlid.

J.J. (Jacques) van Eck

Voormalig hoofdofficier van Justitie. Tot 1 september 2021 staatsraad in de Afdeling bestuursrechtspraak van de Raad van State.

Staf

A. (Anup) Jagan, Secretaris

D.W.P. (Dennis) van Loon, Plv. Secretaris

Klankbordgroep

R.G.C. (Ruud) Bik

Voormalig korpschef van het Korps Landelijke Politie Diensten en plv. korpschef van de Nationale Politie.

Prof. mr.dr. E.R. (Erwin) Muller

Hoogleraar Veiligheid en Recht, Universiteit Leiden. Decaan Faculteit Governance and Global Affairs en bestuurder van de campus Den Haag van de Universiteit Leiden.

D. (Dick) van Putten

Luitenant-generaal b.d.. Voormalig commandant der Koninklijke Marechaussee en Gouverneur der Residentie.

B.W.J. (Bob) Steensma

Plv. voorzitter College gerechtelijk deskundigen, actief in diverse adviescommissies/colleges. Voormalig Hoofdofficier van Justitie en bestuurder.

M. (Marco) Zannoni (tot 1 juli)

Directeur COT, Instituut voor Veiligheids- en Crisismanagement.

Lijst respondenten

AIVD

- DG AIVD
- Directeur operaties
- Adviseur bewaken en beveiligen

Experts

- Voormalig directeur bewaken en beveiligen en tevens CBB
- Criminoloog en emeritus hoogleraar
- (Voormalig) te beveiligen personen
- Voorzitter en secretaris van de Nederlandse Veiligheidsbranche

KMar

- Commandant KMar
- Hoofd Bewaken en Beveiligen
- Senior adviseur bewaken en beveiligen

NCTV

- NCTV
- Directeur Nationale Crisisbeheersing en Bewaken en beveiligen
- Coördinator Bewaken en beveiligen

Openbaar ministerie

- Portefeuillehouder bewaken en beveiligen in het College van Procureurs-Generaal
- HOvJ en tevens portefeuillehouder bewaken en beveiligen
- Landelijk BB&C
- BB&C's Den Haag en Rotterdam

Politie

- Korpschef
- Politiechef en tevens portefeuillehouder bewaken en beveiligen
- Sectorhoofd Dienst Regionale Operationele Samenwerking
- Voorzitter regieteam opschalingsstructuur
- Teamchef Informatieknoppunt Bewaken en beveiligen DLIO

Stuurgroep bewaken en beveiligen

- Meerdere groepsinterviews

Geraadpleegde bronnen

Onderzoeksrapporten

- ARQ Kenniscentrum Impact van Rampen en crisis en ARQ IVP, *Rapport Onderzoek Psychosociale effecten van bedreiging en beveiliging*, 2020
- Bureau Beke, *Bescherming van personen: Ontwikkelingen in de dreiging vanuit de georganiseerde criminaliteit*, december 2018
- Commissie Eenhoorn, *Conclusies en aanbevelingen Onderzoeksrapport TweeSteden*, mei 2016
- Commissie feitenonderzoek veiligheid en beveiliging Pim Fortuyn ('Commissie Van den Haak'), *'De veiligheid en de beveiliging van Pim Fortuyn 'feiten en verantwoordelijkheden'*, december 2002
- De Wijk, R., *Het stelsel Bewaken en Beveiligen na Pim Fortuyn*, The Hague Centre for Strategic Studies, 2012
- Fijnaut, C., *De herinrichting van het stelsel van speciale eenheden*, mei 2004
- Inspectie Openbare Orde en Veiligheid (thans Inspectie Justitie en Veiligheid), *Koninginnedag 2009: Een onderzoek door de Inspectie Openbare Orde en Veiligheid*
- Inspectie Justitie en Veiligheid, *Inspectieonderzoek naar de aanpak van de stalking door Bekir E.*, oktober 2019
- Inspectie Justitie en Veiligheid, *Onderzoek naar de taakuitvoering bij de Landelijke Eenheid / DLIO*, januari 2021
- Korten, M.C.P., *Getuigenbescherming in Nederland*, 2015
- NCTV, *Evaluatie veiligheid Nuclear Security Summit 2014*

Kamerstukken

- Brief van de regering, *Uitwerking breed offensief tegen georganiseerde ondermijnende criminaliteit*, 18 juni 2020
- Brief van de regering, *Voortgang aanpak ondermijnende criminaliteit*, 13 november 2020
- Brief van de regering, *Capaciteitsversterkingen Bewaken en Beveiligen* 8 februari 2021
- Circulaire met betrekking tot de bewaking en beveiliging van personen, objecten en diensten 2019, geldend van 01-07-2019 t/m heden, regeling vervalt per 30-06-2023
- Nota Nieuw stelsel van bewaken en beveiligen; Tweede Kamer der Staten-Generaal, Kamerstuk 28974 nr. 2

Overige documenten

- Politie, *Raamregeling Team Grootschalig Bewaken & Beveiligen*, 23 november 2018
- Politie, *Programmaplan Duurzaam Bewaken & Beveiligen 2019-2023*, 9 mei 2019
- Politie, *Werkdocument Team Bewaken & Beveiligen*, 2 juni 2020
- Politie, *Programma Bewaken en Beveiligen: maatregelen 2021-2024*, 1 juli 2020
- OM, *Instructie bewaken en beveiligen van personen, objecten en diensten*, 2016
- NCTV, *Questionnaire Surveillance and Protection System*, 6 august 2018
- U.S. Department of Justice Office of Justice Programs National Institute of Justice, *Protective Intelligence and Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials*, 2000

Position papers

- Position paper AIVD, 18 maart 2021
- Position paper Openbaar Ministerie, 7 juni 2021
- Position paper Politie, april 2021

Verslagen

- Selectie verslagen van Stuurgroep bewaken en beveiligen periode 2014-2021
- Selectie verslagen Uitvoeringsoverleg periode 2020-2021
- Selectie verslagen Afstemmingsoverleg periode 2020-2021
- Selectie verslagen Capaciteitsoverleg periode 2019-2021
- Verslagen van het Directeurenoverleg 'project georganiseerde criminaliteit in relatie tot bescherming van personen' periode 2018
- Verslaglegging van het werkbezoek Italiaanse delegatie in Nederland, in het kader van het project georganiseerde criminaliteit in relatie tot bescherming van personen, 30-07-2018
- Verslag 'Uitkomsten juridische kennissessie inzake de zorgplicht van de overheid in relatie tot de bescherming van personen', 30-10-2018

Lijst met afkortingen

ABB	Afstemmingsoverleg Bewaken Beveiligen	DRIO	Dienst Regionale Informatie Organisatie van de Regionale Eenheid van de Nationale Politie
AIVD BB&C	Algemene inlichtingen en veiligheidsdienst (Beleidsmedewerker) Bewaken, Beveiligen en Crisisbeheersing van de parketten bij het Openbaar Ministerie	DSO	Dienst Speciale Operaties van de Landelijke eenheid van de Politie
BLOOS	Analysemodel bij de politie om een situatieschets te maken: Beleidsuitgangspunten, Locatie, Omstandigheden, Object, Daders en Slachtoffers.	DTN	Dreigingsbeeld Terrorisme Nederland
BSB	Brigade Speciale Beveiligingsopdrachten van de Koninklijke Marechaussee	HOvJ	Hoofdofficier van Justitie van het Openbaar Ministerie
BVA	Beveiligingsambtenaar	HRB	Hoog Risico Beveiliging van de Koninklijke Marechaussee
CBB	Coördinator Bewaken en Beveiligen van de Nationaal Coördinator Terrorismebestrijding en Veiligheid	IBB	Integraal Besluitvormingsberaad (onderdeel van opschalingsstructuur bij grote casussen bewaken en beveiligen)
CCB	(Portefeuillehouder) Conflict en Crisisbeheersing van de regionale politie eenheid	IKBB	Informatieknooppunt Bewaken en Beveiligen van de Dienst Landelijke Informatieorganisatie.
Circulaire	Circulaire met betrekking tot de bewaking en beveiliging van personen, objecten en diensten	IRS	Analysemodel bij de politie om scenario's in kaart te brengen en daarbij kans, risico en effect te schetsen.
DA	Dreigingsanalyse	JenV	Justitie en Veiligheid
DKDB	Dienst Koninklijke en Diplomatieke Beveiliging van de Landelijke Eenheid van de Nationale Politie	IRD	Informatierapport dreiging
DI	Dreigingsinschatting	KMar	Koninklijke Marechaussee
DPG	Directie Protocol en Gastlandzaken van het Ministerie van Buitenlandse Zaken	MIVD	Militaire inlichtingen en veiligheidsdienst
DLIO	Dienst Landelijke Informatie Organisatie van de Landelijke Eenheid van de Nationale Politie	NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
DRIO	Dienst Regionale Informatieorganisatie van de Nationale Politie	OM	Openbaar Ministerie
DLOS	Dienst Landelijke Operationele Samenwerking van de Landelijke Eenheid van de Nationale Politie	OvV	Onderzoeksraad voor Veiligheid
DNB	De Nederlandsche Bank	PBB	Programma bewaken en beveiligen (NCTV)
		RA	Risicoanalyse
		RCCB	(Afdeling) Regionale Conflict en Crisisbeheersing van de Regionale Eenheid van de Nationale Politie
		SGBO	Staf Grootchalig en Bijzonder Optreden

Stelsel	Stelsel Bewaken en Beveiligen
TBP	Te Beveiligen Persoon
TGBB	Team Grootschalig Bewaken en Beveiligen (opschalingsstructuur bij grote casussen)
UO	Uitvoeringsoverleg
VCI	Directie Veiligheid, Crisisbeheersing en Integriteit van het Ministerie van Buitenlandse Zaken
VKL/VKU	Vaste kern Leidinggevend/Vaste kern Uitvoering (onderdeel van opschalingsstructuur bij grootschalige casussen bewaken en beveiligen)
WIV 2017	Wet op de inlichtingen en veiligheidsdiensten 2017



Universiteit Leiden

Dreigingsontwikkelingen relevant voor het stelsel bewaken en beveiligen: een blik op verleden en mogelijke toekomst

Bart Schuurman, Jelle van Buuren en Edwin Bakker

ISGA Rapport

Dreigingsontwikkelingen relevant voor het stelsel bewaken en beveiligen: een blik op verleden en mogelijke toekomst

Bart Schuurman, Jelle van Buuren en Edwin Bakker

3 augustus 2021

Dit rapport is opgesteld in opdracht van het ‘Adviescollege toekomstbestendig stelsel bewaken en beveiligen’. Het college bestaat uit de leden de heer Gertjan Bos (voorzitter), mevrouw Magda Bernds-Jansen en de heer Jacques van Eck en wordt ondersteund door ambtelijk secretaris de heer Anup Jagan.

© 2021, Schuurman / Van Buuren / Bakker, Universiteit Leiden

De auteurs bedanken Jessy Hendriks en Erwin Muller voor hun hulp bij het tot stand komen van dit rapport.

Dit rapport is onderdeel van een reeks uitgegeven door het Institute of Security and Global Affairs (ISGA) van de Universiteit Leiden.

ISSN 2452-0551
e-ISSN 2452-056X

Omslagontwerp: Oscar Langley
www.oscarlangley.com

Inhoudsopgave

Inleiding en achtergrond	4
Stelselrelevante dreigingen, 2000-heden	6
<i>Jaren 1970-2000</i>	6
2002	6
2003	7
2004 & 2005	7
2006	8
2007-2009	8
2010	9
2011	10
2012	10
2013 & 2014	11
2015	11
2016	12
2017	12
2018	13
2019	15
2020	16
2021	18
Dreiging in cijfers	21
<i>Internationale vergelijking</i>	25
Ontwikkeling stelselrelevante dreigingen	26
1. <i>Fluctuatie en nuancering</i>	26
2. <i>De actie-reactie cyclus</i>	27
3. <i>Verruwing en toenemend geweld vanuit de georganiseerde misdaad</i>	27
4. <i>Aanhoudende terroristische dreiging</i>	28
5. <i>(On)voorstelbare dreigingen</i>	29
6. <i>Dreigers met mentale-gezondheid gerelateerde problematiek</i>	29
7. <i>Internet, complotdenken en de dreiging van statelijke actoren</i>	29
8. <i>Dreigingen van binnenuit</i>	30
9. <i>De grote invloed van (internationale) incidenten en ontwikkelingen</i>	31
10. <i>Een brede groep bedreigden</i>	31
<i>Valkuilen van vooruitblikken</i>	32
Conclusie	33
Geraadpleegde bronnen	36

Inleiding en achtergrond

Op 10 februari 2021 is door de ministerraad een adviescollege ingesteld om bij te dragen aan de toekomstbestendigheid van het stelsel bewaken en beveiligen.¹ Het stelsel bewaken en beveiligen (verder ‘het stelsel’) wordt vormgegeven door verschillende overheidsdiensten op nationaal en lokaal niveau en omvat ‘het geheel van regelgeving en afspraken die gaan over het voorkomen van aanslagen op personen, objecten en diensten’.² Kerntaak van het college is om voorstellen te doen ter waarborging van de effectiviteit van het stelsel om nu en in de toekomst deze beschermende taken te kunnen uitvoeren.³ Om deze adviserende rol te vervullen, wenst het college onder andere inzicht te krijgen in de aard van de dreigingen waar het stelsel de komende jaren mee te maken krijgt. Dit heeft in mei 2021 geleid tot een vraag aan de Universiteit Leiden om aan de hand van een beknopte beschouwing de te verwachten ontwikkelingen in kaart te brengen.

De Universiteit Leiden voorziet in deze behoefte door het voorliggende rapport. Op basis van relevante wetenschappelijke studies, overheidsrapportages en andere publicaties schetsen de volgende pagina’s hoe de dreigingen die het stelsel hebben geconfronteerd zich sinds de eeuwwisseling hebben ontwikkeld. Dit feitelijke overzicht wordt aangevuld met de beschikbare cijfers over (ernstige) bedreigingen van onder andere politici, ambtsdragers en journalisten in Nederland. Ook wordt gebruik gemaakt van de inschattingen van wetenschappers met domeinrelevante kennis die in een expertsessie naar hun inzichten over mogelijke dreigingsontwikkelingen zijn gevraagd.⁴ Hun inzichten zijn verwerkt in het descriptieve deel van het rapport. Deze informatiebronnen dienen vervolgens als fundering voor een reflectie op voor het stelsel relevante ontwikkelingen qua aard en omvang van de dreiging die naar verwachting ook de komende jaren beeldbepalend zullen zijn. Afsluitend volgt een korte beschouwing op de valkuilen van vooruitblikken op dreigingsontwikkelingen, om zo de bevindingen van de juiste nuance en context te voorzien.

Overeenkomstig met de wens van het adviescollege wordt in dit rapport een breed perspectief gehanteerd op dreigingen die het werkveld van het stelsel raken. Daarmee komt direct een lastige vraag naar voren, want de invulling van ‘stelselrelevante dreigingen’ hangt nauw samen met hoe tegen de reikwijdte van het stelsel wordt aangekeken.⁵ Als bijvoorbeeld naast directe fysieke bedreigingen ook de waarborging van het ongestoord functioneren van politici en ambtenaren tot de verantwoordelijkheid van stelsel wordt gerekend, dan zou beargumenteerd kunnen worden dat optreden tegen cyberspionage en digitale desinformatiecampagnes daar ook bij hoort.⁶ Een heldere afbakening van de verantwoordelijkheden en reikwijdte van het stelsel lijkt zo direct al een belangrijke voorwaarde voor effectief functioneren in de toekomst.

In navolging van de ‘Circulaire bewaking en beveiliging 2019’ worden stelselrelevante dreigingen in eerste instantie gezien als dreigingen tegen personen, objecten en diensten. Bij die eerste categorie gaat het dan met name om de dreiging van een ernstige schending van de

¹ Minister van Justitie en Veiligheid, ‘Instelling van het adviescollege toekomstbestendig stelsel’.

² Openbaar Ministerie, Politie Nederland en NCTV, ‘Factsheet: stelsel bewaken en beveiligen.’

³ Nationaal Coördinator Terrorismebestrijding en Veiligheid, ‘Bewaken en beveiligen.’

⁴ De expertsessie vond digitaal plaats op 9 juni 2021. Aanwezig waren (naast de auteurs van dit rapport) twee medewerkers van het Ministerie van Binnenlandse Zaken, drie medewerkers van de politie, twee medewerkers van de NCTV, een wetenschapper verbonden aan het ICCT en een medewerker van de Universiteit Leiden die notuleerde.

⁵ Medewerker Ministerie van Binnenlandse Zaken, Bijdrage aan de expertsessie; Medewerker Politie 2, Bijdrage aan de expertsessie.

⁶ Algemene Inlichtingen- en Veiligheidsdienst, ‘Jaarverslag AIVD 2020,’ 16.

fysieke integriteit.⁷ Om te kunnen voldoen aan de wens om stelselrelevantie dreigingen vanuit een breed perspectief te bekijken, wordt in dit rapport ten aanzien van concrete bedreigingen tegen personen zowel gekeken naar uitingen van de intentie ‘om iemand, of diens naasten, wat aan de toen’ als het meer ambigue ‘intimidatie’ waarbij het vooral gaat om het oproepen van ‘een gevoel van onveiligheid bij de getroffene’.⁸ Er wordt ook rekening gehouden met dreigingen voor het functioneren van ambtsdragers, politici en de rechtsstaat in bredere zin. Bovendien wordt niet alleen gekeken naar directe bronnen van dreigingen, zoals georganiseerde misdaad of boze burgers, maar ook naar ontwikkelingen die aanleiding kunnen geven voor een verandering in de ernst of omvang van dreigingen, zoals de groei van complotdenken. Tevens is het belangrijk om te benadrukken dat er een brede blik op de bedreigden wordt gehanteerd; van ambtenaren en politici tot journalisten, medewerkers van het Openbaar Ministerie en de politie, personen actief binnen de Rechtspraak en leden van diasporagemeenschappen.

Tot slot nog kort wat *niet* aan bod komt. Dit rapport is geen evaluatie van hoe het stelsel de afgelopen jaren heeft gefunctioneerd in operationele of beleidsmatige zin. De organisatie van het stelsel of de samenwerking tussen de betrokken partijen komen evenmin aan bod. Het gaat hier specifiek om een bespiegeling op de ontwikkeling van stelselrelevante dreigingen en de vraag welke de komende jaren als bijzonder relevant worden geacht.

⁷ ‘Circulaire met betrekking tot de bewaking en beveiliging,’ paragraaf 1.

⁸ Klein Kranenburg et al., ‘Bedreigingen en intimidaties van burgemeesters,’ 6.

Stelselrelevante dreigingen, 2000-heden

Met welke typen dreigingen heeft het stelsel de afgelopen twee decennia te maken gehad? Het volgende chronologisch overzicht maakt dit inzichtelijk. Zo wordt de basis gelegd voor een reflectie op de trends en ontwikkelingen die ook de komende jaren relevant zullen zijn.

Jaren 1970-2000

Tot de moord op Pim Fortuyn in 2002 was er in Nederland weinig belangstelling voor het opzetten van een systeem voor persoonsbeveiliging waar in principe iedere ernstige bedreigde Nederlander aanspraak op zou kunnen maken. De destijds geldende afspraken en maatregelen, die vanaf de jaren 1970 waren ontstaan, waren vooral geënt op het voorkomen van terroristische aanslagen tegen specifieke objecten en personen, in het bijzonder het Koninklijk Huis, diplomaten en andere buitenlandse vertegenwoordigers. Nederlandse burgers, maar ook de meeste politici, bestuurders, ambtenaren, magistraten, advocaten en andere beroepsgroepen waarbij blootstelling aan bedreigingen en intimidatie voorstelbaar is, werden in eerste instantie op hun eigen verantwoordelijkheid voor het nemen van beveiligingsmaatregelen gewezen. Bovendien werden beveiligingsmaatregelen slechts getroffen wanneer er sprake was van een concrete dreiging en dus niet in gevallen waar de dreiging slechts voorstelbaar was.⁹

Vanaf de jaren 1980 krijgt de bestrijding van georganiseerde misdaad in Nederland meer prioriteit. Een belangrijke ontwikkeling is de aanvulling van de strafrechtelijke aanpak met bestuurlijke middelen, waardoor lokale overheden gaandeweg de jaren '90 een grotere rol gaan spelen in misdaadbestrijding.¹⁰ Ook worden officieren van justitie prominenter afgebeeld als *crime fighters*, wat hen in de ogen van sommige criminelen een persoonlijke tegenstander maakt in plaats van slechts een representant van het Openbaar Ministerie. Met name vanuit de georganiseerde misdaad wordt op deze ontwikkelingen gereageerd door toenemend gebruik van bedreiging en intimidatie richting openbaar bestuurders, medewerkers van politie en justitie, en leden van de advocatuur.¹¹ Bedreiging en intimidatie lijkt niet alleen vaker voor te komen, het wordt ook opzichtiger in verschijningsvorm; bijvoorbeeld door inbraak en ontvoering.¹² Ook politiek gemotiveerd geweld komt voor, zoals aanslagen op de Centrum Democraten in 1986 en staatssecretaris Aad Kosto in 1991.¹³ Toch wordt in deze periode bedreiging en intimidatie in de meeste gevallen gezien als iets dat simpelweg erbij hoort.¹⁴

2002

De terroristische aanslagen van 11 september 2001 in de Verenigde Staten geven een eerste impuls om de aanpak van persoonsbeveiliging en objectbewaking te herzien. Maar het is de moord op Pim Fortuyn in 2002 die tot een stroomversnelling leidt. Niet alleen de moord zelf is aanleiding om het stelsel van maatregelen te heroverwegen, ook de plotselinge toename van (doods)bedreigingen aan het adres van landelijke politici, burgemeesters, raadsleden en wethouders in de nasleep van de aanslag draagt daar aan bij.¹⁵ De commissie Van den Haak, ingesteld om de moord op Fortuyn te onderzoeken met specifieke aandacht voor de beveiliging

⁹ Van den Haak et al., *De veiligheid en de beveiliging van Pim Fortuyn*, 37, 46, 66–67, 73, 98–99, 108–9; Akerboom, 'Tien jaar Nederlands contraterrorismebeleid,' 395.

¹⁰ Prins, 'De bestuurlijke aanpak van georganiseerde criminaliteit in Nederland,' 152–55.

¹¹ Bovenkerk, 'Bedreigingen in Nederland,' 51, 90–91; Van der Torre, Gieling en Bruinsma, 'Bedreigen en intimideren van OM- en politiemedewerkers,' 20–21.

¹² Van der Torre, Gieling en Bruinsma, 'Bedreigen en intimideren van OM- en politiemedewerkers,' 20.

¹³ Van Soest, Van der Aa en Van der Wal, 'Bedreigingen en fysieke aanvallen.'

¹⁴ Bovenkerk, 'Bedreigingen in Nederland,' 37–38, 186–87.

¹⁵ De Wijk, 'Het stelsel na Pim Fortuyn,' 20; Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2002,' 73; Bovenkerk, 'Bedreigingen in Nederland,' 51; Van den Haak et al., *De veiligheid en de beveiliging van Pim Fortuyn*, 70.

van de politicus, doet eind 2002 verschillende aanbevelingen die zullen bijdragen aan een grondig herzien stelsel van afspraken en maatregelen rondom het beveiligen en bewaken van personen, objecten en diensten.¹⁶

In het stelsel zoals destijds aangepast blijft eigen verantwoordelijkheid voor bewaking en beveiliging een belangrijk uitgangspunt, maar de nadruk op specifieke (diplomatieke) personen en objecten verdwijnt. Ook personen die de democratische rechtsstaat personifiëren, zoals ministers, partijvoorzitters en magistraten, vallen nu onder het stelsel bewaken en beveiligen. Sommigen van hen, zoals de minister-president, worden standaard van beveiliging voorzien, anderen als dreigingsinschattingen daar reden toe geven. Naast een gelimiteerd aantal personen, objecten en diensten dat onder verantwoordelijkheid van de rijksoverheid valt (het zogenaamde centrale of rijksdomein), ligt in het nu decentraal georganiseerde stelsel de verantwoordelijkheid voor bewaking en beveiliging van Nederlanders en buitenlanders op Nederlands grondgebied in eerste instantie bij regionale politiekorpsen (nu eenheden). Als lokale autoriteiten hier onvoldoende middelen voor hebben kan de rijksoverheid om assistentie worden gevraagd. Een laatste verandering relevant voor dit rapport, is dat het aangepaste stelsel expliciet gebruik gaat maken van risicoanalyses om naast concrete dreigingen ook voorstelbare dreigingen in kaart te brengen.¹⁷

2003

De moord op Fortuyn blijkt een keerpunt in zowel de aanpak als ontwikkeling van bedreiging en intimidatie in Nederland. In 2003 treedt het aangepaste stelsel in werking tegen een achtergrond van toenemende vraag om persoon- en objectbewaking. Al snel wordt besloten tot een forse uitbreiding van het personeelsbestand van de Dienst Koninklijke en Diplomatieke Beveiliging (DKDB) en diens moederorganisatie het Korps Landelijke Politiediensten (KLPD).¹⁸

2004 & 2005

In maart 2004 plegen jihadistische terroristen aanslagen op vier treinen in Madrid. Er vallen bijna 200 doden en meer dan 1800 gewonden.¹⁹ In november 2004 wordt in Amsterdam publicist en filmmaker Theo van Gogh vermoord door een jihadistische aanslagpleger. Politici Ayaan Hirsi Ali en Geert Wilders worden ernstig bedreigd. Op 7 juli 2005 vinden vier explosies plaats in het Londense openbaar vervoer. Weer zijn jihadistische terroristen verantwoordelijk. Er sterven 52 slachtoffers en meer dan 700 mensen raken gewond.²⁰ In Nederland volgt in oktober met de arrestatie van Samir A. de ontknoping van de ‘Piranha’ zaak en het definitieve einde van de Hofstadgroep. De gebeurtenissen onderstrepen dat het jihadisme niet langer alleen een externe dreiging is, vormgegeven door groeperingen als al-Qaeda die opereren van buiten de Europese Unie, maar ook een *homegrown* dimensie kent. De dreiging wordt er steeds meer een van geradicaliseerde jonge moslims die geboren en getogen zijn in de landen waar ze zich later tegen keren.²¹

Van een terroristische dreiging vanuit links- of rechts-extremistische groeperingen is in deze periode in Nederland geen sprake. Wel zorgen in 2005 met name antifascisten en tegenstanders

¹⁶ De Wijk, ‘Het stelsel na Pim Fortuyn,’ 8–9.

¹⁷ Ibid., 8–15, 19; Openbaar Ministerie, Politie Nederland en NCTV, ‘Factsheet: stelsel bewaken en beveiligen.’

¹⁸ De Wijk, ‘Het stelsel na Pim Fortuyn,’ 15.

¹⁹ Nesser, *Islamist terrorism*, 138.

²⁰ Home Office, ‘Official account of the bombings,’ 2.

²¹ Schuurman, *Becoming a European homegrown jihadist*, 15, 68–74.

van het vreemdelingenbeleid voor ordeverstoringen en komt het vooral bij demonstraties tegen neonazistische opposanten geregeld tot gewelddadigheden.²²

In 2005 publiceert criminoloog Frank Bovenkerk met zijn collega's een studie naar bedreigingen van gezagsdragers in Nederland. Eén van de conclusies luidt dat met name officieren van justitie, rechters, advocaten en journalisten een toename in het aantal bedreigingen merken. Verruwing van omgangsvormen, verminderd respect voor het gezag, en de laagdrempeligheid van het internet als medium om bedreigingen te uiten, spelen daarbij belangrijke rollen. Als drijfveren tekenen de onderzoekers expressieve en instrumentele motieven op. Het gaat lang niet alleen om burgers die 'slechts' uiting geven aan hoogoplopende emoties of grieven, maar ook om bewuste pogingen tot beïnvloeding. Daarnaast wordt gewezen op de toegenomen dreiging vanuit het terrorisme en de georganiseerde misdaad.²³ Veel van deze ontwikkelingen zullen ook de hierop volgende jaren beeldbepalend blijven.

2006

Na de arrestatie van Samir A. en zijn medeverdachten eind 2005 lijkt er in Nederland geen volgende generatie *homegrown* jihadisten op te staan. De AIVD noteert in ieder geval een tijdelijke afwezigheid van leidersfiguren en verzwakking van de netwerken.²⁴ De dreiging van het (jihadistisch) terrorisme lijkt dus te fluctueren.²⁵ De terroristische dreiging blijft in deze periode ideologisch gezien tot het jihadisme beperkt. Wel ziet de AIVD een toenemende bereidheid van links-extremisten om hun rechts-extremistische tegenstanders bij confrontaties fysiek te lijf te gaan. Die laatste beweging wordt daarentegen met name door versnippering getypeerd.²⁶

2007-2009

In zijn proefschrift wijst Jelle van Buuren op een toename van complotdenken en 'systeemhaat' die in deze jaren in Nederland plaatsvindt. Het internet speelt hierbij een belangrijke rol als medium dat toegang verleent tot de digitale gemeenschappen waarin deze ideeën gedeeld en aangewakkerd worden. Daarnaast kan het ook als vliegwiel dienen in het versterken van ressentiment: burgers hebben door het internet weliswaar meer mogelijkheden om hun stem te laten horen, maar dat betekent niet dat er ook naar ze geluisterd wordt, wat tot toenemende frustratie en de drang om nog harder te schreeuwen kan leiden.²⁷

Een tweede relevante ontwikkeling in deze periode is de hernieuwde aandacht voor de bestuurlijke aanpak van georganiseerde misdaad. De wet BIBOB geeft sinds 2003 lokale overheden verruimde mogelijkheden om de georganiseerde criminaliteit aan te pakken, onder andere door het weigeren of terugtrekken van subsidies of vergunningen bij een aantoonbaar vermoeden dat de ontvangende partij zich aan crimineel handelen schuldig maakt. In 2007 gaan projecten van start in Rotterdam en Amsterdam die als voorbeeld zullen dienen voor hoe lokaal bestuur kan optreden tegen georganiseerde criminaliteit, in dit geval rondom de vastgoedwereld en de prostitutie. Vergelijkbaar met de jaren '90 leidt de toegenomen druk op het criminele circuit echter ook tot meer (ernstige) bedreigingen richting lokale bestuurders.²⁸

²² Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2004,' 43-46; Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2005,' 47-51.

²³ Bovenkerk, 'Bedreigingen in Nederland,' 186-96.

²⁴ Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2006,' 19-20.

²⁵ Dit werd in de expertsessie beaamd: Medewerker NCTV 1, Bijdrage aan de expertsessie.

²⁶ Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2006,' 53-58.

²⁷ Van Buuren, 'Doelwit Den Haag?,' 236-38.

²⁸ Prins, 'De bestuurlijke aanpak van georganiseerde criminaliteit in Nederland,' 154-55, 162-63.

Er lijkt in deze periode sprake te zijn van een bredere trend qua bedreigingen. In 2009 rapporteert de AIVD in zijn jaarverslag dat het al enkele jaren het aantal bedreigingen richting politici, opiniemakers and overheidsdoelwitten ziet toenemen. De laagdrempeligheid van het internet als medium om dreigingen te uiten wordt onderstreept. Ook de zogenaamde ‘solistische dreiger’ die in ieder geval deels door persoonlijkheidsstoornissen wordt gedreven, wordt expliciet benoemd.²⁹

Wat extremisme en terrorisme betreft lijkt de periode 2007-2009 gekenmerkt door voortdurende verdeeldheid, inactiviteit en algehele verzwakking van de jihadistische beweging in Nederland. Binnen het links-extremisme ziet de AIVD in deze jaren een voortdurende bereidheid om ideologische tegenstanders met fysiek geweld te lijf te gaan en blijft ook het asielbeleid van de overheid een bron van verzet dat soms gepaard gaat met vernieling en intimidatie. Het rechts-extremistische milieu blijft door versnippering gekenmerkt. Hoewel er in 2009 volgens de dienst een opleving plaatsvindt van links- en dierenrechtenextremisme, lijken deze bewegingen met name te zorgen voor openbare-orde problematiek zoals bij demonstraties waar bewust de confrontatie met ideologische tegenstanders wordt opgezocht.³⁰

Op 30 april 2009 probeer Karst T. met zijn auto op leden van de Koninklijk Huis in te rijden. Hij slaagt daar niet in, maar zijn poging kost aan 7 omstanders en hemzelf het leven. Er vallen 18 gewonden.³¹ Onderzoek toont aan dat het stelsel op basis van de beschikbare dreigings- en risico-informatie goed heeft gefunctioneerd. Dat er desondanks een aanslag kon plaatsvinden onderstreept enerzijds de onmogelijkheid om totale veiligheid te garanderen in een open samenleving en anderzijds de voortdurende noodzaak om ook met onwaarschijnlijke risico's, zoals in dit geval een aanslag met een auto, rekening te houden.³²

2010

In 2010 lijkt bedreiging van (lokale) politici en bestuurders verder toe te nemen.³³ Volgens de AIVD gaat het bij personen in het rijksdomein vaak om zogenaamde ‘straattaaldreigers’; boze of gefrustreerde jongeren die de laagdrempeligheid van het internet gebruiken om hun beklag te doen. Van een concreet gevaar is bij dit type dreigers zelden sprake.³⁴ Enquête-onderzoek onder lokale bestuurders toont echter aan dat bedreigingen in het decentrale domein veelal een reactie zijn op specifieke beslissingen en dat met name burgemeesters te maken krijgen met dreigers die verstoring van hun criminele activiteiten willen voorkomen.³⁵ Ook de solistische dreiger blijft een fenomeen dat volgens de AIVD steeds meer aandacht vergt.³⁶ De zogeheten ‘verwarde-gefrustreerde’ dreiger wordt ook in een NCTb³⁷ onderzoek naar politici die tussen 2005 en 2008 zijn bedreigd als een hoog risico gezien, verantwoordelijk voor 43% van de onderzochte zaken.³⁸

²⁹ Algemene Inlichtingen- en Veiligheidsdienst, ‘Jaarverslag AIVD 2009,’ 41.

³⁰ Algemene Inlichtingen- en Veiligheidsdienst, ‘Jaarverslag AIVD 2007,’ 30, 49-53; Algemene Inlichtingen- en Veiligheidsdienst, ‘Jaarverslag AIVD 2008,’ 17, 35-37; Algemene Inlichtingen- en Veiligheidsdienst, ‘Jaarverslag AIVD 2009,’ 13, 24-25.

³¹ Inspectie Openbare Orde en Veiligheid, ‘Koninginnedag 2009 Apeldoorn,’ 13.

³² Nationaal Coördinator Terrorismedebestrijding en Veiligheid, ‘Bewaken en beveiligen Koninginnedag 2009,’ 5-6, 8.

³³ De Wijk, ‘Het stelsel na Pim Fortuyn,’ 32.

³⁴ Algemene Inlichtingen- en Veiligheidsdienst, ‘Jaarverslag AIVD 2010,’ 23.

³⁵ Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, ‘Bedreigd bestuur 2010,’ 18.

³⁶ Algemene Inlichtingen- en Veiligheidsdienst, ‘Jaarverslag AIVD 2010,’ 23.

³⁷ Voorloper van de NCTV.

³⁸ Borgesius et al., ‘Individuele bedreigers van publieke personen,’ 11, 28.

De dreiging van het *homegrown* jihadistisch terrorisme blijft ook dit jaar laag. Het rechts-extremistische milieu is nog altijd versnipperd en gekenmerkt door onderlinge onenigheid. Dierenrechtenactivisten zijn na een opleving in 2009 dit jaar weer minder actief. Antifascisten blijven wel de confrontatie met hun ideologische tegenstanders opzoeken.³⁹

2011

In juli pleegt de Noor Anders Breivik aanslagen op Oslo en Utøya die aan 77 mensen het leven kosten. De AIVD onderstreept met verwijzing naar Breivik opnieuw het probleem van de solistische dreigers. De gebeurtenissen maken ook duidelijk dat het terroristische gevaar niet alleen uit jihadistische hoek komt; Breivik legitimeert zijn moorden op basis van een rechts-extremistisch wereldbeeld.⁴⁰

In Nederland ziet het Openbaar Ministerie bedreigingen van politici toenemen, met een belangrijke rol voor sociale media.⁴¹ De risico's die lokale bestuurders kunnen lopen in de aanpak van georganiseerde criminaliteit wordt geïllustreerd door de casus van burgemeester Fons Jacobs van Helmond, die tussen eind 2010 en medio 2011 met zijn gezin moet onderduiken na bedreigingen.⁴² Tegelijkertijd blijven de 'straattaal dreigers' met een relatief laag concreet risico op geweld nog altijd verantwoordelijk voor een groot deel van de geuite bedreigingen.⁴³ Mogelijkerwijs is een deel van de (gepercipieerde) toename te wijten aan het 'copycat effect'; onderzoek uit 2011 suggereert namelijk dat met name bedreigingen tot nabootsing kunnen leiden.⁴⁴

De relatieve inactiviteit binnen de Nederlandse jihadistische beweging lijkt doorbroken. De AIVD noteert een toenemend aantal reisbewegingen naar conflictgebieden zoals Afghanistan. In 2011 breekt ook de Syrische burgeroorlog uit die zich de komende jaren zal ontwikkelen tot brandpunt van de internationale jihad. Wat andere vormen van extremisme betreft blijft de dreiging vanuit rechts-extremistische hoek gering maar is er onder links-extremistische groeperingen met name qua het verzet tegen het Nederlandse asielbeleid sprake van een intensivering, wat soms tot intimidaties en vernielingen leidt. De activiteiten van antifascisten die bewust uit zijn op confrontaties met rechts-extremisten, daarentegen, lijken te zijn afgenomen.⁴⁵ Ook binnen de links-extremistische beweging lijkt er sprake te zijn van een fluctuerend patroon qua mate van activiteit.

2012

Vanuit Nederland vertrekt een toenemend aantal jihadisten om zich aan te sluiten bij de strijd tegen het regime van Assad in Syrië. Zij vormen in eerste instantie een bedreiging voor de bevolking ter plaatse. Maar hun gevechtservaring en training verhoogt volgens de AIVD ook hun capaciteit om na terugkeer naar Nederland terroristische aanslagen op touw te zetten.⁴⁶

In Nederland zelf begint eind 2012 excessief vuurwapengebruik door criminele organisaties nadrukkelijker in beeld te komen na een dubbele moord in Amsterdam. De volgende jaren lijkt

³⁹ Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2010,' 9, 14-16; Algemene Inlichtingen- en Veiligheidsdienst, 'Afkalvend front, blijvend beladen'.

⁴⁰ Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2011,' 37-38.

⁴¹ 'Politici steeds vaker ernstig bedreigd.'

⁴² Snijders, "'Het zit na jaren nog tussen de oren.'"

⁴³ Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2011,' 37-38.

⁴⁴ Bos, van Es en Vasterman, 'Copycat,' 13-16.

⁴⁵ Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2011,' 11, 16-18, 27.

⁴⁶ Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2012,' 12.

niet alleen het aantal liquidaties toe te nemen, ook de steeds jongere leeftijd van daders en slachtoffers, het gebruik van zwaardere wapens en de verminderde zorgen om het treffen van omstanders vallen op.⁴⁷ Een toename in dodelijk geweld tussen criminelen valt ook op als uitzondering op algemene cijfers over moord in Nederland, die sinds de jaren '90 een dalende lijn laten zien.⁴⁸ Tot slot: wat bedreigingen in algemene zin betreft wijst de AIVD er ook dit jaar op dat de meeste dreigers geen concreet risico op geweld vormen.⁴⁹

2013 & 2014

De groeiende groep Syriëgangsters blijft beeldbepalend voor de terroristische dreiging tegen Nederland. Gevechtservaring en harding door strijddeelnemers worden onder (mogelijke) terugkeerders nog steeds als risico verhogend gezien.⁵⁰ De aantrekkingskracht van Syrië op de jihadistische beweging neemt in 2014 nog verder toe als Islamitische Staat (IS) veroverde delen van Syrië en Irak tot 'kalifaat' uitroept.⁵¹ Ook de dreiging van aanslagen in Europa door individuen en groepen gelieerd aan (of geïnspireerd door) IS of al-Qaeda neemt in deze periode toe. Dit blijkt onder andere uit de aanslag op het Joods Museum in Brussel op 24 mei 2014. De dreiging vanuit de jihadistische beweging wordt dan ook specifiek door de AIVD benoemd in relatie tot het stelsel.⁵²

Binnen de links-extremistische beweging in Nederland blijft verzet tegen het asiel- en vreemdelingenbeleid een zwaartepunt maar lijken gematigde actievoerders de extremistische elementen in toom te houden. Ook onder groeperingen die zich inzetten voor dierenwelzijn lijkt de toon milder. De rechts-extremistische beweging wordt door de AIVD nog altijd als een marginaal fenomeen getypeerd.⁵³ De dreiging van terroristische aanslagen en ander serieus politiek gemotiveerd geweld lijkt nog altijd vooral van het jihadisme uit te gaan.

Onderzoek naar bedreigingen tegen medewerkers van het Openbaar Ministerie toont aan dat circa 29% van de dreigers met mentale gezondheidsproblematiek lijkt te kampen. Binnen de politie wordt dat percentage op 41% geschat.⁵⁴ Gerelateerd aan dit onderwerp informeert de regering in 2013 de Kamer dat de term 'potentieel gewelddadige eenlingen' (PGE) gebruikt wordt als overkoepelende term voor eenlingen waar een potentiële dreiging vanuit gaat. De term 'solistische dreigers' wordt gereserveerd voor individuen die zich specifiek richten tegen personen in het rijksofbeeld.⁵⁵

2015

In januari lukt het Tarik Z. door te dreigen met een namaak-vuurwapen om een NOS-studio in Hilversum binnen te dringen, waar hij vervolgens wordt overmeesterd. Z. wordt gediagnosticeerd met bovengemiddelde narcistische trekken en een opmerkelijke mate van achterdochtigheid.⁵⁶ Het incident is extra verontrustend doordat het plaatsvindt tegen een achtergrond van toenemend jihadistisch geweld. In januari 2015 wordt Parijs opgeschrikt door een dodelijke aanslag tegen het kantoor van het satirische tijdschrift *Charlie Hebdo*.⁵⁷ In

⁴⁷ Van Gestel en Verhoeven, 'Liquidaties nieuwe stijl,' 9.

⁴⁸ Aarten en Liem, 'Unravelling the homicide drop'.

⁴⁹ Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2012,' 50.

⁵⁰ Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2013,' 9–10.

⁵¹ Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2014,' 8–9.

⁵² Ibid, 34.

⁵³ Ibid, 25-26.

⁵⁴ Van der Torre, Gieling en Bruinsma, 'Bedreigen en intimideren van OM- en politiemedewerkers,' 48, 52.

⁵⁵ Opstelten, 'Kamerstuk 29754, nr 233.'

⁵⁶ Rechtbank Midden-Nederland, NL:RBMNE:2015:4919.

⁵⁷ Bilefsky en De la Baume, 'Terrorists strike Charlie Hebdo.'

februari vindt een aanslag plaats tegen de Zweedse cartoonist Lars Vilks, die op dat moment in Kopenhagen is. Vilks ontkomt, maar er vallen twee dodelijke slachtoffers.⁵⁸ De dodelijkste terroristische aanslag in Europa vindt echter in november plaats, als aan IS gelieerde terroristen 130 mensen vermoorden in Parijs.⁵⁹ Niet alleen politici en bestuurders blijken kwetsbare doelwitten voor dreigers en terroristen, maar ook journalisten en burgers.

In Nederland zelf komt naast de dreiging van het jihadistisch terrorisme ook beïnvloeding van het lokale bestuur door criminelen wederom onder de aandacht, met name in relatie tot drugscriminaliteit in Noord-Brabant.⁶⁰ Ook de vluchtelingencrisis die dit jaar de Europese Unie treft leidt tot een toegenomen aantal bedreigingen richting burgemeesters.⁶¹ Zowel links- als rechts-extremistische groeperingen ondernemen activiteiten rondom het thema, wat soms voor geweld bij demonstraties zorgt.⁶² Tot slot wordt in december 2015 met de moord op een Nederlander van Iraanse komaf het risico dat van statelijke actoren uit kan gaan onderstreept. Het gaat waarschijnlijk om een liquidatie uitgevoerd met betrokkenheid van de Iraanse overheid waarbij vergelding voor een bomaanslag in de jaren 1980 het motief lijkt.⁶³

2016

Dodelijke aanslagen in onder andere Brussel in maart, Nice in juli en Berlijn in december benadrukken de voortdurende dreiging van het jihadistisch terrorisme. Het gebruik van vrachtwagens als wapens in de laatste twee gevallen toont bovendien het aanpassingsvermogen van terroristen. Vanaf circa 2014 beginnen jihadistische groeperingen hun volgers op te roepen om aanslagen te plegen met wat ze maar voorhanden hebben, zoals messen en voertuigen. Dit maakt terroristisch geweld laagdrempelig en door de minimale vereiste voorbereiding worden aanslagplannen buitengewoon moeilijk voortijdig op te sporen.⁶⁴

De aanslagen benadrukken ook de transnationale aard van de terroristische dreiging en de noodzaak tot internationale samenwerking op het gebied van contraterrorisme. De verantwoordelijken voor de bomaanslagen in Brussel waren onderdeel van de 'Bataclan' cel die in november 2015 in Parijs toesloeg.⁶⁵ De dader van de aanslag in Berlijn wist direct na zijn daad te ontkomen en een omzweving door meerder EU-lidstaten te maken, waaronder Nederland, voordat hij in Italië door de politie werd doodgeschoten.⁶⁶

De dodelijke aanslag op Brits parlementslid Jo Cox door een rechtsextremist in juni laat opnieuw zien dat de terroristische dreiging breder is dan het jihadisme alleen. De moord onderstreept bovendien de voortdurende dreiging van eenlingen.⁶⁷

2017

Zogenaamde 'ondermijning' van het (lokale) bestuur treedt meer en meer op de voorgrond als problematische ontwikkeling in Nederland. Het gaat hier om criminele activiteiten met dusdanige sociale en economische invloed dat het functioneren van de rechtsstaat wordt

⁵⁸ Chrisafis, 'Copenhagen shooting suspect.'

⁵⁹ Rubin, 'Paris: one year on.'

⁶⁰ Winter et al., 'Criminele beïnvloeding,' 1.

⁶¹ Klein Kranenburg et al., 'Bedreigingen en intimidaties van burgemeesters,' 7; Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2015,' 32.

⁶² Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2015,' 27-28.

⁶³ AIVD, MIVD en NCTV, 'Dreigingsbeeld statelijke actoren,' 21-22; Vugts, 'In Almere geliquideerde "Ali".'

⁶⁴ Veilleux-Lepage, 'How and why vehicle ramming.'

⁶⁵ Masschelin, 'Terroristen in Brussel en Parijs in zelfde netwerk.'

⁶⁶ 'Anis Amri verbleef enkele uren in Amsterdam.'

⁶⁷ Aspden, 'Making of a bedsit Nazi.'

bedreigd.⁶⁸ Hoewel critici het gebrek aan een heldere definitie en een soms wel zeer breed toepassingskader noemen, lijkt het met name ten aanzien van de georganiseerde drugscriminaliteit een belangrijke ontwikkeling te duiden. Door de groeiende schaduw economie rondom de productie en verkoop van drugs, kunnen criminelen zich in toenemende mate ook in de ‘bovenwereld’ inkopen, bijvoorbeeld op de vastgoedmarkt. Daarnaast wordt gewaarschuwd dat de grote hoeveelheden crimineel verkregen geld corrumperend kunnen werken; voor jongeren die het als aantrekkelijke levensstijl kunnen zien, maar ook voor ambtenaren en lokale bestuurders.⁶⁹

Vooralsnog stelt in 2017 verschenen onderzoek vast dat bedreiging van lokale bestuurders weliswaar veel voorkomt, en ook in het gehele land, maar dat er geen sprake is van structurele aantasting van democratische instituties. Dat neemt niet weg dat er lokaal problemen zijn met bedreiging, omkoping of (pogingen tot) infiltratie van bestuursorganen.⁷⁰ De AIVD stelt ook dit jaar dat er sprake is van aanhoudende bedreigingen richting politici, maar dat daadwerkelijk fysiek geweld zeldzaam blijft.⁷¹

Twee andere binnenlandse ontwikkelingen relevant voor het stelsel vallen op. Ten eerste is dat een in 2017 verschenen rapport in opdracht van de Nederlandse Vereniging van Journalisten. De auteurs betogen dat circa 43% van de beroepsgroep jaarlijks met bedreigingen kampt. Het rapport geeft aan dat de ernst van de bedreigingen is toegenomen.⁷² Ten tweede wordt er in Den Haag nog een Nederlander met Iraanse wortels gedood, wederom waarschijnlijk een liquidatie in opdracht van het Iraanse regime.⁷³

Internationaal valt de opkomst van de zogenaamde *alt-right* beweging in de Verenigde Staten op. Het potentieel voor geweld komt tijdens de ‘*Unite the Right*’ rally in Charlottesville duidelijk naar voren als een rechts-extremist met zijn auto op tegendemonstranten inrijdt waarna één van hen overlijdt.⁷⁴ Het incident suggereert bovendien het imitatief vermogen van extremistische bewegingen; aanslagen met voertuigen lijken door Palestijnse strijders te zijn gepopulariseerd, vervolgens met name door jihadisten te zijn overgenomen en mogelijk ook steeds meer in zwang te raken bij rechts-extremisten.⁷⁵

In Nederland blijft het jihadisme de voornaamste terroristische dreiging. Wel lijkt er op basis van het AIVD-jaarverslag sprake te zijn van nieuwe rechts-extremistische groeperingen die zich niet alleen tegen immigratie en buitenlanders keren maar ook de overheid steeds vijandiger tegemoet treden. Ook wordt melding gemaakt van steeds grimmigere confrontaties tussen rechts- en links-extremisten, bijvoorbeeld tijdens demonstraties rondom het immigratiebeleid of het Sinterklaasfeest.⁷⁶

2018

In 2018 worden in het ‘Marengo’ proces verschillende leden van de criminele organisatie bekend als de Moco-maffia vervolgd. Eind maart wordt de broer van kroongetuige Nabil B.

⁶⁸ Tops en Schilders, ‘Meervoudige aanpak van ondermijning,’ 12.

⁶⁹ Boutellier et al., ‘Een einde aan ondermijning,’ 4, 7, 11–12; Kortleven, ‘Een boekje open,’ 76–77.

⁷⁰ Winter et al., ‘Criminele beïnvloeding,’ 3, 7–8.

⁷¹ Algemene Inlichtingen- en Veiligheidsdienst, ‘Jaarverslag AIVD 2017,’ 17.

⁷² Odekerken en Brenninkmeijer, ‘Een dreigend klimaat,’ 3.

⁷³ AIVD, MIVD en NCTV, ‘Dreigingsbeeld statelijke actoren,’ 21–22; ‘Blok: Iran zat achter moorden in Nederland.’

⁷⁴ Zraick en Jacobs, ‘Charlottesville attacker pleads guilty.’

⁷⁵ Veilleux-Lepage, ‘The radical right’s legitimisation of vehicle ramming,’ 305–6.

⁷⁶ Algemene Inlichtingen- en Veiligheidsdienst, ‘Jaarverslag AIVD 2017,’ 12-17.

doodgeschoten in een poging de procesgang te beïnvloeden.⁷⁷ Het is de eerste keer dat de kroongetuigenregeling direct tot een liquidatie heeft geleid, hoewel er in ieder geval twee eerdere voorbeelden zijn van personen die gedood werden omdat ze overwogen of op het punt stonden om kroongetuige te worden.⁷⁸

Enkele maanden later rijdt een bestelbusje opzettelijk op het gebouw van de *Telegraaf* in. De aanslag lijkt verband te houden met berichtgeving van die krant over het Marengo proces.⁷⁹ Niet veel eerder wordt het redactiegebouw van weekblad *Panorama* beschoten met een antitankwapen. De daders zijn verbonden aan de criminele motorclub Caloh Wagoh.⁸⁰ Beide incidenten en de moord op de broer van een kroongetuige benadrukken dat ernstige bedreigingen niet alleen aan politici en bestuurders voorbehouden zijn. Ook voeden ze het idee dat de drempel tot het uitvoeren van een liquidatie steeds lager lijkt te worden en dat er vanuit de georganiseerde misdaad steeds grover geweld wordt ingezet tegen een breder scala aan tegenstanders. Hoewel het moeilijk is om precies te bepalen of het aantal dreigementen vanuit de georganiseerde misdaad gestegen is, lijkt in ieder geval de ernst ervan te zijn toegenomen.⁸¹

Een rapport van de Nederlandse Politiebond dat in februari 2018 verschijnt stelt dat ondermijning door drugscriminelen dusdanig is dat Nederland een ‘narco-staat’ genoemd kan worden.⁸² Opvallend is ook dat er vanaf 2018 een sterke toename lijkt plaats te vinden in het gebruik van handgranaten, met name tegen gebouwen. Het lijkt voornamelijk om intimidatie tussen criminelen onderling te gaan om zo een groter deel van de drugsomzet in handen te krijgen.⁸³ De toenemende geweldsbereidheid vanuit de georganiseerde misdaad komt in deze periode dus op verschillende manieren naar voren.

Op 5 mei steekt Malek F. drie mensen neer in Den Haag. Hoewel zijn gedrag in eerste instantie wijst op een jihadistische overtuiging, blijkt hij te lijden aan een psychotische stoornis en wordt hij in 2019 bij zijn berechting volledig ontoerekeningsvatbaar verklaard.⁸⁴ In augustus hoort de Afghaanse vluchteling Jawed S. dat Geert Wilders een cartoonwedstrijd heeft uitgeschreven over de profeet Mohammed. S. ontsteekt in woede en reist vanuit tijdelijk onderkomen in Duitsland af naar Nederland, waar hij op Amsterdam C.S. twee Amerikaanse toeristen neersteekt. S. werkt niet mee aan persoonlijkheidsonderzoek, waardoor niet kan worden vastgesteld of hij net als F. aan een stoornis lijdt.⁸⁵

De dreiging van het jihadistisch terrorisme blijft in Nederland en buurlanden de boventoon voeren. Opmerkelijk is echter dat de AIVD in 2018 ook specifiek op ontwikkelingen binnen de rechts-extremistische beweging ingaat. Er lijkt sprake te zijn van een opleving die in 2014 à 2015 in gang is gezet. Qua gedachtegoed heeft het klassieke neonazisme terrein verloren en is er meer nadruk op anti-islam en *alt-right* stromingen gekomen. Hoewel de geweldsdreiging vooralsnog als beperkt wordt gezien, wijst de dienst op het agressieve (online) taalgebruik en de kans dat met name de meer ‘intellectueel’ verpakte racistische ideeën van de *alt-right* beweging onder een bredere groep burgers gehoor vinden.⁸⁶

⁷⁷ Tieleman, ‘Rechtbank legt 20 jaar cel op.’

⁷⁸ Crijns, Dubelaar en Pitcher, ‘Overgeleverd aan de wolven?’, 1564–65.

⁷⁹ ‘Aanslag op het Telegraaf-gebouw.’

⁸⁰ Tieleman, ‘OM eist tot 7 jaar celstraf voor aanslag Panorama.’

⁸¹ Van Ham en Van Wijk, ‘Bescherming van personen,’ 6–8; Fijnaut, ‘De moord op advocaat D. Wiersum,’ 14.

⁸² Nederlandse Politiebond, ‘Noodkreet recherche’, 7.

⁸³ Liem en Krüsselmann, ‘Explosief geweld’; Van den Heuvel en Van Wely, ‘Gouden eeuw’.

⁸⁴ Rechtbank Den Haag, NL:RBDHA:2019:7308.

⁸⁵ Koops, ‘Aanslagpleger CS Jawed S. veroordeeld tot bijna 27 jaar cel.’

⁸⁶ Algemene Inlichtingen- en Veiligheidsdienst, ‘Rechts-extremisme in Nederland,’ 21.

In oktober wordt de Saoedische journalist Jamal Khashoggi vermoord in het Saoedische consulaat in Istanbul, hoogstwaarschijnlijk in opdracht van de Saoedische kroonprins Mohammed bin Salman.⁸⁷ Hoewel er geen direct verband met Nederland bestaat, bevestigt de moord enerzijds de dreiging die van statelijke actoren uit kan gaan en anderzijds het buitengewone risico dat journalisten kunnen lopen.

De moord op de 16-jarige scholiere Hümeyra Ergincanli in december herinnert eraan dat ook burgers slachtoffer kunnen worden van zeer ernstige bedreigingen. De scholiere doet vanaf mei meerdere malen aangifte tegen haar ex-vriend Bekir E., onder andere voor mishandeling en stalking. Hoewel E. onder toezicht staat van Reclassering Nederland, een gevangenisstraf van 6 weken wordt opgelegd en een contactverbod heeft, weet hij toch toe te slaan. In zijn rapport verwijt de Inspectie dat betrokken partijen waaronder politie en OM te weinig oog hebben gehad voor de veiligheid van Hümeyra en dat ze tekort zijn geschoten in het beoordelen van de risico's die ze liep.⁸⁸

2019

Gökmen T. pleegt in maart een aanslag op een tram in Utrecht waarbij 4 doden en meerdere gewonden vallen. De aanslag lijkt gemotiveerd door een jihadistische overtuiging maar de rechtsgang maakt ook duidelijk dat T. een persoonlijkheidsstoornis heeft met narcistische en antisociale kenmerken.⁸⁹ Na de aanslagen in 2018 staat het gevaar van de – al dan niet verwarde – eenling weer volop in de aandacht.

De gebeurtenissen in Utrecht volgen enkele dagen op een rechts-extremistische aanslag in Nieuw-Zeeland die wereldwijd tot consternatie leidt. De Australische dader maakt 51 dodelijke slachtoffers en laat 40 personen (ernstig) gewond achter.⁹⁰ De aanslag vestigt aandacht op het internationale karakter van rechts-extremistische netwerken en ideeën, hun groeiende invloed en de mate waarin terroristen zoals Anders Breivik tot rolmodellen worden. Ook wordt de rol die het internet kan spelen als digitale kweekvijver én afzetmarkt voor extremisme onderstreept; de dader zond zijn aanslag live uit via het digitale medium en garandeerde zo volop aandacht voor zijn 'manifest' en zijn modus operandi.⁹¹ De invloed van de Christchurch-aanslag blijkt al in oktober als in het Duitse Halle een rechts-extremist een aanslag pleegt en die ook 'live' uitzendt met een camera op zijn helm.⁹² De moord op Duits politicus Walter Lübcke in juni lijkt de groeiende dreiging van rechts-extremistisch terrorisme nogmaals te onderstrepen.⁹³ De opleving van deze vorm van extremisme lijkt ook Nederland door te zetten, als is het hier voornamelijk een online fenomeen.⁹⁴

In Nederland zorgt in september de Marengo-zaak wederom voor een grote schok als Derk Wiersum, advocaat van kroongetuige Nabil B., hoogstwaarschijnlijk in naam van Moccro-maffia kopstuk Ridouan T. voor zijn woning in Amsterdam wordt vermoord.⁹⁵ Het is de eerste

⁸⁷ 'Kroonprins zat achter moord op journalist Khashoggi.'

⁸⁸ Inspectie Justitie en Veiligheid, 'Inspectieonderzoek naar de aanpak van de stalking door Bekir E.,' 4-8, 14-35.

⁸⁹ Rechtbank Midden-Nederland, NL:RBMNE:2020:1046.

⁹⁰ Royal Commission of Inquiry into the terrorist attacks on Christchurch mosques on 15 March 2019, 'Report of the Royal Commission of Inquiry: Volume 1,' 46.

⁹¹ Macklin, 'The Christchurch attacks.'

⁹² Rafael, 'Nach Dem Attentat.'

⁹³ Hagemann, 'Mordfall Lübcke.'

⁹⁴ Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2019,' 3, 17.

⁹⁵ Tieleman, 'Spoor liquidatie advocaat Derk Wiersum leidt naar Utrecht.'

keer in de Nederlandse geschiedenis dat een strafadvocaat is geliquideerd in het kader van zijn werk.⁹⁶ De moord leidt tot toegenomen onveiligheidsgevoelens onder advocaten. Sommigen noemen het hun 11 september en nemen uit angst bepaalde zaken niet meer aan.⁹⁷ Ook beveiligers werkzaam in het stelsel zien dit als een omslagpunt; criminelen lijken geen schroom meer te hebben in het gebruik van geweld tegen vertegenwoordigers van de rechtsstaat.⁹⁸ Als reactie op het toegenomen geweld vanuit de georganiseerde misdaad wordt het Multidisciplinair Interventie Team opgericht, een samenwerking tussen verschillende overheidsdiensten waaronder politie, justitie, Marechaussee en de Belastingdienst.⁹⁹

Vervolgonderzoek naar bedreigingen tegen journalisten toont aan dat 37% van de vrouwelijke journalisten jaarlijks met bedreigingen geconfronteerd wordt. De dreigementen hebben in een significant aantal gevallen ook consequenties voor de persvrijheid. Bijvoorbeeld doordat 18% van de respondenten niet meer aan sommige onderwerpen begint of 15% bewust bepaalde informatie weglaat.¹⁰⁰ Het thema bedreiging van journalisten komt ook naar voren in een rapportage waaruit blijkt dat regionale verslaggevers steeds vaker kampen met bedreigingen en intimidatie.¹⁰¹ Het beeld van een rechtsstaat onder druk wordt ook buiten de Nederlandse grenzen vaker gezien.¹⁰²

2020

Onderzoek toont aan dat lokale bestuurders de afgelopen jaren vaker worden bedreigd. Dit gebeurt met name op sociale media.¹⁰³ Ook medewerkers van het stelsel benadrukken dat er meer en zwaarder gedreigd wordt en dat criminelen sneller grof geweld inzetten. De politie heeft grote moeite om adequate bescherming te bieden aan slachtoffers van ernstige bedreigingen door een sterke toename van het aantal zaken. Er lijkt niet alleen meer (ernstig) gedreigd te worden, het toenemende gebruik van risico-inschattingen brengt ook meer potentiële gevaren in beeld waartegen opgetreden wordt.¹⁰⁴

Ook bedreigingen tegen journalisten zijn in 2020 weer onderwerp van debat. In oktober besluit de NOS om het logo van de omroep van voertuigen te verwijderen om de kans op bedreiging van werknemers te verminderen.¹⁰⁵ De door Amerikaans president Trump vaak gebruikte aantijging ‘fake news’ lijkt ook in Nederland gemeengoed te worden en de geloofwaardigheid van journalisten in ieder geval in sommige kringen te ondermijnen.¹⁰⁶

De aantasting van de geloofwaardigheid van instituties, experts, politici en bestuurders komt door het uitbreken van de coronacrisis in een stroomversnelling. De crisis blijkt ook in Nederland een rijke voedingsbodem voor samenzweringsdenken. Virologen, politici en ambtenaren die zich met de bestrijding van het virus bezighouden worden al snel doelwit van

⁹⁶ Vugts, ‘Een reconstructie van de aanslag op Derk Wiersum.’

⁹⁷ ‘Dossier Derk Wiersum’; Stoker, ‘Een jaar na de moord.’

⁹⁸ Vermaas, ‘Het werk van de BBC’ers van het OM.’

⁹⁹ Den Hartog, ‘Hoe moeten we het onkruid wieden?’

¹⁰⁰ Odekerken en Das, ‘Een onveilig klimaat,’ 1–3.

¹⁰¹ Oostveen, ‘Regionale verslaggevers worden vaak bedreigd.’

¹⁰² Lauriks en Korsten, ‘Strategisch Omgevingsbeeld 01,’ 16, 20; Korsten, Hendrix en Van der Sloot, ‘Strategisch omgevingsbeeld 2020,’ 16.

¹⁰³ Van Hoof et al., ‘Psychosociale effecten van bedreiging en beveiliging,’ 8–9.

¹⁰⁴ Andringa, ‘Veel meer dreigingen van criminelen’; Vermaas, ‘Het werk van de BBC’ers van het OM.’

¹⁰⁵ De Jager, ‘Geweld en middelvingers nopen NOS logo te verwijderen.’

¹⁰⁶ Thomas en Zonderop, ‘Journalistiek moet zelf vertrouwen herstellen.’

dreigementen.¹⁰⁷ De AIVD ziet anti-overheidsactivisten vaker een dreiging vormen.¹⁰⁸ Bovendien komt het strafrechtelijk apparaat onder druk door de coronacrisis.¹⁰⁹ Ook deelnemers aan de expertsessie benadrukken dat de coronacrisis en het online discours hieromtrent sommige mensen heeft gesterkt in de overtuiging dat ze in opstand moeten komen. Er lijkt een groter risico dat het online domein het offline handelen beïnvloedt.¹¹⁰

De problematiek rondom bedreigingen beperkt zich niet tot een kleine groep specifieke thema's. Toenemende aantallen demonstraties over uiteenlopende onderwerpen zoals het klimaat, de coronamaatregelen, zwarte piet of de *Black Lives Matter*-beweging duiden op een verdieping van maatschappelijke tegenstellingen. Ook op sociaaleconomisch gebied neemt de ongelijkheid toe en groeit de groep 'achterblijvers' die een dalend vertrouwen in de rechtsstaat heeft.¹¹¹ De internationale politiek lijkt instabieler te worden door een verschuiving naar een multipolaire wereldorde waarin onder andere China en Rusland steeds assertiever optreden.¹¹²

Binnen de EU blijkt de jihadistische dreiging beslist niet te zijn weggevallen met de teloorgang van het fysieke kalifaat van IS. In november 2020 wordt Wenen opgeschrikt door een aanslag van een jihadistische eenling.¹¹³ Niet veel eerder werden in Frankrijk verschillende aanslagen gepleegd waaronder op docent Samuel Paty die spotprenten over Mohammed had besproken in zijn les.¹¹⁴ In de nasleep van de moord op Paty moet ook een Rotterdamse leraar onderduiken na dreigementen. De ophef draait om een spotprent over de *Charlie Hebdo* aanslag in 2015 die de leraar al jaren in zijn lokaal had hangen.¹¹⁵ De casus illustreert hoe plotselinge ontwikkelingen in het buitenland invloed kunnen hebben op stelselrelevante dreigingen.

Internationaal gezien drukt ook het rechts-extremisme zijn stempel op 2020. Duitsland wordt in februari wederom opgeschrikt door een rechts-extremistische aanslag, ditmaal in Hanau.¹¹⁶ Een reeks incidenten in de Duitse, Britse en Amerikaanse krijgsmachten vormt aanleiding voor toenemende bezorgdheid over infiltratie door rechts-extremisten.¹¹⁷ In Nederland blijft het rechts-extremisme echter vooralsnog beperkt en is het veelal een online fenomeen.¹¹⁸ Wel lijkt met name de *alt-right* variant een breder publiek te bereiken door rechts-extremistische ideeën over bijvoorbeeld racisme en Joden op een 'intellectuele' manier te verpakken. Waar het rechts-extremisme in Nederland sterker voet aan de grond lijkt te krijgen en -gezien aanslagen in anderen landen- ook een potentie tot terroristische geweld in zich draagt, lijkt het links-extremistische milieu zich veelal op burgerlijke ongehoorzaamheid te richten en minder dan voorheen op gewelddadige confrontaties uit te zijn.¹¹⁹

Tot slot komen in 2020 statelijke actoren nadrukkelijker naar voren in het dreigingsbeeld van de AIVD, met name ten opzichte van diplomaten, diplomatieke objecten en internationale

¹⁰⁷ Du Pré, 'Oververhit coronadebat raakt ook het OMT.'

¹⁰⁸ Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2020,' 16.

¹⁰⁹ Korsten, Hendrix en Van der Sloot, 'Strategisch omgevingsbeeld 2020,' 8.

¹¹⁰ Medewerker Politie 1, Bijdrage aan de expertsessie.

¹¹¹ Lauriks en Korsten, 'Strategisch Omgevingsbeeld 01,' 12; Korsten, Hendrix en Van der Sloot, 'Strategisch omgevingsbeeld 2020,' 10; Analistennetwerk Nationale Veiligheid, 'Horizonscan 2020,' 25–26.

¹¹² Nationaal Coördinator Terrorismebestrijding en Veiligheid, 'Nationale veiligheid strategie 2019,' 19–20.

¹¹³ Bennhold, Eddy en Schuetze, 'Vienna reels.'

¹¹⁴ Renout, 'Fransen massaal de straat op uit woede om moord op leraar.'

¹¹⁵ Kouwenhoven, 'Docent duikt onder om cartoon in klas.'

¹¹⁶ Haschnik, 'Neue Details.'

¹¹⁷ Koehler, 'A threat from within?'

¹¹⁸ Analistennetwerk Nationale Veiligheid, 'Horizonscan 2020,' 21.

¹¹⁹ Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2020,' 4, 6.

organisaties zoals de Organisatie voor het Verbod op Chemische Wapens.¹²⁰ Een andere cruciale ontwikkeling op dit gebied is ongewenste buitenlandse inmenging in berichtgeving rondom politiek of maatschappelijk gevoelige thema's, zoals verkiezingen en het MH-17 tribunaal, met als doel het aanwakkeren van polarisering. Staten als Rusland doen dit bijvoorbeeld door desinformatiecampagnes via sociale media. Ook wordt het cyberdomein gebruikt voor (economische) spionage.¹²¹ De AIVD stelt in zijn jaarverslag dat deze digitale dreigingen ook onder het stelsel zouden moeten vallen.¹²²

2021

De groeiende invloed van desinformatiecampagnes door partijdige media en toenemende steun voor antidemocratische en rechtsextremistische sentimenten onder zowel delen van de Amerikaanse bevolking als het Republikeinse politieke establishment, komen in de presidentiele verkiezingen duidelijk naar voren. Opgezwepen door zittend president Trump omdat de verkiezingen 'gestolen' zouden zijn, die op zijn beurt daarin gesteund wordt door kanalen als *Fox News*, bestormt op 6 januari een menigte het Capitool.¹²³ In de maanden nadien blijkt dat grote delen van de Republikeinse partij onwillend zijn om de valse aantijgingen van verkiezingsfraude tegen te spreken, noch om voor Trumps afzetting te stemmen.¹²⁴ Antidemocratische sentimenten zijn niet alleen een externe bedreiging voor rechtsstaten, maar kunnen ook van binnenuit greep krijgen.

De ondermijning van objectieve journalistiek door politici vindt ook in Nederland zijn weerklank. In de aanloop naar de Tweede Kamerverkiezingen bestempelt bijvoorbeeld een lijsttrekker de NOS als *fake news*.¹²⁵ Ook de voortdurende coronacrisis ondergraaft het vertrouwen in instituties, bestuurders en politici. Naast ongenoegen over de genomen maatregelen is er een groeiende groep complotdenkers en vaccinweigeraars die zich afkeert van de overheid en van wetenschappelijke expertise. Desinformatie verspreidt via het internet speelt hierbij een belangrijke rol, zeker als min-of-meer bekende Nederlanders er een hand in hebben. De toegenomen invloed van complotdenken laat zich ook optekenen uit de groeiende aanhang voor de in de VS ontstane 'QAnon' beweging. Daarnaast zijn er ook in Nederland rechtsextremistische 'accelerationisten' actief die de crisis bewust aangrijpen om middels desinformatiecampagnes, bijvoorbeeld over vaccins, de val van het door hun gehate systeem te bespoedigen.¹²⁶

De dreiging van complotdenkers en corona-ontkenners blijft niet geheel virtueel. In maart wordt een coronateststraat in Bovenkarspel getroffen met een zelfgemaakt explosief. De schade is gering.¹²⁷ Een maand later wordt een man uit Den Helder aangehouden op verdenking van het voorbereiden van een aanslag op een vaccinatie locatie in zijn woonplaats.¹²⁸ Eind mei voorkomen de Oostenrijkse autoriteiten een aanslag van corona-ontkenners door beslag te leggen op wapens en munitie, waarmee de internationale dimensie van deze dreiging wordt aangetoond.¹²⁹ Tegenover deze zorgwekkende incidenten stellen deelnemers aan de

¹²⁰ Ibid, 16.

¹²¹ Analistennetwerk Nationale Veiligheid, 'Horizonscan 2020,' 21.

¹²² Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2020,' 16.

¹²³ Kuin, 'Opgestookt door leugens en oorlogsretoriek.'

¹²⁴ Den Hond, 'Republikeinen dulden geen enkele kritiek meer op Trump.'

¹²⁵ Nieber en Smouter, 'Ombudsman Smit (NPO).'

¹²⁶ Schoonhoven, 'Doorslaan in achterdocht; Nederland kent poldervariant van QAnon'; Van Buuren, 'De nieuwe complotecologie'; 'Nederlands trollenleger.'

¹²⁷ 'Explosief bij teststraat Bovenkarspel.'

¹²⁸ 'Plan aanslag op vaccinatie locatie.'

¹²⁹ Ouhajji en Boonman, 'Wapens gevonden bij Oostenrijkse coronategenstanders.'

expertsessie dat, afgezet tegen de toename van geuite dreigementen, het aantal gewelddadige incidenten in relatie tot de coronacrisis vooralsnog betrekkelijk laag is.¹³⁰

De zorgen om rechts-extremisme binnen het krijgsbedrijf laaien in mei op als een Belgisch militair een arsenaal wapens uit een kazerne steelt en vervolgens verdwijnt. De militair lijkt het op een Belgische viroloog gemunt te hebben, wat op een overlap tussen samenzweringsdenken rondom corona en rechts-extremisme duidt. De tienduizenden steunbetuigingen voor de militair van andere Belgen wijzen bovendien op een gedachtegoed dat niet langer als marginaal te bestempelen is.¹³¹ In Nederland is de krijgsmacht ook aantrekkelijk voor rechts-extremisten maar zijn er volgens de demissionair minister van defensie ‘geen aanwijzingen dat rechts-extremisme een gevaar vormt in de cultuur van defensie’.¹³² Hoewel voorbeelden van rechts-extremisme onder militairen wereldwijd vaker in het nieuws komen, is er nog onvoldoende data om te beoordelen of er sprake is van een trend.¹³³

De dreiging van statelijke actoren zoals China, Rusland en Iran blijft actueel, met name ten aanzien van het digitale domein.¹³⁴ Beïnvloedingsoperaties hebben als doel het aanwakkeren van polarisatie en het ondergraven van de cohesie in landen als Nederland maar ook binnen organisaties als de EU en de NAVO. Ook economische en militaire spionage en cyberaanvallen vallen te onderscheiden. Nieuwe technologieën worden volop ingezet en attributie, oftewel het achterhalen van de gebruiker, wordt steeds lastiger.¹³⁵ In zijn ‘Cybersecuritybeeld Nederland’, waarschuwt de NCTV dat niet alleen statelijke actoren Nederlandse belangen en nationale veiligheid kunnen schaden via het digitale domein maar dat ook enkele cybercriminele groepen hiertoe in staat zijn.¹³⁶

Onderzoek van *Freedom House* toont aan dat statelijke actoren ook vaker repressie gebruiken tegen leden van diaspora en vluchtelingengemeenschappen dan gedacht.¹³⁷ Illustratief hiervoor is de kaping van een passagiersvliegtuig door Wit-Rusland in mei 2021. Het toestel is onderweg van Athene naar Vilnius als het onder valse voorwendselen wordt gedwongen om te landen in Wit-Rusland zodat de lokale autoriteiten een blogger en journalist kunnen arresteren die zich al jaren kritisch uit over het regime.¹³⁸

Begin juli 2021 wordt misdaadverslaggever Peter R. de Vries in Amsterdam neergeschoten en belandt hij zwaargewond in het ziekenhuis, waar hij op 15 juli aan zijn verwondingen bezwijkt. Op het moment van schrijven is het nog onduidelijk wat de precieze toedracht van de moordaanslag is. Gezien zijn rol als vertrouwenspersoon van kroongetuige Nabil B. Lijkt het aannemelijk dat de aanslag verband houdt met het Marengo proces en de criminele organisatie rondom Ridouan T.¹³⁹ De aanslag bevestigt de grote druk die door de georganiseerde misdaad

¹³⁰ Medewerker NCTV 2, Bijdrage aan de expertsessie; Medewerker Ministerie van Binnenlandse Zaken, Bijdrage aan de expertsessie.

¹³¹ ‘Voortvluchtige Belgische militair kon door "grote fouten" aan wapens komen’; Medewerker ICCT 1, Bijdrage aan de expertsessie.

¹³² ‘Ook in Nederland vinden rechts-extremisten het leger aantrekkelijk.’

¹³³ Radicalisation Awareness Network, ‘Radicalised police, military and prison staff.’

¹³⁴ Korsten, Hendrix en Van der Sloot, ‘Strategisch omgevingsbeeld 2020,’ 20; Medewerker Ministerie van Binnenlandse Zaken, Bijdrage aan de expertsessie.

¹³⁵ Korsten, Hendrix en Van der Sloot, ‘Strategisch omgevingsbeeld 2020,’ 14, 20; AIVD, MIVD en NCTV, ‘Dreigingsbeeld statelijke actoren,’ 17–21.

¹³⁶ Nationaal Coördinator Terrorismebestrijding en Veiligheid, ‘Cybersecuritybeeld Nederland 2021,’ 9.

¹³⁷ Schenkkan en Linzer, ‘The global scale and scope of transnational repression,’ 1–2.

¹³⁸ ‘EU en VS veroordelen "ongekende kaping vliegtuig door Wit-Rusland”.’

¹³⁹ Schildkamp en Tieleman, ‘Moordaanslag op Peter R. de Vries’.

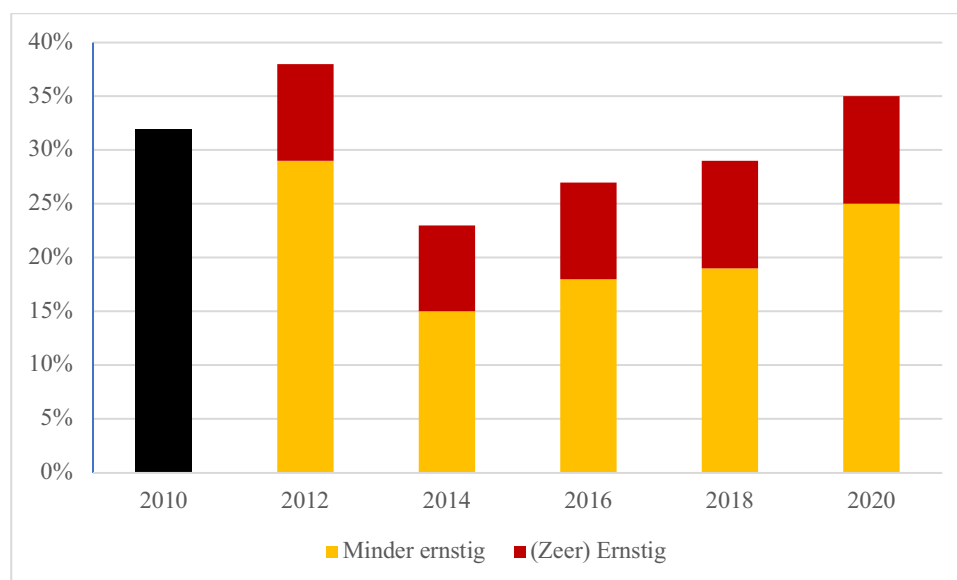
op de fundamenten van de Nederlandse rechtsstaat wordt uitgeoefend. Zoals de moord op Derk Wiersum onder advocaten tot grote zorgen leidde, zorgt ook de moord op De Vries voor consternatie onder misdaadverslaggevers. Ook al lijkt deze moord specifiek met de Marengo-zaak verband te houden, de gevolgen van de aanslag hebben een effect op de beroepsgroep als geheel.¹⁴⁰

¹⁴⁰ Lüdke en Rojkov, 'Fears mount following attack'.

Dreiging in cijfers

Het voorgaande overzicht maakt in grote lijnen inzichtelijk hoe stelselrelevante dreigingen zich de afgelopen twintig jaar hebben ontwikkeld. Maar om de aard en omvang van dreigingen in deze periode nauwkeurig te kunnen beoordelen, is het belangrijk om ook het beschikbare cijfermateriaal de revue te laten passeren.

De ‘Monitor agressie en geweld openbaar bestuur’ en de ‘Monitor integriteit en veiligheid’ omvatten verschillende rapporten die inzicht geven in de percentages politieke ambtsdragers in het lokaal bestuur die jaarlijks met agressie, bedreiging en intimidatie te maken krijgen. Figuur 1 vat de beschikbare informatie samen en neemt waar mogelijk ook het door de monitors gehanteerde onderscheid tussen minder en (zeer) ernstige bedreigingen over.¹⁴¹ Gezien vanaf de eerste meting in 2010 lijkt het aantal bedreigingen te fluctueren, hoewel de trend de afgelopen zes jaar stijgende is. Een belangrijke kanttekening is dat het percentage ‘(zeer)ernstige’ bedreigingen min of meer stabiel lijkt. De toename zit vooral in de als minder ernstig bestempelde incidenten.



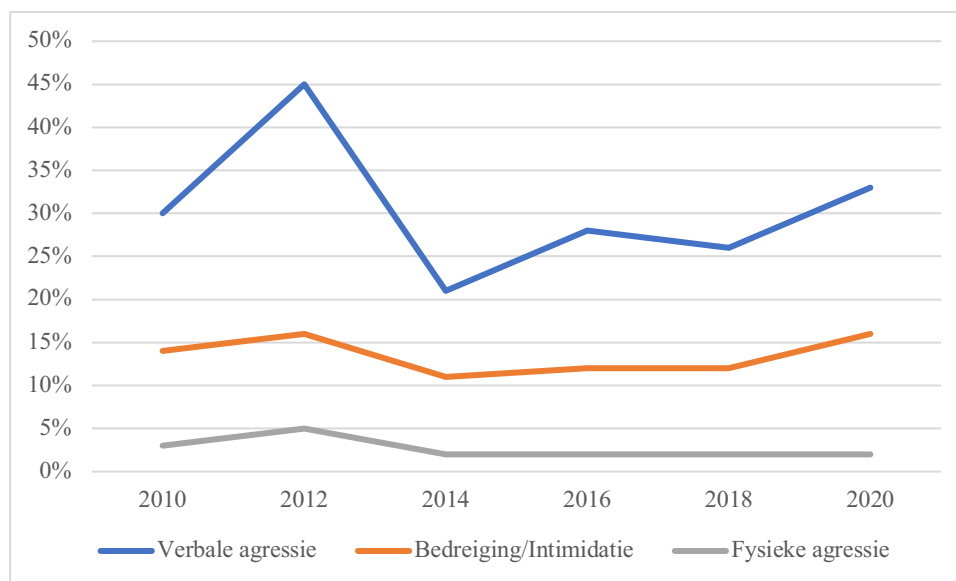
Figuur 1: Agressie en geweld tegen politiek ambtsdragers (decentraal)¹⁴²

In Figuur 2 is de ontwikkeling van het type agressie tegen politiek ambtsdragers op decentraal niveau weergegeven. Ook hier valt op dat er vanaf 2014 meer gevallen van bedreiging worden geregistreerd maar dat fluctuaties de periode in zijn geheel het beste samenvat. Fysieke agressie lijkt al jaren stabiel op 2%.¹⁴³ De meeste groei en de sterkste fluctuaties zit in de categorie ‘verbale agressie’. Het is echter de vraag of deze uitingen, hoe onprettig ook voor de ontvanger, gezien hun minder serieuze aard meegewogen moeten worden in het algehele beeld van stelselrelevante dreigingen.

¹⁴¹ Dit onderscheid is niet beschikbaar voor 2010, hier wordt alleen het totaal weergegeven.

¹⁴² Bouwmeester en Löb, ‘Monitor agressie & geweld 2018,’ 11, 15; Klein Kranenburg et al., ‘Monitor integriteit en veiligheid 2020,’ 20.

¹⁴³ In 2010, 2012 en 2014 werden ook ‘discriminatie’ en ‘seksuele intimidatie’ apart bijgehouden. Vanaf 2016 zijn deze vormen van bedreiging samengevoegd met respectievelijk ‘verbale agressie’ en ‘bedreiging/intimidatie’. Voor de duidelijkheid van het totaalbeeld is die samenvoeging hier over de gehele linie doorgevoerd. Daarnaast zijn de cijfers voor 2014 en 2016 bij benadering omdat ze visueel moesten worden afgelezen uit het document. De foutmarge zal hooguit 2 tot 3 procent bedragen en heeft dus nauwelijks invloed op het totaalbeeld. Zie: Bouwmeester en Löb, ‘Monitor agressie & geweld 2018,’ 13.



Figuur 2: Types agressie en geweld tegen politiek ambtsdragers (decentraal)¹⁴⁴

Een mogelijke verklaring voor de recente toename van bedreigingen tegen lokale bestuurders zoals die vooral uit Figuur 1 naar voren komt, is dat burgemeesters tussen 2010 en 2020 meer gebruik zijn gaan maken van hun openbare orde en veiligheids-bevoegdheden (OOV) in de strijd tegen met name georganiseerde misdaad. Toch waarschuwen onderzoekers om een al te causaal verband met de toegenomen aantallen dreigementen te zien.¹⁴⁵ Verschillende studies wijzen erop dat het internet en sociale media het uiten van bedreigingen heel laagdrempelig hebben gemaakt. Ook wordt regelmatig betoogd dat de toegenomen bedreigingen en de deels ernstigere vorm die ze aannemen, een weerspiegeling zijn van maatschappelijke verharding en afbrokkelend vertrouwen in gezagsdragers.¹⁴⁶

Toch zien Klein Kranenburg en collega's wel een relatie tussen de inzet van OOV-bevoegdheden en bedreigingen tegen decentraal bestuurders, al hangt dat wel af van hoe en tegen wie die middelen worden gebruikt. In het algemeen kan worden gesteld dat 'naarmate een bevoegdheid dieper ingrijpt in het persoonlijke leven of iemand harder treft in diens (criminele) activiteiten, de financiën of andere belangen, het risico op bedreiging of intimidatie voor de burgemeester groter wordt'.¹⁴⁷

Na de moorden op Fortuyn (2002) en Van Gogh (2004) is in 2005 binnen de politie het Team Bedreigde Politici (TBP) opgericht. Het team houdt sindsdien cijfers bij van de aantallen bedreigingen richting personen in het rijksdomein alsook lokale bestuurders die onder de

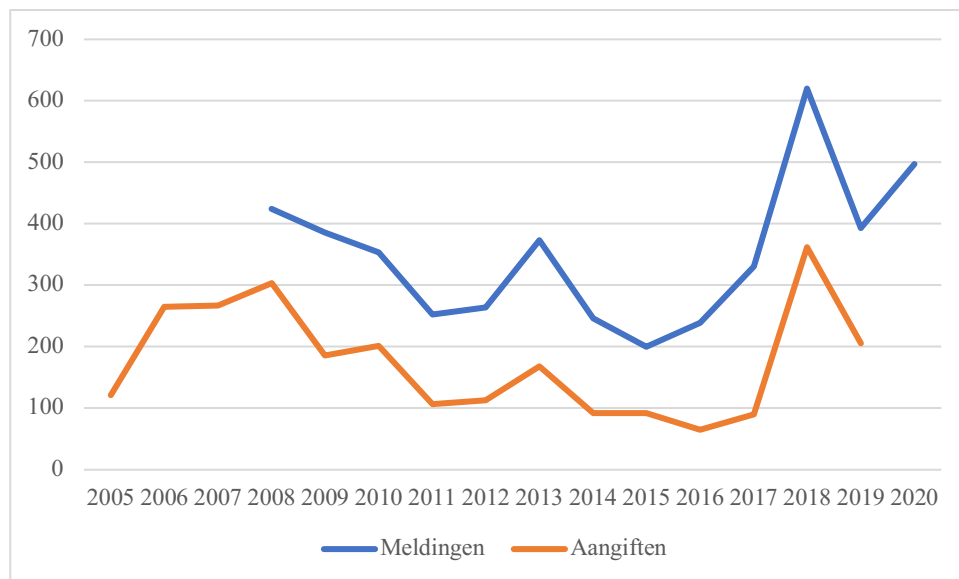
¹⁴⁴ Van den Tillaart et al., 'Monitor agressie en geweld 2012,' 9; Bouwmeester en Löb, 'Monitor agressie & geweld 2018,' 13; Klein Kranenburg et al., 'Monitor integriteit en veiligheid 2020,' 4.

¹⁴⁵ Klein Kranenburg et al., 'Bedreigingen en intimidaties van burgemeesters,' 11.

¹⁴⁶ Borgesius et al., 'Individuele bedreigers van publieke personen,' 76; De Wijk, 'Het stelsel na Pim Fortuyn,' 35; Klein Kranenburg et al., 'Bedreigingen en intimidaties van burgemeesters,' 46, 57-58; Van Gestel en Verhoeven, 'Liquidaties nieuwe stijl,' 9; Andringa, 'Veel meer dreigingen van criminelen'; Van Ham en Van Wijk, 'Bescherming van personen,' 4; Winter et al., 'Criminele beïnvloeding,' 22; Odekerken en Brenninkmeijer, 'Een dreigend klimaat,' 14. Dit thema werd ook door meerdere deelnemers aan de expertsessie benadrukt.

¹⁴⁷ Klein Kranenburg et al., 'Bedreigingen en intimidaties van burgemeesters,' 68.

politie-eenheid Den Haag vallen.¹⁴⁸ In Figuur 3 is de in open bronnen beschikbare informatie weergegeven over de hoeveelheid meldingen van bedreiging en intimidatie en het aantal waarvan daadwerkelijk aangifte is gedaan omdat ze als strafbaar feit zijn beoordeeld. Vergelijkbaar met ambtsdragers op decentraal niveau toont het aantal bedreigingen tegen personen in het rijksdomein ook een fluctuerend patroon over de periode waarin gegevens beschikbaar zijn. Ook hier is vanaf ongeveer 2015 een toename merkbaar die echter veel sterker lijkt te stijgen dan op het decentrale niveau.¹⁴⁹ Een belangrijke kanttekening is dat met name onder de bedreigde politici een kleine groep de meerderheid van de dreigementen ontvangt.¹⁵⁰ Algemeen gesteld lijkt de mate van zichtbaarheid in debatten over maatschappelijk controversiële onderwerpen van invloed op de kans dat politici bedreigd worden.¹⁵¹



Figuur 3: Bedreigingen geregistreerd door het TBP¹⁵²

Cijfers over bedreigingen tegen medewerkers van de politie en het Openbaar Ministerie zijn helaas veel minder compleet. Figuur 4 geeft de uitkomsten van verschillende onderzoeken op dit gebied weer. De resultaten zijn niet altijd direct met elkaar te vergelijken en voor veel jaren is geen informatie beschikbaar; het gaat hier dus expliciet om een ruwe schets. Het percentage politie- en OM-medewerkers dat per jaar met bedreigingen te maken krijgt lijkt ook hier te fluctueren. Daarnaast is opmerkelijk dat specifieke groepen medewerkers binnen beide organisaties beduidend vaker en soms ernstiger worden bedreigd; met name politiepersoneel met burgercontact en officieren van justitie.¹⁵³

¹⁴⁸ 'Team Bedreigde Politici.'

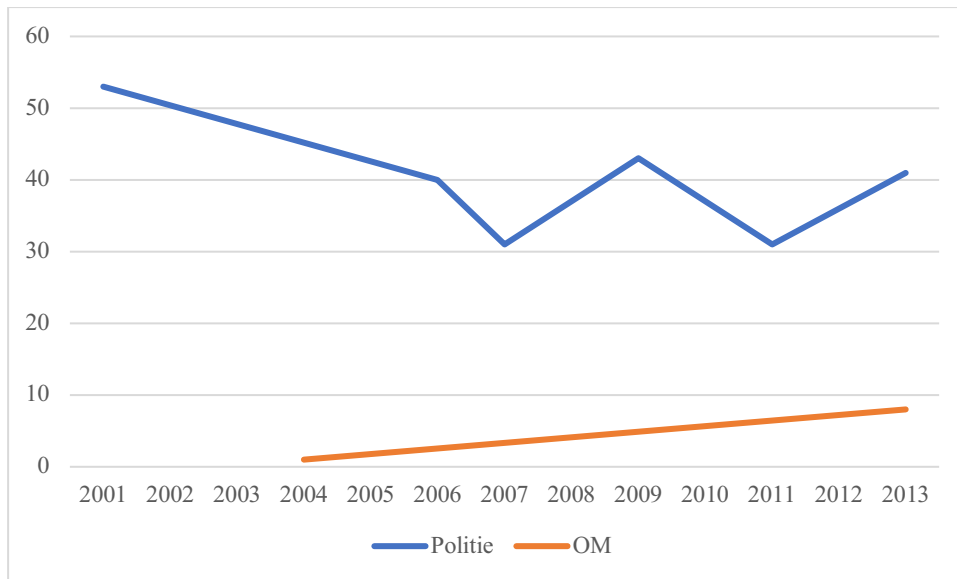
¹⁴⁹ Het aantal aangiften in 2020 was op het moment van schrijven nog niet beschikbaar.

¹⁵⁰ Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2007,' 70.

¹⁵¹ Bjørge en Silkoset, 'Threats and threatening approaches to politicians,' 21–22.

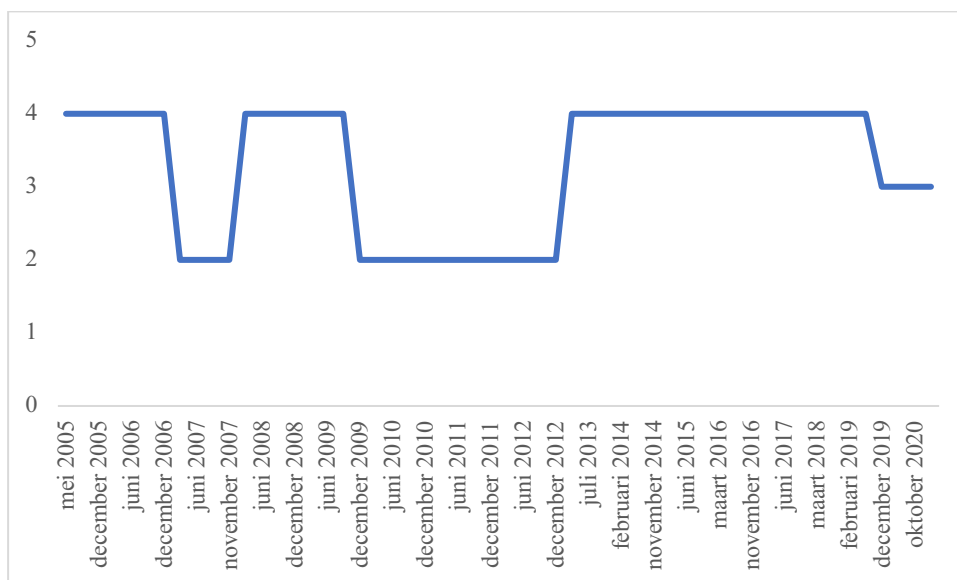
¹⁵² 'Politici werden 121 keer bedreigd'; 'Aangifte bedreigde politici neemt vlucht'; 'Minister en Kamerlid worden vaker bedreigd'; 'Politici 424 keer bedreigd'; 'Iets meer politici bedreigd in 2010'; 'Minder politici bedreigd in 2011'; 'Forse stijging bedreigde politici'; 'Politici vorig jaar 113 keer bedreigd,' 113; Van Haenen, 'Facebook-dreiger vindt zichzelf nu een ezel'; 'Minder strafbare bedreigingen tegen politici'; 'Stijging strafbare bedreigingen tegen politici'; 'Ruim tweehonderd strafbare bedreigingen tegen politici in 2019'; 'Politici vaker en ernstiger bedreigd, zelfs door kinderen onder de 12 jaar.'

¹⁵³ Van der Torre, Gieling en Bruinsma, 'Bedreigen en intimideren van OM- en politiemedewerkers,' 16, 19, 52.



Figuur 4: Schets van bedreigingen tegen medewerkers politie en OM¹⁵⁴

Tot slot laat Figuur 5 de ontwikkeling van de dreiging op een terroristische aanslag in Nederland zien. Dit dreigingsniveau wordt sinds 2005 door de NCTV (toen nog NCTb) vastgesteld in het periodiek verschijnende ‘Dreigingsbeeld Terrorisme Nederland’. Vanaf juli 2016 is het aantal niveaus van 4 naar 5 uitgebreid waardoor niveau 3 pas recent tot de mogelijkheden is gaan horen. Wat vooral opvalt is de regelmatige fluctuatie; de dreiging van een aanslag is meerdere keren van ‘substantieel’ naar ‘beperkt’ en omgekeerd gegaan, voordat het in december 2019 op het nieuwe tussenliggende niveau ‘aanzienlijk’ is gesteld. Internationale ontwikkelingen zoals in het jaaroverzicht hierboven vaak genoemd (oorlog in Syrië, ophef over cartoons, opleving rechts-extremisme) lijken een sterke invloed te hebben op de terroristische dreiging in Nederland.



Figuur 5: Dreigingsniveau terroristische aanslag in Nederland¹⁵⁵

¹⁵⁴ Ibid., 6, 16, 18–19, 45, 49.

¹⁵⁵ Gebaseerd op DTN 1 t/m 51: Nationaal Coördinator Terrorismebestrijding en Veiligheid, ‘Dreigingsbeeld terrorisme Nederland.’

Hoewel er de laatste jaren een duidelijke stijging is in het aantal geregistreerde bedreigingen op zowel centraal als decentraal niveau, suggereren de langere termijn cijfers dat het om een fluctuerend patroon gaat. Het is dus niet gezegd dat deze stijging zich ook de komende jaren onverminderd doorzet. Dat maakt de recente toename niet minder ernstig, maar onderstreept wel dat de huidige situatie niet zondermeer een accuraat beeld van de toekomst schetst. Opvallend is dat de recente stijging in het aantal bedreigingen met name personen binnen het rijksofgebied treft; er is geen uniform 'bedreigingsniveau' in Nederland maar er moet onderscheid gemaakt worden naar type politicus of bestuurder. Dat blijkt ook uit cijfers over de aard van de bedreigingen; instrumentele motieven komen met name bij burgemeesters en wethouders voor.¹⁵⁶ Burgemeesters krijgen ook vaker te maken met dreigementen vanuit de georganiseerde misdaad.¹⁵⁷ Dit is deels te wijten aan de toegenomen rol van het lokaal bestuur in de strijd tegen georganiseerde misdaad, maar houdt ook verband met de laagdrempeligheid van het internet als medium om bedreigingen te uiten, maatschappelijke verharding en afgenomen vertrouwen in gezagsdragers.

Internationale vergelijking

Bedreigingen aan het adres van politici, ambtenaren, lokale bestuurders en journalisten zijn geen uniek Nederlands fenomeen. Ook internationaal worstelen nationale en lokale overheden met dit type uitdagingen. Zo stelt onderzoek uit 2015 dat 30 à 93% van de bevroegde politici in Canada, het Verenigd Koninkrijk, Australië, Zweden en Nieuw-Zeeland ooit te maken heeft gehad met stalking, bedreiging of geweld.¹⁵⁸ Een andere studie uit 2015 laat zien dat 55% van de respondenten onder leden van het Britse parlement in een jaar tijd een vorm van bedreiging of agressief gedrag heeft meegemaakt.¹⁵⁹ Ook in Noorwegen en het Verenigd Koninkrijk constateren onderzoekers toenemende aantallen bedreigingen van politici die via sociale media worden geuit.¹⁶⁰ Net als in Nederland wordt internationaal ook opgemerkt dat dreigers en geweldplegers tegen politici opvallend vaak kampen met mentale gezondheidsproblematiek.¹⁶¹

¹⁵⁶ Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 'Bedreigd bestuur 2010,' 18; Klein Kranenburg et al., 'Bedreigingen en intimidaties van burgemeesters,' 52.

¹⁵⁷ Klein Kranenburg et al., 'Monitor integriteit en veiligheid 2020,' 27; Klein Kranenburg et al., 'Bedreigingen en intimidaties van burgemeesters,' 52, 55; Winter et al., 'Criminele beïnvloeding,' 3.

¹⁵⁸ Every-Palmer, Barry-Walsh en Pathé, 'Harassment, stalking, threats and attacks.'

¹⁵⁹ James et al., 'Aggressive/intrusive behaviours.'

¹⁶⁰ Bjørge en Silkoset, 'Threats and threatening approaches to politicians,' 5, 12; Akhtar en Morrison, 'The prevalence and impact of online trolling.'

¹⁶¹ Pathé et al., 'Public figure fixation'; Riess, Gonzalez en Koreniz, 'Management of patients who make threats against elected officials'; James et al., 'The role of mental disorder in attacks on European politicians.'

Ontwikkeling stelselrelevante dreigingen

De terugblik op stelselrelevante dreigingen heeft een veelvoud aan incidenten en ontwikkelingen aan het licht gebracht. In hoeverre laten zich patronen herkennen die zicht bieden op de uitdagingen waar het stelsel zich de komende jaren mee geconfronteerd kan zien? Hieronder wordt op deze vraag puntsgewijs ingegaan.

1. Fluctuatie en nuancering

Journalisten, onderzoekers en beleidsmakers hebben begrijpelijkerwijs veel aandacht voor de nieuwste ontwikkelingen als het op dreigingen aankomt. Toch blijft het van belang om recente ontwikkelingen in een bredere (historische) context te plaatsen om hun relevantie voor het dreigingsbeeld met nuance te kunnen beoordelen. Dreigingen tegen en zelfs aanslagen op hoogwaardigheidsbekleders zijn van alle tijden.¹⁶² Bedreigingen vanuit de georganiseerde misdaad richting lokale bestuurders, officieren van justitie en advocaten zijn al sinds de jaren 1980 een regelmatig terugkerend onderwerp van debat.¹⁶³ Die continuïteit geldt ook voor liquidaties onder criminelen, dreigementen aan het adres van journalisten, terrorisme en in zekere zin zelfs voor de dreiging van statelijke actoren.¹⁶⁴ Cijfers over bedreigingen richting lokale bestuurders en politici die onder het rijksdomein vallen, laten bovendien zien dat recente toenames in breder perspectief onderdeel lijken te zijn van een fluctuerend patroon.¹⁶⁵ Dat geldt ook voor de dreiging van terrorisme zoals door de NCTV vastgesteld.

Een tweede punt dat van belang is bij het interpreteren van met name de kwantitatieve informatie over de ontwikkeling van stelselrelevante dreigingen, is dat een meerderheid van de geuite bedreigingen geen daadwerkelijk risico op een geweldsdaad vormt.¹⁶⁶ Verreweg de meeste dreigers komen niet verder dan het uiten van grieven en voor een groot deel is dat simpelweg het doel.¹⁶⁷ Op basis van de hierboven weergegeven cijfers en bevindingen van onderzoekers uit binnen- en buitenland, lijkt er vooral veel groei te zitten in de expressieve bedreigingen die via internet en sociale media worden geuit. Bedreigingen die met fysiek geweld gepaard gaan, daarentegen, lijken bijvoorbeeld op basis van de cijfers over lokale ambtsdragers stabiel op een relatief laag niveau. Een toenemend aantal bedreigingen betekent dus niet zondermeer dat er ook een grotere noodzaak is tot daadwerkelijke persoonsbeveiliging. Dit geldt des te meer voor de als minder ernstig ingeschatte ‘verbale agressie’.

Deze observaties zijn niet bagatelliserend bedoeld. Er lijkt de laatste jaren inderdaad sprake van toenemende aantallen bedreigingen, met name richting politici in het rijksdomein. Ook dodelijk geweld onder criminelen valt steeds meer op, met toenemende risico's voor omstanders.¹⁶⁸ Bovendien kunnen ook relatief minder ernstige bedreigingen grote negatieve gevolgen hebben voor de persoonlijke levenssfeer van de getroffen. De moorden op Fortuyn en Van Gogh zijn daarnaast tekenend voor de grote invloed die ook een enkele geweldsdaad kan hebben. De beschikbare cijfers drukken ook maar ten dele uit dat de *ernst* van de dreigingen in recente jaren lijkt te zijn toegenomen, zoals de moorden op advocaat Derk Wiersum en

¹⁶² De Wijk, ‘Het stelsel na Pim Fortuyn,’ 6; Pathé, ‘Stalking public figures,’ 295; Kuiper, ‘Het woord en de daad,’ 13.

¹⁶³ Buruma, ‘Ondermijning en de veerkracht van de rechtsstaat’; Bovenkerk, ‘Bedreigingen in Nederland,’ 90–91.

¹⁶⁴ AIVD, MIVD en NCTV, ‘Dreigingsbeeld statelijke actoren,’ 8; Van Ham en Van Wijk, ‘Bescherming van personen,’ 4; Van Gestel en Verhoeven, ‘Liquidaties nieuwe stijl,’ 15.

¹⁶⁵ Klein Kranenburg et al., ‘Bedreigingen en intimidaties van burgemeesters,’ 7.

¹⁶⁶ Algemene Inlichtingen- en Veiligheidsdienst, ‘Jaarverslag AIVD 2010,’ 23; Algemene Inlichtingen- en Veiligheidsdienst, ‘Jaarverslag AIVD 2011,’ 37.

¹⁶⁷ Borgesius et al., ‘Individuele bedreigers van publieke personen,’ 10–11.

¹⁶⁸ Aarten en Liem, ‘Unravelling the homicide drop’; Van Gestel en Verhoeven, ‘Liquidaties nieuwe stijl,’ 9.

journalist Peter R. de Vries illustreren. Waar cijfers vooral op wijzen is dat het hier-en-nu geen bijzonder accurate graadmeter is voor de langere termijn ontwikkeling van stelselrelevante dreigingen en dat omvang en ernst niet noodzakelijkerwijs aan elkaar verbonden zijn.

Vooruitblikkend lijken op dit punt drie zaken van belang. Allereerst, dat het stelsel in praktische zin in staat is om snel en flexibel te reageren op toenames in het aantal (ernstige) bedreigingen en voldoende capaciteit heeft om al-dan-niet tijdelijke pieken in het aantal te beveiligen personen, locaties of instituties op te kunnen vangen. Ten tweede, dat methoden om ernstige en minder-ernstige dreigingen van elkaar te kunnen scheiden van toenemend belang lijken te zijn. Zo kan de beschikbare capaciteit zo effectief mogelijk worden ingezet. Tot slot, dat een proportionele respons op nieuwe ontwikkelingen in de omvang of ernst van stelselrelevante dreigingen baat kan hebben bij een zekere mate van distantie en het plaatsen van die ontwikkelingen in hun recente historische context.

2. De actie-reactie cyclus

De ernst en omvang van bedreigingen tegen met name lokale bestuurders, maar ook officieren van justitie, advocaten en journalisten, lijkt onderhevig aan een actie-reactie cyclus. Meer aandacht voor de lokale aanpak van criminaliteit, het in de media portretteren van officieren van justitie als *crime fighters*, vervolging van een machtige criminele organisatie door inzet van kroongetuigen, diepgravende rapportages over drugscriminelen; het leidt in veel gevallen tot (ernstige) bedreigingen en zelfs moordaanslagen vanuit criminele netwerken die zich in het nauw gedreven voelen.¹⁶⁹ Vooral instrumentele bedreigingen lijken sterk contextgebonden. Recente uitbreidingen van de wettelijke bevoegdheden voor lokale bestuurders om op te treden in het kader van de openbare orde en veiligheid, en een toegenomen bereidheid om deze middelen in te zetten, dragen bij aan deze wisselwerking.¹⁷⁰ De toenemende zorgen voor ondermijning van (lokale) overheidsstructuren door met name invloedrijke drugscriminelen en lopende rechtszaken tegen machtige criminele organisaties, maakt het waarschijnlijk dat deze cyclus ook de komende jaren tot bedreigingen en dodelijk geweld zal leiden.¹⁷¹

3. Verruwing en toenemend geweld vanuit de georganiseerde misdaad

Benadrukken dat veel stelselrelevante dreigingen meerjarige continuïteit vertonen mag niet verhullen dat er wel degelijk veranderingen in aard en ernst lijken te zijn. Twee belangrijke meerjarige trends in dit kader zijn maatschappelijke verruwing, waar wetenschappers al sinds de moord op Fortuyn op wijzen, en met name de toegenomen geweldd bereidheid vanuit de georganiseerde criminaliteit. Verruwing van omgangsvormen en afnemend respect voor gezagsdragers en bestuurders hebben voor veel burgers de drempel tot het uiten van bedreigingen verlaagd. De opkomst van het internet en sociale media hebben het bovendien zeer eenvoudig gemaakt om vanuit relatieve anonimiteit te dreigen en intimideren. Zoals op meerdere punten in dit rapport is aangegeven, gaat van de meerderheid van dit soort bedreigingen een klein risico op daadwerkelijk geweld uit.

Wat de geweldd bereidheid vanuit de georganiseerde criminaliteit betreft, valt op dat criminelen sneller tot liquidaties overgaan, dat daders steeds jonger worden en dat grof vuurwapengeweld

¹⁶⁹ Van der Torre, Gieling en Bruinsma, 'Bedreigen en intimideren van OM- en politiemedewerkers,' 21; Klein Kranenburg et al., 'Bedreigingen en intimidaties van burgemeesters,' 68.

¹⁷⁰ Klein Kranenburg et al., 'Bedreigingen en intimidaties van burgemeesters,' 30.

¹⁷¹ Zorgen over ondermijning werden in de expertsessie door verschillende deelnemers beaamd: Medewerker Politie 2, Bijdrage aan de expertsessie; Medewerker NCTV 1, Bijdrage aan de expertsessie.

de norm wordt, met grote risico's voor omstanders.¹⁷² Ook lijken er steeds minder grenzen aan wie er doelwit van een liquidatie wordt. Zoals de moord op advocaat Derk Wiersum, de moord op de broer van kroongetuige Nabil B. en onlangs de moord op journalist Peter R. de Vries aantonen, is geweld vanuit het criminele milieu allesbehalve een interne aangelegenheid die aan onderlinge competitie ontspringt. Steeds vaker lijken representanten van de rechtsstaat het doelwit. De aanslagen die vanuit het netwerk rondom Ridouan T. zijn uitgevoerd schakelen niet alleen zijn directe tegenstanders uit maar hebben bedoeld of onbedoeld ook een grote negatieve invloed op het werk van advocaten, journalisten en professionals in aanpalende velden in bredere zin.

Zo lijken er twee tendensen te zijn die naar verwachting ook de komende jaren invloedrijk zullen blijven. Enerzijds is het waarschijnlijk dat (lokale) bestuurders, ambtenaren en politici in toenemende mate en vooral via sociale media bedreigd zullen worden. Zonder de gevolgen op persoonlijk niveau te willen bagatelliseren gaat het hier echter veelal om expressieve dreigementen met een laag concreet risico op geweld. Anderzijds lijkt er met name in het criminele milieu sprake van een lagere drempel om dodelijk geweld toe te passen tegen rivalen in de onderwereld maar ook, zoals de Marengo-zaak aantoont, in toenemende mate tegen vermeende tegenstanders in de bovenwereld. Gekoppeld aan de al jaren groeiende zorgen over criminele ondermijning van (lokale) overheidsstructuren en de hierboven genoemde actie-reactie cyclus, is het waarschijnlijk dat het stelsel in de nabije toekomst ingericht moet zijn en blijven op (zeer) ernstige dreigingen vanuit de georganiseerde misdaad.

4. Aanhoudende terroristische dreiging

De dreiging van terroristisch geweld in Nederland en de EU is decennia oud en zal aanhouden. Op dit moment vertegenwoordigt het jihadisme nog altijd de grootste dreiging qua terroristische aanslagen in de Nederlandse context. De opkomst van met name rechts-extremistisch terrorisme in landen als Duitsland, Noorwegen en de VS, of de verspreiding van rechts-extremistische ideeën onder bijvoorbeeld militairen, is tot op heden nog maar in geringe mate weerspiegeld in het Nederlandse dreigingsbeeld. Echter, de terroristische dreiging is sterk gedreven door internationale ontwikkelingen en het is dus voorstelbaar dat ook in Nederland andere vormen van extremisme dan het jihadisme tot aanslagen zullen leiden. De NCTV noemt in deze context specifiek rechts-, identitair- en anti-overheidsextremisme.¹⁷³

Dat de terroristische dreiging voorsnog met name uit jihadistische hoek komt, neemt ook niet weg dat er wel degelijk (tijdelijke) oplevingen van andere vormen van extremisme voorstelbaar zijn. Zo zag de AIVD bijvoorbeeld in 2009 het links- en dierenrechtenextremisme plots toenemen.¹⁷⁴ Recentelijk lijkt de rechts-extremistische beweging nieuw elan te hebben gekregen en, met name door het subtieler verpakken van het gedachtegoed, een groter publiek te bereiken met racistische ideeën en complottheorieën. Ook de vorm die de terroristische dreiging neemt is aan verandering onderhevig; was het jihadisme omstreeks 11 september 2001 vooral een dreiging van buitenaf, zo maakten de aanslagen in Madrid (2004), Amsterdam (2004) en Londen (2005) duidelijk dat er een *homegrown* dimensie aan de dreiging was toegevoegd. Vanaf circa 2011 is bovendien de dreiging van jihadistische en

¹⁷² Van Gestel en Verhoeven, 'Liquidaties nieuwe stijl,' 9, 20–21; Van Ham en Van Wijk, 'Bescherming van personen,' 6–7.

¹⁷³ Nationaal Coördinator Terrorismebestrijding en Veiligheid, 'Nationale veiligheid strategie 2019,' 26; Medewerker NCTV 2, Bijdrage aan de expertsessie.

¹⁷⁴ Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2009,' 24–25.

rechtsextremistische eenlingen toegenomen.¹⁷⁵ Kortom, ook al blijft het jihadisme voorlopig de voor Nederland voornaamste terroristische dreiging, de vorm van deze dreiging zal blijven veranderen en met name vanuit rechts-extremistische hoek lijkt terroristisch geweld ook voorstelbaar.

5. (On)voorstelbare dreigingen

Terroristische aanslagen genereren aandacht maar leiden ook vrij snel tot een vorm van gewenning. Terroristen zijn daardoor steeds opzoek naar aanslagen die qua vorm of doelwitten opnieuw weten te shockeren. Dergelijke tactische innovatie werkt aanstekelijk; de aanslagen met voertuigen in Berlijn en Nice hebben andere jihadisten tot nabootsing aangezet en lijken ook in rechts-extremistische kringen als legitiem gewelddmiddel te worden gezien. Het blijft dus essentieel om naast gekende ook *voorstelbare* aanslagen in risicoanalyses mee te nemen en om daarbij vooral ook naar ontwikkelingen buiten Nederland te kijken. Bovendien geven met name de moord op advocaat Wiersum in 2019 en de moord op journalist Peter R. de Vries in 2021 aan dat voorheen onwaarschijnlijke of onvoorstelbare vormen van geweld niet alleen aan terroristen zijn voorbehouden maar ook kunnen voortkomen uit bijvoorbeeld de georganiseerde misdaad.

Bij het inschatten van mogelijke toekomstige dreigingen blijft het dus belangrijk om niet alleen terug te kijken op bekende bronnen van dreiging en geweld, maar vooral ook met fantasie uiteenlopende en zelfs vooralsnog fictieve scenario's de revue te laten passeren. Het nauwgezet volgen van internationale ontwikkelingen op het gebied van dreigingen kan hierbij helpen. Tegelijkertijd dringt juist de onvoorspelbaarheid van dreigingen, maar ook de continue aanpassing van de modus operandi van opposenten zoals terroristen en statelijke actoren aan heersende veiligheidsmaatregelen, een ongemakkelijke conclusie op. Het is simpelweg niet mogelijk om alle dreigingen vroegtijdig te onderkennen en neutraliseren. Ook in de toekomst zal onze maatschappij met enige regelmaat geschokt gaan worden door nieuwe aanslagen, nog excessiever geweldgebruik en verdere verzuivering. Dit betekent niet noodzakelijkerwijs dat het stelsel gefaald heeft. Een risicoloze samenleving is simpelweg niet haalbaar en bovendien in veel opzichten ook niet wenselijk.

6. Dreigers met mentale-gezondheid gerelateerde problematiek

Zowel in Nederland als daarbuiten lijken personen met problemen op het vlak van de mentale gezondheid verantwoordelijk voor een aanzienlijk deel van de geuite bedreigingen.¹⁷⁶ Ook bij recente (terroristische) aanslagen in Nederland is de invloed van deze brede categorie stoornissen en problemen zichtbaar (Malek F. en Gökmen T.). De toenemende invloed van complotdenken en desinformatie verspreid via het internet zou specifiek op deze groep personen een mobiliserend effect kunnen hebben. Naar verwachting zal de potentieel gewelddadige eenling, waarbij in veel gevallen een mentale gezondheidscomponent een rol speelt, ook in de toekomst een dreiging vormen.

7. Internet, complotdenken en de dreiging van statelijke actoren

Het internet is bijzonder relevant geworden voor de ontwikkeling van stelselrelevante dreigingen. Op de eerste plaats biedt het internet zeer laagdrempelige mogelijkheden om met een mate van anonimiteit bedreigingen te uiten en dit komt dan ook steeds vaker voor. Op de tweede plaats geeft het toegang tot radicale en extremistische ideeën en de digitale gemeenschappen waarbinnen deze wereldbeelden gepropageerd worden. Complotdenken is in

¹⁷⁵ De (jihadistische) eenling werd ook expliciet benoemd als aanhoudende dreiging in de expertsessie: Medewerker NCTV 1, Bijdrage aan de expertsessie.

¹⁷⁶ Van der Torre, Gieling en Bruinsma, 'Bedreigen en intimideren van OM- en politiemedewerkers,' 53.

sterke mate door het internet aangewakkerd en heeft geleid tot de verspreiding van allerlei desinformatie over bijvoorbeeld de werking van vaccins, de coronacrisis en de Amerikaanse verkiezingen. Dit heeft niet alleen potentieel schadelijke gevolgen voor de volksgezondheid en voor vertrouwen in de overheid en wetenschap. Hoewel de meeste complotdenkers en systeemhaters niet verder gaan dan online hun ongenoegen uiten, zijn er de afgelopen maanden in Nederland en daarbuiten ook pogingen geweest om aanslagen te plegen op instituties en personen betrokken bij de bestrijding van het Covid-19 virus.¹⁷⁷

Het internet is ook een steeds belangrijker domein voor statelijke actoren met vijandelijke intenties. Cyberspionage bedoeld om waardevolle economische, wetenschappelijke en militaire informatie te stelen en pogingen om via het internet sabotageacties door te voeren onderstrepen het toenemende belang van de monitoring en bescherming van ICT-infrastructuur. Ook sommige cybercriminelen hebben de capaciteit om de Nederlandse digitale infrastructuur te ontwrichten. Een thema dat statelijke en non-statelijke actoren gemeen hebben is de digitale verspreiding van desinformatie om maatschappelijk vertrouwen in onder andere objectieve journalistiek, het politieke systeem en wetenschappelijke expertise te ondergraven. In een gezamenlijke publicatie benadrukken de AIVD, MIVD en NCTV dat het moeilijk vast te stellen is of digitale inlichtingen- en beïnvloedingsactiviteiten de laatste jaren zijn toe- of afgenomen.¹⁷⁸ Het lijkt echter zeer waarschijnlijk dat met name de verspreiding van desinformatie, zowel door burgers als door staten, in toenemende mate een bron van frictie en afkalvend vertrouwen in instituties en gezaghebbers zal worden en dat het zo zal bijdragen aan de vorming van nieuwe dreigingen die onder de verantwoordelijkheid van het stelsel zullen vallen.¹⁷⁹ Gezien de grenzenloosheid van het internet is het hier in het bijzonder aan te bevelen om oog te houden voor de ervaringen van bondgenoten zoals de VS, het VK en andere EU-lidstaten op dit gebied om zo voor Nederland relevante ontwikkelingen tijdig te onderkennen.

8. Dreigingen van binnenuit

Het merendeel van de behandelde literatuur ziet dreigingen richting politici, bestuurders, ambtenaren en journalisten als iets waarvan de bron buiten het directe leef- of werkveld van de slachtoffers ligt. Het zijn boze burgers, gefrustreerde eenlingen of criminelen die hun inkomstenbron proberen veilig te stellen. De rol die voormalig president Trump had in het aanzetten tot de bestorming van het Capitool en de weigering van grote delen van de Republikeinse partij om hem rekenschap te laten afleggen voor het ondergraven van een essentieel democratisch beginsel als vrije verkiezingen, suggereren dat democratische staten ook kwetsbaar zijn voor groeiend extremisme binnen de eigen instituties.

Op kleinere en wellicht concretere schaal geldt het risico op ondermijning van binnenuit ook voor rechts-extremistische militairen waar in landen als Duitsland en de VS toenemend aandacht voor is. Een directe vergelijking op deze thema's met Nederland gaat gelukkig niet op, hoewel een politicus die tijdens de laatste verkiezingen de NOS afdoet als *fake news* zorgen baart. Deze voorbeelden dienen vooral ter herinnering dat dreigingen uit onverwachte hoek kunnen komen, zelfs in ogenschijnlijk stabiele staten. Het lijkt verstandig om de komende jaren expliciet rekening te houden met zowel externe als interne dreigingen voor de Nederlandse staat en zijn instituties en zicht te houden op de hier beschreven buitenlandse ontwikkelingen.¹⁸⁰

¹⁷⁷ Van Buuren, 'Doelwit Den Haag?', 240–46.

¹⁷⁸ AIVD, MIVD en NCTV, 'Dreigingsbeeld statelijke actoren,' 20.

¹⁷⁹ Piazza, 'Fake news'.

¹⁸⁰ Medewerker ICCT 1, Bijdrage aan de expertsessie.

9. De grote invloed (internationale) incidenten en ontwikkelingen

Dat de ontwikkeling van stelselrelevante dreigingen zich lastig laat voorspellen is in belangrijke mate te wijten aan de invloed van incidenten of onvoorziene ontwikkelingen. Des meer omdat deze zich vaak in het buitenland voordoen om vervolgens ook in Nederland invloed uit te oefenen.¹⁸¹ Zo tekenen AIVD-jaarverslagen tussen 2005 en 2011 een Nederlandse jihadistische beweging die lethargisch en stuurloos lijkt. Het uitbreken van de Syrische burgeroorlog in 2011 en vooral het uitroepen van het IS-kalifaat in 2014 brengen een ommekeer teweeg en grote getalen Nederlandse jihadisten reizen uit naar het strijdgebied. Ook op kleinere schaal kunnen incidenten of kortstondige gebeurtenissen een toename van stelselrelevante dreigingen betekenen. Bijvoorbeeld een groot internationaal overleg, zoals de *Nuclear Security Summit* die Nederland in 2014 organiseerde of de vluchtelingencrisis die de EU in 2015 trof.¹⁸²

Kunnen inspelen op plotselinge gebeurtenissen met dreiging-verhogend effect en over de grenzen kijken om de mogelijke invloed van internationale gebeurtenissen te anticiperen, zal ook de komende jaren van groot belang blijven. Naast deze alertheid moet echter gewaakt worden om niet in ieder opzienbarend gewelddadig incident de aankondiging van een nieuwe trend te zien. De moorden op Fortuyn (2002) en Van Gogh (2004) hebben bijvoorbeeld niet geleid tot een golf van aanslagen en politieke moorden, ondanks hun grote invloed op de Nederlandse samenleving. Bovendien zijn veel dreiging-verhogende gebeurtenissen van (relatief) korte duur; nu bijvoorbeeld het einde van coronacrisis in zicht lijkt te komen, is te verwachten dat het aantal hieraan gerelateerde bedreigingen ook zal afnemen.¹⁸³ Enige kritische distantie kan helpen om bedreigingen en de noodzakelijke respons vanuit het stelsel in proportie te zien, hoewel dit uiteraard in crisismomenten uitermate moeilijk is.

10. Een brede groep bedreigden

Stelselrelevante dreigingen treffen niet alleen bestuurders, politici en ambtenaren. Zoals de gebeurtenissen rondom het Marengo-proces hebben laten zien, en zoals in bredere zin de uit geraadpleegde bronnen naar voren komt, zijn ook advocaten en journalisten beroepsgroepen die met (zeer) ernstige bedreigingen en (dodelijk) geweld te maken hebben. Alle twee zijn onontbeerlijk in een rechtsstaat en het dient de aanbeveling dat het stelsel zich in de toekomst breed blijft oriënteren op personen en instituties die wellicht aanvullende bescherming nodig hebben. De moord op Khashoggi en de recente kaping van een passagiersvliegtuig door Wit-Rusland om een journalist te kunnen arresteren, illustreren dat met name journalisten ook internationaal doelwit kunnen worden van agressief optredende statelijke actoren. De twee moorden op Iraanse Nederlanders in 2015 en 2017 brengen bovendien in herinnering dat ook politieke dissidenten en bredere diaspora gemeenschappen die in Nederland wonen het doelwit kunnen worden van vijandig opererende staten. Tot slot onderstreept de moord op scholiere Hümeyra in 2018 dat ook 'gewone burgers' slachtoffer kunnen worden van zeer ernstige dreigingen die in dodelijk geweld uitmonden.¹⁸⁴

¹⁸¹ Medewerker Ministerie van Binnenlandse Zaken, Bijdrage aan de expertsessie.

¹⁸² De Wijk, 'Het stelsel na Pim Fortuyn,' 33–35; Binnenlandse Veiligheidsdienst, 'Jaarverslag Binnenlandse Veiligheidsdienst 2000,' 16; Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2007,' 70; Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2010,' 23–24; Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2012,' 50; Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2013,' 27; Klein Kranenburg et al., 'Bedreigingen en intimidaties van burgemeesters,' 7.

¹⁸³ Medewerker NCTV 2, Bijdrage aan de expertsessie.

¹⁸⁴ Medewerker Politie 2, Bijdrage aan de expertsessie.

Dit leidt tot een pleidooi voor flexibiliteit ten aanzien van de individuen en instanties die in het kader van het stelsel bescherming nodig kunnen hebben. Door de coronacrisis zijn op dit moment bijvoorbeeld wetenschappers van het RIVM en het *Outbreak Management Team* (OMT) tamelijk zwaar bedreigd. Afhankelijk van de maatschappelijke crisis of onrust kunnen ook andere personen in het vizier komen van dreigers.¹⁸⁵ Recente voorbeelden zijn onder andere boze boeren die politici thuis bezochten en windmolenbestrijders die bestuurders bedreigden.¹⁸⁶ Een deelnemer aan de expertsessie sprak in deze context over de ‘democratisering van bedreigingen’.¹⁸⁷ Vooruitblikken blijft uitermate lastig, maar naar alle waarschijnlijkheid zullen er ook in de (nabije) toekomst nieuwe vormen van onrust ontstaan die aanleiding vormen voor bedreigingen, bijvoorbeeld in verband met een ingrijpende energietransitie, de mogelijke economische gevolgen van de coronacrisis of een langlopende strafzaak tegen groepen en personen die bereid zijn om geweld te gebruiken in een poging om de rechtsgang te ondermijnen. Zowel op centraal als decentraal niveau zal het voor de effectiviteit van het stelsel essentieel zijn om snel te kunnen schakelen tussen de personen of instituties die bescherming nodig hebben.

Valkuilen van vooruitblikken

De geschiedenis van het vooruitblikken op toekomstige ontwikkelingen qua dreigingen is er één vol missers. De val van de Sovjet Unie en het einde van de Koude Oorlog, bijvoorbeeld, kwam voor veel experts als een verassing.¹⁸⁸ In de jaren voorafgaand aan de aanslagen van 11 september waren er amper terrorismeonderzoekers die zich met het Soennitisch jihadisme bezighielden.¹⁸⁹ Over de toekomst van oorlog stelt Colin Gray dat we alleen met zekerheid kunnen zeggen dát conflicten zullen blijven plaatsvinden, niet precies in welke vorm, wanneer, waar of wie erbij betrokken zal zijn.¹⁹⁰ Terughoudendheid is dus geboden, net als een mate van acceptatie voor het gegeven dat de onvoorspelbaarheid van dreigingen betekent dat niet ieder geweldsincident voorkomen kan worden.

Naast deze voorbehouden komt uit de literatuur ook een duidelijke aanbeveling naar voren als het gaat om het inschatten van toekomstige dreigingen. Namelijk, om zoveel mogelijk los te komen uit de tunnelvisie op de meest recente dreiging. Het is onvermijdelijk en ook noodzakelijk dat ontwikkelingen op dreigingsgebied op de voet gevolgd worden. Tegelijkertijd betogen onderzoekers als Marieke de Goede dat onze ideeën over toekomstige dreigingen in belangrijke mate voortvloeien uit onze percepties van wat *op dit moment* de meest prangende dreigingen zijn.¹⁹¹ Uit het hier-en-nu loskomen en breder kijken dan de meest recente crisis lijkt dus essentieel om toekomstige ontwikkelingen zo goed en kwaad als het kan in kaart te brengen. Ontwikkelingen in de landen om ons heen bieden daartoe een mogelijkheid, net als (recent) historisch onderzoek om de actualiteit in perspectief te plaatsen. Wellicht nog effectiever is om specifiek te rade te gaan bij de professionals die het stelsel vormgeven. Wat zijn ontwikkelingen of dreigingen die volgens hen in de waan van de dag soms uit het oog verloren worden? Aangevuld met externe experts zoals wetenschappers zou dit de basis voor een vruchtbare dialoog kunnen vormen.

¹⁸⁵ Medewerker Politie 3, Bijdrage aan de expertsessie; Medewerker ICCT 1, Bijdrage aan de expertsessie.

¹⁸⁶ Rutten, ‘Thuisbezoek boeren aan Jetten onacceptabel’; Bouma, ‘Het gezicht van verzet tegen windmolens.’

¹⁸⁷ Medewerker ICCT 1, Bijdrage aan de expertsessie.

¹⁸⁸ Freedman, *The future of war*, xiv–xix, 286–87.

¹⁸⁹ Schuurman, ‘Topics in terrorism research,’ 465.

¹⁹⁰ Gray, *The future of strategy*, 107–8.

¹⁹¹ De Goede, ‘Beyond risk.’

Conclusie

De afgelopen twintig jaar hebben stelselrelevante dreigingen een aantal kenmerken vertoond die naar verwachting ook beeldbepalend zullen zijn in de nabije toekomst. Zo lijkt de omvang van geuite bedreigingen, zoals tegen politici en (lokale) bestuurders, op de langere termijn eerder te fluctueren dan jaar na jaar toe te nemen. Dat geldt ook wat betreft de dreiging van een terroristische aanslag. Het is dus niet zeker dat de toename in het aantal bedreigingen die zich de laatste jaren aftekent ook zal doorzetten. Bovendien valt op dat relatief minder ernstige bedreigingen en verbale agressie verantwoordelijk zijn voor het leeuwendeel van deze recente groei. Het aantal gevallen waarin dreigers overgaan tot daadwerkelijk geweld lijkt al jaren vrij stabiel op een relatief laag percentage te blijven.

In tegenstelling tot de veranderlijke omvang van het aantal stelselrelevante dreigingen, lijkt er wat betreft hun ernst wel sprake te zijn van een duidelijkere trend. De laatste jaren zijn er toenemende zorgen over groeiende macht van drugscriminelen en de ondermijning van (lokale) bestuursorganen door met name drugsgelateerde criminaliteit. Ook valt de lagere drempel tot excessief geweld vanuit criminele netwerken op. Liquidaties zijn geen nieuw fenomeen in Nederland, maar het gebruik van zware vuurwapens en de onverschilligheid over mogelijke slachtoffers onder omstanders tekenen zich af. De moord op een familielid van een kroongetuige en op een advocaat in het kader van het Marengo-proces zijn zondermeer grensoverschrijdend te noemen en zetten de Nederlandse rechtsstaat onder druk. Hoewel op het moment van schrijven het nog niet zeker is of de aanslag op Peter R. de Vries ook voortkomt uit het netwerk rondom de Marengo-verdachten, lijkt dit wel aannemelijk. Het is in elk geval een verdere aantasting van de rechtsstaat door de georganiseerde misdaad.

Plotselinge toenames in ernst of omvang van stelselrelevante dreigingen lijken in belangrijke mate te wijten aan een actie-reactie dynamiek. Al vanaf de jaren '90 leidt meer aandacht voor de lokale bestrijding van criminaliteit tot meer en ernstigere bedreigingen tegen bijvoorbeeld burgemeesters en officieren van justitie. Het Marengo-proces laat zien dat dit net zo goed geldt voor de aanpak van machtige criminele netwerken op landelijk niveau. De coronacrisis, maar ook bijvoorbeeld de aanpak van het stikstofprobleem, tonen bovendien dat overheidsmaatregelen om crises te bestrijden voor sommige burgers zo impopulair of controversieel zijn dat ze een acute toename van bedreigingen en intimidaties veroorzaken.

Uit het rapport komt ook naar voren dat er plotselinge veranderingen kunnen optreden in wie er beveiligd moet worden. Zo zijn er de laatste jaren toenemende zorgen over bedreiging en intimidatie van journalisten en heeft de coronacrisis opeens wetenschappers en experts van organisaties als het RIVM blootgesteld aan bedreiging van onder andere complotdenkers. De moord op de scholiere Hümeyra illustreert bovendien dat zeer ernstige dreigingen ook 'gewone burgers' kunnen treffen. Tot slot kunnen ook statelijke actoren een dreiging vormen voor in Nederland aanwezige diaspora gemeenschappen, zoals de moorden op twee mannen van Iraanse komaf in 2015 en 2017 aantoonde.

De veranderlijkheid van zowel de omvang als de ernst van stelselrelevante dreigingen en de invloed van het actie-reactie mechanisme zullen ook de komende jaren beeldbepalend zijn. Voor de toekomstbestendigheid van het stelsel lijkt de flexibiliteit om snel te kunnen inspelen op (een wellicht tijdelijke) toenemende vraag naar persoonsbeveiliging of objectbewaking een belangrijke voorwaarde. Dat geldt ook voor het blijven investeren in methoden en technieken waarmee zo goed mogelijk een onderscheid kan worden gemaakt tussen ernstige en minder-ernstige bedreigingen om op die manier de beschikbare capaciteit van het stelsel optimaal te benutten.

De coronacrisis is illustratief voor een andere belangrijke conclusie, namelijk de grote invloed van onverwachte incidenten en ontwikkelingen. De Nederlandse jihadistische beweging was bijvoorbeeld tussen 2005 en 2011 getekend door inactiviteit en gebrek aan leiders. Dat veranderde haast plotsklaps toen de Syrische burgeroorlog het land veranderde tot spil in een heroplevende internationale jihad die in 2014 zou uitmonden in het kalifaat van IS. Dergelijke ontwikkelingen laten zich niet of nauwelijks voorspellen, temeer omdat ze vaak internationaal van aard zijn. Dit probleem wordt versterkt doordat nieuwe dreigingen vaak voorheen onvoorstelbare vormen aannemen, zoals de aanslag op het Koninklijk Huis met een auto in 2009, de moord op advocaat Derk Wiersum in 2019 en de recente dodelijke aanslag op journalist Peter R. de Vries. Deze tendensen zullen ook in de toekomst ervoor zorgen dat onze maatschappij verrast wordt door geweldsincidenten die we in vorm of omvang nog niet kennen. Dit is in veel opzichten onvermijdelijk en moet niet per definitie worden gezien als het falen van het stelsel.

De terroristische dreiging in Nederland is de afgelopen twee decennia voornamelijk jihadistisch van aard geweest. Het concrete risico op een aanslag, afgelezen aan het dreigingsbeeld van de NCTV, vertoont net als andere vormen van dreiging een fluctuerend patroon. Naar verwachting zal zowel het jihadisme als dit patroon voorlopig beeldbepalend blijven, hoewel de terroristische dreiging er bij uitstek één is die door plotselinge ontwikkelingen, nieuwe aanslagen of een aangepaste modus operandi wordt getypeerd. Wel lijkt er een grotere diversiteit te ontstaan qua extremistische stromingen die groepen of individuen de motivatie en rechtvaardiging voor terroristisch geweld kunnen bieden. Rechts-extremistisch terrorisme is in landen als de VS en Duitsland in opkomst en de coronacrisis heeft ook tot een toename in het complotdenken en anti-overheidsextremisme geleid. Terrorismen is meer dan altijd een grensoverschrijdend fenomeen en het verdient dan ook de aanbeveling om ontwikkelingen in andere landen op de voet te volgen om mogelijke nieuwe dreigingsvormen die ook Nederland kunnen treffen zo goed mogelijk voor te zijn.

Zowel binnen de terroristische dreiging als in het bredere palet aan dreigers neemt de eenling een bijzondere plaats in. Vanaf 2009 wordt er in Nederland in toenemende mate voor de ‘solistische dreiger’ en later ‘potentieel gewelddadige eenling’ gewaarschuwd. Ook internationaal springen eenlingen eruit, bijvoorbeeld door de aanslag van Anders Breivik in 2011 en de moord op Brits parlementslid Jo Cox in 2016. De onvoorspelbaarheid van deze brede categorie dreigers zit niet alleen in het solistische opereren, maar ook in de frequente aanwezigheid van een vorm van mentale gezondheidsproblematiek. Zeker gezien de groeiende invloed van via het internet verspreide samenzweringstheorieën, die vooral op deze groep mensen van invloed kan zijn, zal de PGE-problematiek ook in de toekomst het stelsel voor uitdagingen blijven stellen.

Een andere ontwikkeling die uit de voorgaande pagina's duidelijk naar voren komt is de groeiende rol die het internet speelt bij stelselrelevante dreigingen. In de eerste plaats doordat het een zeer laagdrempelig en relatief anoniem middel is om bedreigingen te uiten. De rol van met name sociale media wordt in dit opzicht veelvuldig aangehaald in zowel de Nederlandse als de internationale context. Op de tweede plaats, en dit is gedurende de coronacrisis nog duidelijker geworden, biedt het internet toegang tot uiteenlopende extremistische ideeën en samenzweringstheorieën alsook de digitale gemeenschappen die deze opvattingen uitdragen. Ten derde lijkt het internet vaker door vijandelijke statelijke actoren gebruikt te worden om te spioneren, saboteren en om door middel van nepnieuws het vertrouwen in democratische

instituties en processen zoals de pers en verkiezingen te ondermijnen. Met name deze laatste activiteit kan in de toekomst een toename van stelselrelevante dreigingen veroorzaken.

Het rapport roept ook op om rekening te houden met potentiële dreigingen voor instituties die van binnenuit plaatsvinden. De recente presidentsverkiezingen in de Verenigde Staten hebben laten zien dat ook eeuwenoude democratieën kwetsbaar zijn voor aantijgingen van verkiezingsfraude en ander *fake news*, zeker als die door machthebbers worden verspreid. Op kleinere schaal is er de laatste jaren in landen als Duitsland en de VS toenemende bezorgdheid over rechts-extremisme onder militairen. Gelukkig treffen beide ontwikkelingen Nederland niet direct, maar met het oog op de neiging van dreigingen om uit voorheen onvoorstelbare hoeken te komen, is waakzaamheid geboden.

Het brede perspectief dat hier gehanteerd is vestigt de aandacht op zowel directe fysieke bedreiging en intimidatie van personen als dreigingen voor het ongestoord functioneren van politici, bestuurders en de Nederlandse rechtsstaat in bredere zin. Zoals in de inleiding al werd gesteld, is de toekomstbestendigheid van het stelsel op de eerste plaats afhankelijk van een heldere afbakening. Wordt bijvoorbeeld ook het bewaken en beveiligen van *digitale* objecten en diensten hiertoe gerekend, dan staat het stelsel uiteraard qua capaciteit en middelen voor een grotere uitdaging dan wanneer de nadruk meer op het fysieke domein blijft liggen. Het scheppen van heldere kaders wat betreft de reikwijdte van het stelsel lijkt dus een belangrijke voorwaarde om überhaupt toekomstbestendig te kunnen opereren.

Op meerdere punten in dit rapport manen de auteurs tot nuance en kritische distantie. Niet om de reële dreigingen waarmee het stelsel te maken heeft te bagatelliseren, maar om met gepaste afstandelijkheid dreigingen, hun ontwikkeling qua aard en omvang en ook de meest effectieve respons in de juiste proporties te blijven zien. Verschillende publicaties wijten toenemende bedreigingen onder andere aan maatschappelijke verzuim. Net zo goed lijkt er echter een tendens vanuit burgers en overheid om ieder risico te willen uitsluiten en ieder geweldsincident of terroristische aanslag te zien als representatief voor fundamentele tekortkomingen bij aan het stelsel betrokken diensten als politie en AIVD. Totale veiligheid bestaat niet en het nastreven ervan is niet te verenigen met een open en democratische samenleving. Cru gesteld hoort het er nou eenmaal bij dat het soms misgaat. Dat is geen vrijbrief om tekortkomingen van het stelsel weg te wuiven of om betrokkenen niet ter verantwoording te roepen. Het is slechts de nuchtere gevolgtrekking uit een recente geschiedenis waarin de meest invloedrijke geweldsincidenten en dreigingsontwikkelingen zich van tevoren moeilijk lieten voorspellen.

De toekomst zal het stelsel voor legio uitdagingen plaatsen, van voortdurende ondermijning door (drugs)criminaliteit tot de invloeden van toenemende geopolitieke instabiliteit en afkalvend vertrouwen in de overheid, experts en objectieve nieuwsvergarung. Tegelijkertijd is er ook de noodzaak tot enige relativering. Ten eerste blijft het belangrijk om te benadrukken dat het in de meeste gevallen van bedreiging van personen daarbij blijft. Hoe onsmakelijk en onwenselijk dit ook is, tot daadwerkelijk geweld wordt nog altijd relatief zelden overgegaan. Ten tweede is het erg moeilijk om met het heden op het netvlies de toekomst te voorspellen; schokkende gebeurtenissen zoals de moord op Fortuyn of op advocaat Derk Wiersum zijn niet noodzakelijkerwijs tekenen van een nieuwe trend van soortgelijk geweldgebruik. Er lijkt eerder sprake te zijn van contextgebonden toenames in aantal en ernst van stelselrelevante dreigingen. De flexibiliteit om hier snel en daadkrachtig op in te kunnen spelen lijkt een belangrijke vereiste voor de toekomst van het stelsel. Maar een breed en kritisch perspectief op dreigingsontwikkelingen strekt eveneens tot de aanbevelingen om zo het stelsel op gebalanceerde en proportionele wijze waar nodig te kunnen aanpassen.

Geraadpleegde bronnen

- ‘Aangifte bedreigde politici neemt vlucht’, *Trouw* (18 juli 2008).
- Aarten, Pauline G.M., en Marieke C.A. Liem, ‘Unravelling the homicide drop: disaggregating a 25-year homicide trend in the Netherlands’, *European Journal on Criminal Policy and Research* (2021).
- AIVD, MIVD en NCTV, ‘Dreigingsbeeld statelijke actoren’, (Den Haag: AIVD, MIVD & NCTV 2021).
- Akerboom, E.S.M., ‘Tien jaar Nederlands contraterrorismebeleid’, *Militaire Spectator* 180 (2011) 387–397.
- Akhtar, Shazia, en Catriona M. Morrison, ‘The prevalence and impact of online trolling of UK members of parliament’, *Computers in Human Behavior* 99 (2019) 322–327.
- Algemene Inlichtingen- en Veiligheidsdienst, ‘Afkalvend front, blijvend beladen: extreemrechts en rechts-extremisme in Nederland’, (Den Haag: Algemene Inlichtingen- en Veiligheidsdienst 2010).
- , ‘Jaarverslag AIVD 2002’, (Den Haag: Algemene Inlichtingen- en Veiligheidsdienst 2003).
- , ‘Jaarverslag AIVD 2005’, (Den Haag: Algemene Inlichtingen- en Veiligheidsdienst 2006).
- , ‘Jaarverslag AIVD 2006’, (Den Haag: Algemene Inlichtingen- en Veiligheidsdienst 2007).
- , ‘Jaarverslag AIVD 2007’, (Den Haag: Algemene Inlichtingen- en Veiligheidsdienst 2008).
- , ‘Jaarverslag AIVD 2008’, (Den Haag: Algemene Inlichtingen- en Veiligheidsdienst 2009).
- , ‘Jaarverslag AIVD 2009’, (Den Haag: Algemene Inlichtingen- en Veiligheidsdienst 2010).
- , ‘Jaarverslag AIVD 2010’, (Den Haag: Algemene Inlichtingen- en Veiligheidsdienst 2011).
- , ‘Jaarverslag AIVD 2011’, (Den Haag: Algemene Inlichtingen- en Veiligheidsdienst 2012).
- , ‘Jaarverslag AIVD 2012’, (Den Haag: Algemene Inlichtingen- en Veiligheidsdienst 2013).
- , ‘Jaarverslag AIVD 2013’, (Den Haag: Algemene Inlichtingen- en Veiligheidsdienst 2014).
- , ‘Jaarverslag AIVD 2014’, (Den Haag: Algemene Inlichtingen- en Veiligheidsdienst 2015).
- , ‘Jaarverslag AIVD 2015’, (Den Haag: Algemene Inlichtingen- en Veiligheidsdienst 2016).
- , ‘Jaarverslag AIVD 2017’, (Den Haag: Algemene Inlichtingen- en Veiligheidsdienst 2018).
- , ‘Jaarverslag AIVD 2019’, (Den Haag: Algemene Inlichtingen- en Veiligheidsdienst 2020).
- , ‘Jaarverslag AIVD 2020’, (Den Haag: Algemene Inlichtingen- en Veiligheidsdienst 2021).
- , ‘Rechts-extremisme in Nederland: een fenomeen in beweging’, (Den Haag: Algemene Inlichtingen- en Veiligheidsdienst 2018).
- ‘Amerikaans rapport: Saoedische kroonprins zat achter moord op journalist Khashoggi’, *De Volkskrant* (26 februari 2021).
- Analistennetwerk Nationale Veiligheid, ‘Horizonscan nationale veiligheid 2020’, (Bilthoven: RIVM 2020).
- Andringa, Remco, ‘Veel meer dreigingen van criminelen: politie kan beveiliging nauwelijks nog aan’, *NOS* (23 februari 2020).
- ‘Anis Amri verbleef enkele uren in Amsterdam’, *Het Parool* (4 januari 2017).
- Aspden, Kester, ‘The making of a bedsit Nazi: who was the man who killed Jo Cox?’, *The Guardian* (6 december 2019).
- Bennhold, Katrin, Melissa Eddy en Christopher F. Schuetze, ‘Vienna reels from a rare terrorist attack’, *The New York Times* (3 november 2020).
- Bilefsky, Dan, en Maïa de la Baume, ‘Terrorists strike Charlie Hebdo newspaper in Paris, leaving 12 dead’, *The New York Times* (7 januari 2015).
- Binnenlandse Veiligheidsdienst, ‘Jaarverslag Binnenlandse Veiligheidsdienst 2000’, (Den Haag: Binnenlandse Veiligheidsdienst 2001).
- Bjørge, Tore, en Emilie Silkoset, ‘Threats and threatening approaches to politicians: A survey of Norwegian parliamentarians and cabinet ministers’, (Oslo: Politihøgskolen 2018).
- ‘Blok: Iran zat achter moorden in Nederland’, *Het Parool* (8 januari 2019).

- Borgesius, Els, e.a., 'Individuele bedreigers van publieke personen in Nederland: fenomeenanalyse en een beleidsverkenning', (Den Haag: Nationaal Coördinator Terrorismebestrijding (NCTb) 2010).
- Bos, J.G.H., A.M.D. van Es en P. Vasterman, 'Copycat: een fenomeenonderzoek', (Den Haag: COT Instituut voor Veiligheids- en Crisismanagement 2011).
- Bouma, Joop, 'Het gezicht van verzet tegen windmolens werd gearresteerd: 'Alsof ik zes moorden had gepleegd'', *Trouw* (14 augustus 2019).
- Boutellier, Hans, e.a., 'Een einde aan ondermijning', *Tijdschrift voor Veiligheid* 19 (2020) 3–16.
- Bouwmeester, Jaap, en Nora Löb, 'Monitor agressie & geweld 2018: decentraal bestuur', (Amsterdam / Enschede: I&O Research 2018).
- Bovenkerk, Frank, 'Bedreigingen in Nederland: verkenning in opdracht van Politie en Wetenschap', (Utrecht: Universiteit Utrecht 2005).
- Buruma, Ybo, 'Ondermijning en de veerkracht van de rechtsstaat', *Nederlands Juristenblad* (2019) <<https://www.njb.nl/blogs/ondermijning-en-de-veerkracht-van-de-rechtsstaat/>> [geraadpleegd 19 mei 2021].
- Chrisafis, Angelique, 'Copenhagen shooting suspect Omar el-Hussein – a past full of contradictions', *The Guardian* (16 februari 2015).
- 'Circulaire met betrekking tot de bewaking en beveiliging van personen, objecten en diensten 2019' (1 juli 2019) <<https://wetten.overheid.nl/BWBR0042437/2019-07-01>> [geraadpleegd 28 juni 2021].
- Crijns, Jan, Marieke Dubelaar en Kelly Pitcher, 'Overgeleverd aan de wolven? De toekomst van de kroongetuige in het Nederlandse strafproces', *Nederlands Juristenblad* (2018) 1564–1571.
- De Goede, Marieke, 'Beyond risk: premediation and the post-9/11 security imagination', *Security Dialogue* 39 (2008) 155–176.
- De Jager, Nick, 'Geweld en middelvingers nopen NOS logo te verwijderen van straalwagens', *De Volkskrant* (15 oktober 2020).
- De Wijk, Rob, 'Het stelsel bewaken en beveiligen na Pim Fortuyn', (Den Haag: The Hague Centre for Strategic Studies 2012).
- Den Hartog, Tobias, 'Hoe moeten we het onkruid wieden?', *Algemeen Dagblad* (8 juli 2021).
- Den Hond, Bas, 'Republikeinen dulden geen enkele kritiek meer op Trump', *Trouw* (12 mei 2021).
- 'Dossier Derk Wiersum', *Advocatenblad* (2021) <<https://www.advocatenblad.nl/dossiers/derk-wiersum/>> [geraadpleegd 19 mei 2021].
- Du Pré, Raoul, 'Oververhit coronadebat raakt ook het OMT: wetenschappers worden ernstig bedreigd', *De Volkskrant* (4 december 2020).
- 'EU en VS veroordelen "ongekende kaping vliegtuig door Wit-Rusland"', *NOS* (23 mei 2021) <<https://nos.nl/artikel/2382051-eu-en-vs-veroordelen-ongekende-kaping-vliegtuig-door-wit-rusland>> [geraadpleegd 26 mei 2021].
- Every-Palmer, Susanna, Justin Barry-Walsh en Michele Pathé, 'Harassment, stalking, threats and attacks targeting New Zealand politicians: A mental health issue', *Australian & New Zealand Journal of Psychiatry* 49 (2015) 634–641.
- Fijnaut, C.J.C.F., 'Naar aanleiding van de moord op advocaat D. Wiersum: de seinen staan al jaren op rood' 17, *Strafblad* (2019) 14–16.
- 'Forse stijging bedreigde politici', *RTL Nieuws* (2014) <<https://www.rtlnieuws.nl/node/1558891>> [geraadpleegd 26 mei 2021].
- Freedman, Lawrence, *The future of war: a history* (Londen: Allen Lane 2017).
- Gray, Colin S., *The future of strategy* (Cambridge / Malden: Polity 2015).

- Hagemann, Florian, 'Mordfall Lübcke: Das Leben des Stephan Ernst', *HNA.de* (2020) <<https://www.hna.de/kassel/luebcke-prozess-mord-leben-stephan-ernst-straftaten-kassel-90091938.html>> [geraadpleegd 17 februari 2021].
- Haschnik, Gregor, 'Hanau: Rassistischer Attentäter wollte noch mehr Menschen töten – Neue Details enthüllt', *Frankfurter Rundschau* (12 februari 2021).
- Home Office, 'Report of the official account of the bombings in London on 7th July 2005', (Londen: The Stationary Office 2006).
- 'Iets meer politici bedreigd in 2010', *Trouw* (22 maart 2011).
- Inspectie Justitie en Veiligheid, 'Inspectieonderzoek naar de aanpak van de stalking door Bekir E.', (Den Haag: Ministerie van Justitie en Veiligheid 2019).
- Inspectie Openbare Orde en Veiligheid, 'Koninginnedag 2009 Apeldoorn: Een onderzoek door de Inspectie Openbare Orde en Veiligheid', (Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2009).
- James, D. V., e.a., 'The role of mental disorder in attacks on European politicians 1990–2004', *Acta Psychiatrica Scandinavica* 116 (2007) 334–344.
- James, D. V., e.a., 'Aggressive/intrusive behaviours, harassment and stalking of members of the United Kingdom parliament: a prevalence study and cross-national comparison', *The Journal of Forensic Psychiatry & Psychology* 27 (2016) 177–197.
- Klein Kranenburg, Laurens, e.a., 'Bedreigingen en intimidaties van burgemeesters in relatie tot de bestuurlijke aanpak', (Enschede: I&O Research 2020).
- , 'Monitor Integriteit en Veiligheid 2020', (Amsterdam: I&O Research 2020).
- Koehler, Daniel, 'A threat from within? Exploring the link between the extreme right and the military', (Den Haag: International Centre for Counter-Terrorism 2019).
- Koops, Ruben, 'Aanslagpleger CS Jawed S. veroordeeld tot bijna 27 jaar cel', *Het Parool* (14 oktober 2019).
- Korsten, Wilrieke, Romy Hendrix en Davien van der Sloot, 'Strategisch omgevingsbeeld 2020', (Den Haag: Ministerie van Justitie en Veiligheid 2021).
- Kortleven, Willem-Jan, 'Een boekje open over ondermijning', *Tijdschrift voor Veiligheid* 19 (2020) 69–82.
- Kouwenhoven, Andreas, 'Docent duikt onder om cartoon in klas', *NRC Handelsblad* (5 november 2020).
- Kuin, Frank, 'Opgestookt door leugens en oorlogsretoriek: bestorming Capitool was allesbehalve spontaan', *NRC Handelsblad* (5 februari 2021).
- Kuiper, Margaret, *Het woord en de daad: kenmerken van dreigbrieven en de intenties waarmee ze geschreven worden* (Proefschrift Universiteit Leiden, Leiden 2018).
- Lauriks, Mark, en Wilrieke Korsten, 'Strategisch omgevingsbeeld 01: 2019/2020', (Den Haag: Ministerie van Justitie en Veiligheid 2019).
- Liem, Marieke en Katharina Krüsselmann, 'Explosief geweld', *Het Tijdschrift voor de Politie* (16 september 2019).
- Lüdke, Steffen en Alexandra Rojkov, 'Fears mount following attack on Dutch journalist', *Spiegel International* (9 juli 2021).
- Macklin, Graham, 'The Christchurch attacks: livestream terror in the viral video age', *CTC Sentinel* 12 (2019) 18–29.
- Masschelin, José, 'Terroristen in Brussel en Parijs in zelfde netwerk', *Algemeen Dagblad* (24 maart 2016).
- Medewerker ICCT, 'Bijdrage aan de expertsessie stelsel bewaken & beveiligen' (9 juni 2021).
- Medewerker Ministerie van Binnenlandse Zaken, 'Bijdrage aan de expertsessie stelsel bewaken & beveiligen' (9 juni 2021).
- Medewerker NCTV 1, 'Bijdrage aan de expertsessie stelsel bewaken & beveiligen' (9 juni 2021).

Medewerker NCTV 2, 'Bijdrage aan de expertsessie stelsel bewaken & beveiligen' (9 juni 2021).

Medewerker Politie 1, 'Bijdrage aan de expertsessie stelsel bewaken & beveiligen' (9 juni 2021).

Medewerker Politie 2, 'Bijdrage aan de expertsessie stelsel bewaken & beveiligen' (9 juni 2021).

Medewerker Politie 3, 'Bijdrage aan de expertsessie stelsel bewaken & beveiligen' (9 juni 2021).

'Minder politici bedreigd in 2011', *Het Parool* (20 maart 2012).

'Minder strafbare bedreigingen tegen politici', *Openbaar Ministerie* (2017) <<https://www.om.nl/onderwerpen/bedreigde-politici/nieuws/2017/03/20/minder-strafbare-bedeigingen-tegen-politici>> [geraadpleegd 26 mei 2021].

'Minister en Kamerlid worden vaker bedreigd', *Het Parool* (18 juli 2008).

Minister van Justitie en Veiligheid, 'Regeling van de Minister van Justitie en Veiligheid van 3 mei 2021, nr. 3291895, houdende instelling van het adviescollege toekomstbestendig stelsel bewaken en beveiligen', *Staatscourant van het Koninkrijk der Nederlanden* 25135 (20 mei 2021).

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 'Bedreigd bestuur 2010: Agressie en geweld tegen politieke ambtsdragers bij gemeenten, provincies en waterschappen', (Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2010).

Nationaal Coördinator Terrorismebestrijding en Veiligheid, 'Bewaken en beveiligen', *nctv.nl* (onbekend) <<https://www.nctv.nl/onderwerpen/bewaken-en-beveiligen>> [geraadpleegd 18 mei 2021].

---, 'Cybersecuritybeeld Nederland: CSBN 2021', (Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid 2021).

---, 'Dreigingsbeeld Terrorisme Nederland', *nctv.nl* (2019) <<https://www.nctv.nl/onderwerpen/dtn>> [geraadpleegd 27 mei 2021].

---, 'Nationale veiligheid strategie 2019', (Den Haag: Ministerie van Justitie en Veiligheid 7 juni 2019) <<https://www.nctv.nl/actueel/nieuws/2019/06/07/nationale-veiligheid-strategie-2019-gepubliceerd>> [geraadpleegd 19 mei 2021].

---, 'Onderzoek functioneren Stelsel Bewaken en Beveiligen Koninginnedag 2009', (Den Haag: Nationaal Coördinator Terrorismebestrijding (NCTb) 2009).

Nederlandse Politiebond, 'Noodkreet recherche: waar blijft onze versterking?', (Baarn: Nederlandse Politiebond 2018).

'Nederlands trollenleger verspreidt en coördineert desinformatie over vaccin', *Pointer* (NPO2 20 mei 2021) <<https://pointer.kro-ncrv.nl/nederlands-trollenleger-verspreidt-en-coördineert-desinformatie-over-vaccin>> [geraadpleegd 20 mei 2021].

Nesser, Petter, *Islamist terrorism in Europe: a history* (Londen: Hurst 2015).

Nieber, Lineke en Karel Smouter, 'Ombudsman Smit (NPO): "Ik kan niet met een kanon naar Hilversum"', *NRC Handelsblad* (28 juni 2021).

Odekerken, M.W.A., en A.F.M. Brenninkmeijer, 'Een dreigend klimaat: verslag van het onderzoek "Bedreigingen van Nederlandse journalisten"', (Utrecht: Nederlandse Vereniging van Journalisten 2017).

---, en L.A. Das, 'Een onveilig klimaat: onderzoek bedreigingen van vrouwelijke journalisten', (Utrecht: Nederlandse Vereniging van Journalisten 2019).

'Ook in Nederland vinden rechts-extremisten het leger aantrekkelijk', *NOS* (19 mei 2021) <https://amp.nos.nl/artikel/2381456-ook-in-nederland-vinden-rechts-extremisten-het-leger-aantrekkelijk.html?__twitter_impression=true> [geraadpleegd 19 mei 2021].

Oostveen, Margriet, 'Regionale verslaggevers worden vaak bedreigd en weinig beschermd', *De Volkskrant* (18 maart 2019).

- Openbaar Ministerie, Politie Nederland en NCTV, 'Factsheet: stelsel bewaken en beveiligen', (2016)
 <<https://www.burgemeesters.nl/sites/www.burgemeesters.nl/files/File/factsheet-stelsel-bewaken-en-beveiligen-07-03-2016.pdf>> [geraadpleegd 18 mei 2021].
- Opstelten, I.W., Kamerstuk 29754 terrorismebestrijding, nr 233: brief van de Minister van Veiligheid en Justitie (2013).
- Ouhajji, Majda, en Vera Boonman, 'Wapens gevonden bij Oostenrijkse coronategenstanders', *NRC Handelsblad* (20 mei 2021).
- Pathé, Michele, 'Stalking public figures', in: Wayne Petherick en Grant Sinnamon (red.), *The psychology of criminal and antisocial behavior* (Elsevier 2017) 295–320.
- Pathé, Michele T., e.a., 'Public figure fixation: cautionary findings for mental health practitioners: public figure fixation: cautionary findings', *Behavioral Sciences & the Law* 34 (2016) 681–692.
- Piazza, James A., 'Fake news: the effects of social media disinformation on domestic terrorism', *Dynamics of Asymmetric Conflict* (2021).
- 'Politici 424 keer bedreigd', *Het Parool* (12 maart 2009).
- 'Politici steeds vaker ernstig bedreigd', *Brabants Dagblad* (23 maart 2011).
- 'Politici vaker en ernstiger bedreigd, zelfs door kinderen onder de 12 jaar', *RTL Nieuws* (2020)
 <<https://www.rtlnieuws.nl/nieuws/politiek/artikel/5196792/politici-vaker-en-ernstiger-bedreigd-daders-woorden-ook-steeds>> [geraadpleegd 26 mei 2021].
- 'Politici vorig jaar 113 keer bedreigd', *NOS* (28 maart 2013) <<https://nos.nl/artikel/489563-politici-vorig-jaar-113-keer-bedreigd>> [geraadpleegd 26 mei 2021].
- 'Politici werden 121 keer bedreigd', *Het Parool* (29 maart 2006).
- 'Politie over explosief bij teststraat Bovenkarspel: 'Zelf gefabriceerd voorwerp'', *Algemeen Dagblad* (3 maart 2021).
- Prins, Ruth, 'De bestuurlijke aanpak van georganiseerde criminaliteit in Nederland: Hoe het lokale bestuur een partner werd in de gezamenlijke strijd tegen georganiseerde criminaliteit', *Cahiers Politiestudies* (2016) 151–165.
- Radicalisation Awareness Network, 'Radicalised police, military and prison staff', Conclusions Paper (Brussel: Europese Commissie 2021).
- Rafael, Simone, 'Nach dem Attentat von Halle: die Boards der Rechtsterroristischen Attentäter als Internationale Kadenschmiede', *Belltower* (18 oktober 2019)
 <<https://www.belltower.news/nach-dem-attentat-von-halle-die-boards-der-rechtsterroristischen-attentaeter-als-internationale-kaderschmiede-92103/>> [geraadpleegd 9 september 2020].
- Rechtbank Den Haag, NL:RBDHA:2019:7308 (2019).
- Rechtbank Midden-Nederland, NL:RBMNE:2015:4919 (2015).
- , NL:RBMNE:2020:1046 (2020).
- Renout, Frank, 'Fransen massaal de straat op uit woede om moord op leraar', *Algemeen Dagblad* (19 oktober 2020).
- Riess, Paulina, Luisa Gonzalez en Panagiota Korenis, 'Management of patients who make threats against elected officials: a case report', *Frontiers in Psychiatry* 9 (2018) 1-3.
- Royal Commission of Inquiry into the terrorist attacks on Christchurch mosques on 15 March 2019, 'Ko tō tātou kāinga tēnei: report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019 - Volume 1: parts 1-3', (Royal Commission 2020) 1–161.
- Rubin, Alissa J., 'Paris: one year on', *The New York Times* (12 november 2016).
- 'Ruim tweehonderd strafbare bedreigingen tegen politici in 2019', *Openbaar Ministerie* (2020)
 <<https://www.om.nl/onderwerpen/bedreigde-politici/nieuws/2020/10/27/ruim>-

- tweehonderd-straftbare-bedreigingen-tegen-politici-in-2019> [geraadpleegd 26 mei 2021].
- Rutten, Eric Reijnen, ‘Kamervoorzitter vindt huisbezoek boeren aan Jetten onacceptabel: ‘Dan ga je een grens over’’, *Algemeen Dagblad* (28 oktober 2020).
- Schenkkan, Nate, en Isabel Linzer, ‘Out of sight, not out of reach: the global scale and scope of transnational repression’, (Washington, D.C: Freedom House 2021).
- Schildkamp, Victor en Yelle Tieleman, ‘Moordaanslag op Peter R. de Vries’, *De Gelderlander* (7 juli 2021).
- Schoonhoven, Silvan, ‘Doorslaan in achterdocht; Nederland kent poldervariant van QAnon’, *De Telegraaf* (9 januari 2021).
- Schuurman, Bart, *Becoming a European homegrown jihadist: a multilevel analysis of involvement in the Dutch Hofstadgroup, 2002-2005* (Amsterdam: Amsterdam University Press 2018).
- , ‘Topics in terrorism research: reviewing trends and gaps, 2007-2016’, *Critical Studies on Terrorism* 12 (2019) 463–480.
- Snijders, Tim Igor, ‘‘Het zit na jaren nog tussen de oren’’, *De Volkskrant* (13 oktober 2018).
- ‘Stijging strafbare bedreigingen tegen politici’, *Openbaar Ministerie* (2019) <<https://www.om.nl/onderwerpen/bedreigde-politici/nieuws/2019/06/19/stijging-straftbare-bedreigingen-tegen-politici>> [geraadpleegd 26 mei 2021].
- Stoker, Elsbeth, ‘Een jaar na de moord op Derk Wiersum: ‘Nog steeds kijken advocaten vaker over hun schouder’’, *De Volkskrant* (18 september 2020).
- ‘Team Bedreigde Politici verrast met Team Award WEP’, *Politie.nl* (4 februari 2020) <<https://www.politie.nl/nieuws/2020/februari/4/06-team-bedreigde-politici-verrast-met-team-award-wep.html>> [geraadpleegd 26 mei 2021].
- Thomas, Casper, en Yvonne Zonderop, ‘Journalistiek moet zelf vertrouwen herstellen’, *NRC Handelsblad* (8 december 2020).
- Tieleman, Yelle, ‘OM eist tot 7 jaar celstraf voor aanslag Panorama’, *Algemeen Dagblad* (20 mei 2019).
- , ‘Rechtbank legt 20 jaar cel op aan moordenaar broer kroongetuige Nabil B.’, *Algemeen Dagblad* (10 januari 2019).
- , ‘Spoor liquidatie advocaat Derk Wiersum leidt naar Utrecht’, *Het Parool* (21 oktober 2020).
- Tops, Pieter, en Henny Schilders, ‘Naar een meervoudige aanpak van ondermijning’ 78, *Tijdschrift voor de Politie* (2016) 12–15.
- ‘Twaalf verdachten opgepakt in verband met de aanslag op het Telegraaf-gebouw’, *Trouw* (8 april 2019).
- Van Buuren, Jelle, ‘De nieuwe complotecologie’, *De Groene Amsterdammer* (26 april 2020).
- , *Doelwit Den Haag? Complotconstructies en systeemhaat in Nederland 2000-2014* (Proefschrift Universiteit Leiden, Den Haag 2016).
- Van den Haak, H.F., e.a., *De veiligheid en de beveiliging van Pim Fortuyn: feiten en verantwoordelijkheden* (Den Haag: Sdu Uitgevers 2002).
- Van den Heuvel, John en Mick van Wely, ‘Gouden eeuw voor Amsterdamse drugspenoze’, *De Telegraaf* (28 augustus 2019).
- Van den Tillaart, Joost, e.a., ‘Monitor agressie en geweld openbaar bestuur: meting 2012’, (Amsterdam: Regioplan 2012).
- Van der Torre, E.J., M. Gieling en M.Y. Bruinsma, ‘Bedreigen en intimideren van OM- en politiemedewerkers: een onderzoek naar frequentie, aard, gevolgen en aanpak’, (Den Haag: Wetenschappelijk Onderzoek- en Documentatiecentrum 2013).
- Van Gestel, B., en M.A. Verhoeven, ‘Liquidaties nieuwe stijl: verruwing en professionalisering bij liquidaties in Nederland’, *Justitiële verkenningen* 43 (2017) 9–28.

- Van Haenen, Marcel, 'Facebook-dreiger vindt zichzelf nu een ezel', *NRC Handelsblad* (29 april 2016).
- Van Ham, Tom, en Anton Van Wijk, 'Bescherming van personen: ontwikkelingen in de dreiging vanuit de georganiseerde criminaliteit', (Arnhem: Bureau Beke 2018).
- Van Hoof, Wera, e.a., 'Onderzoek psychosociale effecten van bedreiging en beveiliging', (Diemen: ARQ Nationaal Psychotrauma Centrum 2020).
- Van Soest, Hans, Edwin Van der Aa en Carla Van der Wal, 'Bedreigingen en fysieke aanvallen: verschillende politici mikpunt van agressie', *Algemeen Dagblad* (9 september 2020).
- Veilleux-Lepage, Yannick, 'How and why vehicle ramming became the attack of choice for terrorists', *The Conversation* (29 maart 2017) <<https://theconversation.com/how-and-why-vehicle-ramming-became-the-attack-of-choice-for-terrorists-75236>> [geraadpleegd 25 mei 2021].
- , 'The radical right's legitimisation of vehicle ramming', in: William Allchorn (red.), *Tracking the rise of the radical right globally* (Stuttgart: Ibidem Verlag 2019) 305–308.
- 'Verdachte vast voor plan aanslag op vaccinatielocatie Den Helder', *Het Parool* (8 april 2021).
- Vermaas, Pieter, 'Het werk van de BBC'ers van het OM', *Opportuun* (december 2020).
- 'Voortvluchtige Belgische militair kon door 'grote fouten' aan wapens komen', *NOS* (25 mei 2021) <<https://nos.nl/artikel/2382235-voortvluchtige-belgische-militair-kon-door-grote-fouten-aan-wapens-komen>> [geraadpleegd 26 mei 2021].
- Vugts, Paul, 'Een reconstructie van de aanslag op Derk Wiersum: niemand zag het onheil naderen', *Het Parool* (12 september 2020).
- , 'In Almere geliquideerde 'Ali' achter beruchtste aanslag Iran', *Het Parool* (mei 2018).
- Winter, Heinrich, e.a., 'Criminele beïnvloeding van het lokale openbaar bestuur' (Groningen: Pro Facto / Rijksuniversiteit Groningen 2017).
- Zraick, Karen, en Julia Jacobs, 'Charlottesville attacker pleads guilty to federal hate crime charges', *The New York Times* (27 maart 2019).

