December 2022

Strategische Onderzoeksagenda Bewaken en Beveiligen 2023-2027

De Strategische Onderzoeksagenda Bewaken en Beveiligen is opgesteld door de Universiteit Leiden in opdracht van het Kenniscentrum Bewaken en Beveiligen.

Edwin Bakker, Jelle van Buuren, Bart Schuurman

Universiteit Leiden

Strategische Onderzoeksagenda Bewaken en Beveiligen 2023-2027

Dit is de Strategische Onderzoeksagenda Bewaken en Beveiligen voor de periode 2023-2027. Deze agenda bevat de strategische thema's voor toegepast wetenschappelijk onderzoek voor het stelsel bewaken en beveiligen, de stelselpartners (Nationale Politie, Openbaar Ministerie, Koninklijke Marechaussee, Nationaal Coördinator Terrorismebestrijding en Veiligheid) en andere aan het stelsel verbonden organisaties in de veiligheidsketen. Op basis van de in deze agenda genoemde thema's wordt elk jaar een onderzoeksprogramma opgesteld rond specifieke onderzoeksonderwerpen die door de Universiteit Leiden en andere kennisinstellingen zullen worden onderzocht.

1 Inleiding

Wetenschappelijke schil

In oktober 2021 publiceerde een door de regering ingestelde adviescommissie een rapport met aanbevelingen om het stelsel bewaken en beveiligen toekomstbestendig te maken. Eén van de adviezen van deze Commissie Bos betreft het toevoegen van een zogeheten 'wetenschappelijke schil' aan het bestaande 'Kenniscentrum bewaken en beveiligen'.[1] Het doel van deze uitbreiding is om de vier stelselpartners en de ketenpartners rond het stelsel van wetenschappelijke inzichten en expertise te kunnen voorzien. Zo kan het beleid en de uitvoering op dit belangrijke maatschappelijke onderwerp gebaseerd worden op gevalideerde kennis en inzichten. Centraal staat het uitvoeren van stelselrelevant toegepast wetenschappelijk onderzoek en het inzetten van onderzoeksresultaten van de wetenschappelijke schil in trainingen en onderwijsprogramma's.[2]

In juni 2022 werd door het Kenniscentrum Bewaken en Beveiligen een meerjarig onderzoeksproject toegekend aan de Universiteit Leiden om op zowel onderzoek als training nieuwe activiteiten te ontwikkelen. De verantwoordelijkheid hiervoor ligt bij de projectgroep Bewaken en Beveiligen van het Institute of Security and Global Affairs (ISGA) van de Universiteit Leiden. Het onderzoeksproject bestaat uit kortlopend, praktijkgericht onderzoek en langere-termijn fundamenteel promotieonderzoek en behelst op onderwijsvlak onder andere ook een bijdrage aan trainingsmodules van het Centre for Professional Learning (CPL) van dezelfde universiteit. Voor de uitvoering van onderzoeken waar de projectgroep van de

[1] Bos et al., 'Adviescommissie toekomstbestendig stelsel bewaken en beveiligen' (Ministerie van Justitie en Veiligheid, oktober 2021), p. 9, 45.

[2] Om dit te realiseren wordt o.a. nadrukkelijk samengewerkt met het *Centre for Professional Learning* (CPL) van de Universiteit Leiden. Het CPL heeft vanuit het Kenniscentrum de opdracht gekregen een leergang te ontwikkelen met als doel de samenwerking te verbeteren tussen de bij het Kenniscentrum betrokken partners. De leergang richt zich op het bevorderen van een gezamenlijk stelselperspectief en kennisproductie en kennisoverdracht op relevante inhoudelijke thema's.

Universiteit Leiden niet zelf de nodige expertise of capaciteit in huis heeft, wordt via een jaarlijkse *call* een beroep gedaan op de expertise van andere universiteiten en kennisinstellingen. Deze constructie maakt het mogelijk om het stelsel een zeer breed scala aan kennis en inzichten ter beschikking te stellen.

Doelen

De Strategische Onderzoeksagenda Bewaken en Beveiligen is ontstaan uit een initiatief van de Universiteit Leiden als onderdeel van het opzetten van de wetenschappelijke schil rond het stelsel bewaken en beveiligen. Deze agenda beoogt samenhang en focus aan te brengen in het onderzoek van de wetenschappelijke schil en biedt een leidraad voor het prioriteren van de meest relevante onderzoeksonderwerpen van de vier stelselpartners. Deze prioritering is daarmee niet voor de looptijd van het project onwrikbaar vastgesteld; het is de bedoeling om in ieder geval jaarlijks te toetsen of de kennisbehoeften zoals hieronder gepresenteerd nog actueel zijn en of er redenen zijn om de prioritering van onderzoeksonderwerpen te veranderen.

De onderzoeksagenda is nadrukkelijk ook bedoeld om samenwerking tussen de onderzoekswereld en beleidsmakers en uitvoerders te stimuleren en het samen opbouwen van kennis ten behoeve van het stelsel bewaken en beveiligen mogelijk te maken. Daarnaast biedt de onderzoeksagenda aanknopingspunten om rond specifieke thema's netwerken en samenwerkingsverbanden te creëren tussen onderzoekers uit het bredere Nederlandse kennislandschap en de stelselpartners.

De agenda heeft voor de onderzoekswereld tevens een stimulerende, faciliterende en sturende functie. Door middelen ter beschikking te stellen voor (promotie)onderzoek op het brede terrein van bewaken en beveiligen worden onderzoekers uit verschillende disciplines gestimuleerd een bijdrage te leveren en wetenschappelijk verdieping aan te brengen rond vraagstukken die leven binnen het stelsel. Daarnaast heeft de agenda een sturende functie die ongewenste doublures van onderzoek kan helpen voorkomen[3] en tevens overbelasting voorkomt van uitvoerende organisaties die keer op keer om data of om medewerking worden gevraagd.

Doorwerking van het onderzoek is een ander belangrijk doel van de agenda. Dit kan worden bevorderd door vroegtijdig contact te leggen tussen onderzoekers, beleidsmakers en de beroepspraktijk. Tevens kan dit worden bevorderd door specifiek na te denken over de op te leveren (tussen)producten en in welke vorm de resultaten zo effectief mogelijk aan eindgebruikers kunnen worden aangeboden. Zo zijn er bij de opzet, de uitvoering en de presentatie van onderzoek mogelijkheden om beleidsmakers en uitvoerders te betrekken en op die manier de kans te vergroten dat van het onderzoek geleerd kan worden en resultaten

[3] Daartoe zal ook gekeken worden naar onderzoek dat wordt uitgevoerd in het kader van andere onderzoeksagenda 's en –programma's. Denk aan de Strategische Onderzoeksagenda van de Politie, de samenwerking tussen de NP en TNO op onderzoeksgebied, en onderzoek verricht door en voor Defensie.

daadwerkelijk de werkvloer bereiken.[4] Hierbij zal gebruik worden gemaakt van de ervaringen die bij de Nationale Politie en de Politieacademie op dit vlak zijn opgedaan.

Het uiteindelijke doel van de investeringen in de wetenschappelijke schil en de strategische onderzoeksagenda is het genereren van nieuwe inzichten en kennis die kunnen helpen om het beleid en de praktijk van bewaken en beveiligen verder te versterken en verbeteren. De uitkomsten van onderzoek kunnen tevens gebruikt worden voor professionele trainingen en opleidingen.

2 Proces vaststellen onderzoeksthema's

Aansluiting bij bestaande voorstellen en ontwikkelingen

Wat betreft onderzoeksthema's en prioriteiten sluit de onderzoeksagenda voor een deel aan bij de voorstellen van de Commissie Bos om het stelsel bewaken en beveiligen toekomstbestendig te maken en de Kamerbrief van april 2022[5] waarin een aantal hoofdthema's van onderzoek genoemd worden genoemd.[6]

Daarnaast kwam uit een uitgebreide inventarisering van kennisbehoeften en onderzoeksprioriteiten naar voren dat er onder de stelselpartners belangstelling is voor nieuwe en verwachte maatschappelijke en technologische ontwikkelingen op het gebied van bewaken en beveiligen.

Gelet op de breedte van het domein bewaken en beveiligen en de diversiteit aan relevante ontwikkelingen, wordt een beroep gedaan op een groot aantal wetenschappelijke disciplines en meerdere wetenschappelijke onderzoeksinstellingen. Relevante wetenschappelijke disciplines zijn bijvoorbeeld veiligheidskunde, bestuurskunde, sociologie, rechtswetenschap en criminologie, maar ook psychologie, ethiek, informatietechnologie, kunstmatige intelligentie en andere technologische disciplines. Dit maakt de betrokkenheid van meerdere wetenschappelijke kennisinstellingen noodzakelijk en verklaart de breedte van de strategische onderzoeksagenda.

[4] Denk bijvoorbeeld aan een rol bij het begeleiden van onderzoek, het inzetten van medewerkers uit de praktijk bij de dataverzameling en bij de analyse van de gegevens.

[5] Yeşilgöz-Zegerius, 'Kamerbrief over voortgang versterking stelsel bewaken en beveiligen', (Ministerie van Justitie en Veiligheid, 14 april 2022).

[6] De in de Kamerbrief genoemde thema's zijn: preventie van bedreigingen binnen het lokale domein; politiek-bestuurlijke aspecten rond bewaken en beveiligen; impact van bewaken en beveiligen op de te beveiligen personen of organisatie; organisatiestructuur en verantwoordelijkheidsverdeling; invulling van de zorgplicht; wijze waarop dreigingsinschattingen worden gemaakt; ervaringen met publiek-private samenwerking; psychosociale (na)zorg voor een te beveiligen persoon en diens naasten. Daarnaast wordt het belang van internationaal vergelijkend onderzoek genoemd.

Specifieke onderzoeksonderwerpen en prioriteiten

Bij het bepalen van de belangrijkste hoofdthema's is, zoals gezegd, aangesloten bij bestaande voorstellen en ontwikkelingen. Deze hoofdthema's vormden het vertrekpunt bij het ophalen van specifieke onderzoeksonderwerpen en prioriteiten rond het stelsel bewaken en beveiligen. Deze werden opgehaald bij de vier partners van het stelsel bewaken en beveiligen - de Nationale Politie, de Koninklijke Marechaussee, het Openbaar Ministerie, de Nationaal Coördinator Terrorismebestrijding en Veiligheid – en een aantal relevante ketenpartners - Dienst Justitiële Inrichtingen, de Politieacademie en het Ministerie van Justitie en Veiligheid. Met name experts op operationeel, tactisch en strategisch niveau werden geconsulteerd. Op deze wijze is gepoogd zowel diepte als breedte in de agenda te verankeren, maximaal aan te sluiten bij de verschillende behoeftes en draagvlak te creëren voor de Strategische Onderzoeksagenda. Ook de resultaten van een workshop van het Centre for Professional Learning van de Universiteit Leiden over de kennis- en trainingsbehoefte van de stelselpartners zijn meegenomen.

Daarnaast werd een *quick scan* gemaakt van bestaande voor het stelsel relevante wetenschappelijke onderzoeken en andere studies en rapporten met betrekking tot bewaken en beveiligen en aanverwante gebieden. Bekeken werd welke onderzoeken de afgelopen jaren zijn verricht, welke kennis en inzichten deze hebben opgeleverd en welke vervolgvragen ze opwierpen. Hoofdconclusie was overigens dat er weinig wetenschappelijk onderzoek naar het stelsel is verricht en dat er slechts op een beperkt aantal deelonderwerpen relevante studies zijn. Tevens viel op dat er amper wetenschappelijke overzichtsstudies en achtergrondstudies zijn over kernelementen van (het stelsel) bewaken en beveiligen. Dit leverde het inzicht op om de komende jaren verder te kijken dan alleen naar bewaken en beveiligen per se of het hier en nu, door vergelijkingsonderzoek te doen naar beleid op andere veiligheidsterreinen of aanpalende vraagstukken, zoals getuigenbescherming, stalking en radicalisering en terrorisme. Daarnaast kan internationaal vergelijkend onderzoek helpen de Nederlandse context en het beleid in perspectief te zien en te leren van ervaringen elders.

Ten slotte werd gekeken naar de mogelijkheden en beperkingen van wetenschappelijk onderzoek in een veiligheidsdomein dat gekenmerkt wordt door geheimhouding, afscherming, (juridische) beperkingen met betrekking tot het delen van informatie, privacy issues, ethische issues, et cetera. Dit betekent dat bepaald onderzoek niet mogelijk is, denk aan onderzoek naar aspecten van het werk van inlichtingen- en veiligheidsdiensten of bepaald type onderzoek naar te beveiligen personen.

Op basis van de aldus opgestelde strategische onderzoeksagenda zal de Universiteit Leiden, in overleg met het Kenniscentrum Bewaken en Beveiligen, jaarlijks het onderzoeksprogramma van de eigen projectgroep en de jaarlijkse *call* voor uit te besteden onderzoek bepalen.

De acht hoofdthema's

Het hierboven geschreven proces heeft de volgende acht hoofdthema's opgeleverd.

1. Dreiging en daders
2. Impact op personen, organisaties en maatschappij
3. Organisatie van het stelsel en politiek-bestuurlijke context
4. Informatie, intelligence en inschattingen
5. Opschalen en afschalen van maatregelen
6. Publiek-private samenwerking
7. Vakmanschap
8. Technologie, wetenschap en innovatie

3 Hoofdthema's en onderzoeksonderwerpen

Zoals gezegd sluit de onderzoeksagenda wat betreft onderzoeksthema's en prioriteiten aan bij de bevindingen van de Commissie Bos en de Kamerbrief van april 2022. Aan de daarin genoemde onderzoeksthema's werden op basis van de consultaties met vertegenwoordigers van partners en stakeholders van het stelsel bewaken en beveiligen specifieke onderzoeksonderwerpen en de hoofdthema's 'vakmanschap' en 'technologie, wetenschap en innovatie' toegevoegd. Per thema volgt een korte omschrijving en worden een aantal mogelijke onderzoeksonderwerpen benoemd voor 2023 en de komende jaren.

1. Dreiging en daders

Achtergronden en kenmerken

Nederland heeft de afgelopen decennia te maken gehad met zeer uiteenlopende dreigingen jegens en aanslagen op personen en objecten. De dreiging is zeer divers. Deze komt, onder meer, uit de hoek van buitenlandse statelijke actoren, extremistische organisaties en georganiseerde criminaliteit, uit relationele kring en van verwarde personen. Sommige bedreigingen leiden niet tot actie en sommige gewelddadige handelingen komen schijnbaar uit het niets. Inzicht in de achtergronden en kenmerken van de dreiging en van individuele daders kan helpen bij het verbeteren van de dreigingsinschatting en preventief beleid. *What makes them tick* is een belangrijke vraag als het gaat om individuen. En wat zijn de kenmerken en beweegredenen van groeperingen? Wie bedreigen politici en wat kunnen we leren van databestanden van aangiften en open bronnen. En is de dreiging in Nederland van dit moment fundamenteel anders dan in het verleden of vergeleken met die in het buitenland?

Doelwitten en modus operandi

De dreiging manifesteert zich in een breed scala aan gewelddadige acties: van dreigbrieven en brandbommen tot aanslagen met granaatwerpers en liquidaties. Voor een deel gaat het om de modus operandi die al tientallen jaren bekend zijn, maar worden er ook nieuwe methoden, technologieën en wapens gehanteerd? Voor een deel zijn ook de doelwitten dezelfde als een decennium geleden, maar zien we ook nieuwe type doelwitten of dat bepaalde beroepsgroepen of type personen nu meer bedreigd worden dan vroeger, denk aan kroongetuigen en advocaten? Wat zijn mogelijke verklaringen hiervoor? Wie of welke beroepsgroep of functionaris trekt (meer of minder) dreiging aan en waarom? Welke dreigementen zijn meer serieus te nemen dan andere? En welke factoren verklaren de groei van online bedreigingen en intimidaties? Ook op dit terrein kan een vergelijking met het buitenland waardevol zijn. Ten slotte blijkt onderzoek naar de effecten van afschrikking van daders en de effectiviteit van *target hardening* relevant in het kader van preventie.

2. Impact op personen, organisaties en maatschappij

Beperken van de impact

Beveiligingsmaatregelen hebben altijd een impact op personen en hun omgeving. Bij het uitvoeren van deze maatregelen wordt gepoogd die impact zo klein mogelijk te laten zijn en de te beveiligen personen (TBP) zo veel mogelijk ongestoord hun leven en hun werk voort te laten zetten. Is een dergelijke ambitie haalbaar gelet op de aard van de maatregelen die noodzakelijk zijn om de veiligheid te waarborgen? En is het haalbaar gelet op de schaarse capaciteit en organisatorische beperkingen? Hoe kunnen op dit vlak zorgvuldige afwegingen gemaakt worden? Wat kan de overheid doen om – op basis van dreiging en risico - de bewegingsvrijheid en het functioneren van de persoon zo goed mogelijk faciliteren en hoe kan de te beveiligen persoon of een werkgever hier ook aan bijdragen? En wat zijn de consequenties als een persoon of werkgever hieraan niet wenst mee te werken?

Ophalen ervaringen van de TBP

Gelet op de impact van beveiligingsmaatregelen op personen en hun omgeving en de doelstelling om die impact zo veel mogelijk te beperken is het van belang de ervaringen van de TBP op te halen. Hoe hebben zij de dreiging en de maatregelen ervaren, hoe verloopt de informatievoorziening en communicatie tussen de overheid en de te beveiligen personen, welke zorg of psychosociale hulp heeft de TBP nodig en welke nazorg zou geboden kunnen worden als iemand niet meer beveiligd hoeft te worden? Wat kan geleerd worden van ervaringen elders in de zorg- en veiligheidsketen, denk aan de ervaringen opgedaan in getuigenbescherming?

Preventie en weerbaarheid

Een belangrijk uitgangspunt van het stelsel bewaken en beveiligen is de eigen verantwoordelijkheid van personen en organisaties om zich te beschermen tegen alle mogelijke vormen van dreiging. Veiligheid is allereerst een eigen verantwoordelijkheid van personen en organisaties. In de praktijk roept dit vragen op over de grens van de eigen verantwoordelijkheid en die van werkgevers. Wat kan preventief gedaan worden om te voorkomen dat iemand overheidsbescherming nodig heeft? Hoe kan de weerbaarheid vergroot worden, bijvoorbeeld door preventieve maatregelen in en rond de woning of door ander (reis)gedrag? Kunnen bepaalde beroepsgroepen weerbaarder gemaakt worden, denk aan politici, rechters, officieren van justitie, advocaten en journalisten? Daarbij zou geleerd kunnen worden van *good practices* elders binnen de overheid en de private sector en van ervaringen in het buitenland.

Maatschappelijke impact

De afgelopen jaren werd Nederland geconfronteerd met meerdere (pogingen tot) aanslagen op criminaliteitsbestrijders, journalisten, advocaten, en politici. De maatschappelijk ophef was in een aantal gevallen groot en politici gaven aan dat het monddood maken van de vrije pers, het aanvallen van onze rechtsstaat en het doelbewust angst willen aanjagen in onze samenleving onacceptabel is. Maar hoe wordt deze dreiging door georganiseerde criminaliteit en politiek gemotiveerde dreigingen gepercipieerd? Wordt het als een incident gezien of als een structureel probleem gericht tegen de democratische rechtstaat? Hoe wordt hier in de samenleving en de media over gecommuniceerd? Wat zijn de kenmerken van het maatschappelijke debat rond deze dreiging en is deze vergelijkbaar met andere debatten rond veiligheidsthema's, zoals bijvoorbeeld terrorisme?

3. Organisatie van het stelsel en politiek-bestuurlijke context

Ontwikkeling van de organisatie van het stelsel

De stelselpartners hebben de afgelopen jaren flink geïnvesteerd in expertise en capaciteit en er zijn ontwikkelingen in gang gezet met als doel het vakgebied te professionaliseren, de aansturing te vereenvoudigen en de besluitvorming te verbeteren. Een van de conclusies van de Commissie Bos was dat het stelsel als geheel desondanks nog te veel overlegstructuren kent en dat het noodzakelijk is het stelsel zo te organiseren dat er een krachtige, integrale sturing mogelijk is. Een dergelijke sturing moet, onder meer, leiden tot meer inzicht en overzicht wat betreft de schaarse operationele capaciteit, expertise en de informatie die nodig is voor risico-inschattingen en besluit- en beleidsvorming. Hoe kan een dergelijk integrale sturing gerealiseerd worden? Welke organisatievormen passen bij het stelsel en bij de verschillende stelselpartners? Hoe worden het lokale gezag en andere ketenpartners hierbij betrokken? Hoe kan de uniformiteit, kwaliteit en doelmatigheid in de operatie geborgd worden? Wat kunnen we leren van eerdere ervaringen rond vergelijkbare vraagstukken en wat kan van het buitenland geleerd worden?

Ontwikkeling van de politiek-bestuurlijke context

Het stelsel bewaken en beveiliging is in zekere zin het product van meerdere aanpassingen van de manier waarop bewaken en beveiligen is georganiseerd, vaak naar aanleiding van schokkende aanslagen. Maatschappelijke en politieke ophef maakt inherent onderdeel uit van de context waarin de stelselpartners opereren binnen een samenleving die weinig risico's lijkt te accepteren, maar ook niet accepteert dat vrijheid en de rechtstaat onder druk staat. Dit roept vragen op over deze context en de invloed hiervan op het stelsel. Wat is de maatschappelijke impact van dreigingen en aanslagen, hoe gaan politici en bestuurders om

met risico's en welke invloed hebben incidenten op de ontwikkeling van het stelsel en hoe kan dit toekomstbestendig gemaakt worden?

Juridische en ethische vraagstukken en uitdagingen

Het stelsel bewaken en beveiligen is van groot belang voor de rechtstaat die bedreigd wordt door aanslagen op personen en objecten. Tegelijkertijd brengt het bewaken en beveiligen in de praktijk ook een beperking van vrijheden met zich mee. Dit roept vragen op over juridische en ethische dilemma's rond het stelsel en over bestaande wet- en regelgeving en over geleerde lessen in de praktijk. Denk aan de (juridische) grondslag van de zorgplicht van de overheid en de mate van de eigen verantwoordelijkheid van bedreigde personen en hun werkgever. Of denk aan juridische en ethische vragen met betrekking tot het verwerven en delen van informatie ten behoeve van bewaken en beveiligen. En waar liggen de grenzen als het gaat om het idee dat bedreigde personen zoveel mogelijk onbelemmerd moeten kunnen functioneren. Ook zijn er gelet op de impact van de dreiging voor de rechtstaat vragen over de strafmaat van het bedreigen van personen en organisaties.

Toekomstbestendigheid van het stelsel

Het stelsel bewaken en beveiligen kent een lange voorgeschiedenis en is het resultaat van een lopend proces van leren en aanpassen dat nooit af is. Het is daarom van belang dat het stelsel in staat is flexibel in te spelen op veranderingen in het dreigingsbeeld en op nieuwe maatschappelijke en technologische ontwikkelingen. Hoe creëer je hiervoor de noodzakelijke wendbaarheid, krachtige aansturing en intensieve samenwerking van ketenpartners, zoals voorgesteld door de Commissie Bos? Hoe kunnen de bij het stelsel betrokken organisaties vanuit een gezamenlijk perspectief op het stelsel en op de toekomst opereren? Hoe creëer je adaptief vermogen en innovatiekracht binnen het stelsel en tussen de verschillende partners en de buitenwereld? En hoe past bewaken en beveiligen binnen een bredere aanpak van geweld en criminaliteit?

4. Informatie, intelligence en inschattingen

Verwerven en delen van informatie

Informatie is voor het bewaken van personen en objecten cruciaal. De Commissie Bos constateert dat de huidige informatiepositie niet meer voldoet aan de behoefte van de praktijk, waarin de dreiging complexer en ongrijpbaarder is geworden. Wat is daarvoor nodig, binnen de verschillende stelselpartners en ten aanzien van de samenwerking binnen het stelsel? Hoe kunnen verschillende informatiestromen beter worden gekoppeld en wat zijn de hierbij behorende juridische randvoorwaarden? Hoe wordt geopereerd binnen het huidige

juridische kader? Wat zijn *good practices* op dit gebied? Welke concrete belemmeringen doen zich in de praktijk voor bij het verwerven en veredelen van informatie en bij het inrichten van een goede informatiepositie, bijvoorbeeld op IT-gebied? Wat zijn praktische, organisatorische, maatschappelijke en juridische vraagstukken rond het verzamelen van informatie uit open sources en het monitoren van sociale media? En hoe kan de informatiepositie worden verbeterd door betere monitoring en rapportage door politie in de wijk of door meer synergie en samenwerking tussen stelselpartners en ketenpartners?

Dreigingsinschatting

De dreigingsinschatting voor het zogenoemde 'rijksdomein' wordt gedaan door de Dienst Landelijke Informatieorganisatie (DLIO) van de Politie, de AIVD en de MIVD. Op decentraal niveau is de Dienst Regionale Informatie - organisatie (DRIO) van de Politie hiervoor verantwoordelijk. Voor het vaststellen van het dreigingsniveau wordt binnen beide domeinen dezelfde methode gehanteerd. Aan de hand van tabellen wordt een inschatting gemaakt van de mate van 'ernst' en 'waarschijnlijkheid' van de dreiging. Op basis van deze dreigingsinschatting wordt een maatregelenadvies gegeven. Deze kwantitatieve benadering roept vragen op over de uniformiteit van de gebruikte processen en de vergelijkbaarheid van de output van genoemde organisaties. En hoe beïnvloedt de kwantiteit en kwaliteit van de informatie de kwaliteit van de inschatting? Daarnaast is het van belang om op basis van informatie proberen vooruit te kijken. Hoe en in welke mate is het juridische en praktisch mogelijk en wenselijk om op basis van fenomenen of veronderstelde dreigingen vooraf een inschatting te kunnen maken om op basis daarvan proactief maatregelen te kunnen treffen of een strategie te bepalen? Welke consequenties heeft de transitie van dreigingsinschattingen gericht op voorspelbaarheid naar inschattingen gericht op voorstelbaarheid? En is het mogelijk om uitspraken over voorstelbare dreigingen meetbaar te maken?

5. Opschalen en afschalen van maatregelen

Besluitvorming en dilemma's rond op- en afschalen

Besluitvorming met betrekking tot het nemen van maatregelen om personen en objecten te bewaken en beveiligen vraagt om heldere dreigingsinschattingen en procedures, die uniform uitgevoerd moeten kunnen worden. Dat is niet eenvoudig binnen een domein met meerdere partners en verschillende niveaus. Dit geldt des te meer als er sprake is van grote, complexe en regio-overstijgende casussen. Hoe kom je in deze context tot uniformering van het besluitvormingsproces van het op- en afschalen van beveiligingsmaatregelen op operationeel niveau? En hoe bouw je tegelijkertijd ruimte in voor maatwerk? Wat kan er met betrekking tot op- en afschalen geleerd worden van *good practices* en van voorbeelden uit het buitenland. Een ander belangrijk issue met betrekking tot het op- en afschalen is de

maatschappelijke druk en politiek-bestuurlijke context. Hiermee verbonden is de vraag, hoe leg je genomen maatregelen uit aan politiek, samenleving en de TBP? En hoe communiceer je over de tijdelijkheid van deze maatregelen en het, uiteindelijk, weer terugvallen op de eigen verantwoordelijkheid of op hulpverlening door andere partners uit de zorg- en veiligheidsketen?

Maatregelenpakketten

Hoewel de dreiging ten aanzien van personen en objecten divers is en maatwerk geleverd wordt, hanteren de politie en de Koninklijke Marechaussee een aantal beveiligingsconcepten dat de basis vormt voor de samen te stellen pakketten. Gestreefd wordt om per dreigingsniveau vaste pakketten vorm te geven, onder meer ter bevordering van de duidelijkheid en gelijkheid voor een TBP. Deze ontwikkeling roept de vraag op of en hoe bepaalde te beveiligen personen en objectenkunnen worden gecategoriseerd en welke mate van flexibiliteit in bestaande beveiligingsconcepten noodzakelijk blijft? Andere vragen bij het werken met (vaste) pakketten hebben betrekking op de criteria en procedures voor het afbouwen en beëindigen van de maatregelen en wat wel en wat niet onder eigen verantwoordelijkheid en werkgeversverantwoordelijkheid valt.

6. Publiek-private samenwerking

Inzet ervaring en diensten private partijen

Bewaken en beveiligen zijn taken die niet alleen door overheidsdiensten, maar ook door veel private partijen geleverd worden. Denk aan veiligheidsmaatregelen in en om woningen, private beveiliging - inclusief patrouilles en meldkamers – veiligheidsadviseurs, privé persoonsbeveiligers en de beveiliging van luchthavens. De private partijen leveren een breed palet aan diensten waar gebruik van gemaakt kan worden. Welke kansen en mogelijkheden biedt dit voor het stelsel en wat zijn obstakels en dilemma’s rond publiek-private samenwerking? Hoe regel en organiseer je rond deze samenwerking informatiedeling, de inzet van geweldmiddelen, toezicht, screening, geheimhouding én transparantie, en de garantie van beschikbare capaciteit? Wat kan geleerd worden van bewaken en beveiligen door private partijen variërend van multinationals tot burgerwachten en blijf van mijn lijf huizen?

Eigen verantwoordelijkheid

Eigen verantwoordelijkheid staat voorop als het gaat om voorkomen dat de veiligheid van personen of objecten in gevaar komt. Dat vraagt om bewustwording en handelen van burgers en hun werkgever als de potentiële dreiging verbonden is met het werk dat personen

uitvoeren. De druk op het stelsel is groot en het is voor de overheid onmogelijk om iedereen te beschermen tegen alle mogelijke vormen van dreiging. Dit roept de vraag op hoe burgers en werkgevers de eigen verantwoordelijkheid concreet gestalte geven en hoe deze kan worden bevorderd. Een andere belangrijke vraag is wanneer de eigen verantwoordelijkheid eindigt en de overheid de verantwoordelijkheid op zich neemt. Zijn er op dit vlak verschuivingen te zien? En houdt de eigen verantwoordelijkheid van personen en werkgevers op wanneer een persoon door de overheid wordt beveiligd? Hoe kan de samenwerking tussen (potentieel) bedreigde private personen, werkgevers en de overheid verbeterd worden? Wat kan er wat betreft deze samenwerking en de eigen verantwoordelijkheid van het buitenland worden geleerd?

7. Vakmanschap

Behoefte aan kennis en vaardigheden

Het stelsel bewaken en beveiligen vraagt om duizenden specialisten en generalisten die direct of indirect betrokken zijn bij het bewaken en beveiligen van personen en objecten. De toenemende druk op het stelsel dat opereert in een complexe maatschappelijke en politiek-bestuurlijke context vraagt om meer en andersoortige kennis en vaardigheden. Hoe verandert de vraag naar trainingen en opleidingen? Welke nieuwe kennis en vaardigheden worden van professionals verwacht bij het geven van advies en het samenwerken met een TBP, het samenwerken met ketenpartners en private partijen, en het organiseren en uitvoeren van bewakings- en beveiligingstaken? En welke kennisbehoefte en vaardigheden zijn nodig voor het implementeren van nieuwe inzichten en technologieën in de praktijk?

Organiseren van trainen en opleiden

Bewaken en beveiligen kost veel capaciteit en zal als hoofdtaak van de politie en de Koninklijke Marechaussee veel vergen als het gaat om werven, opleiden en trainen. Op dit moment zijn er diverse opleidingen op het brede terrein van bewaken en beveiligen. De vraag is welke en hoeveel verschillende generieke opleidingen of specifieke opleidingspakketten nodig zijn? Wat kan geleerd worden van bestaande opleidingen en trainingen in binnen- en buitenland op het brede terrein van bewaken en beveiligen? Welke onderwijsvormen maken het mogelijk om snel veel werknemers te trainen, bij te scholen, of kennis te laten nemen van nieuwe maatschappelijke en technologische ontwikkelingen? En hoe organiseer je certificering, *life long learning*, groepsleren, omscholing en hoe versterk je het vakmanschap onder professionals? Welke rol kunnen private partijen en het regulier onderwijs hierbij vervullen?

8. Technologische en wetenschappelijke ontwikkelingen en innovatie

Relevante technologische en wetenschappelijke ontwikkelingen

De partners van het stelsel bewaken en beveiligen van personen en objecten maken volop gebruik van nieuwe technologieën. Denk aan informatietechnologie, het gebruik van sensoren en slimme camera's. De context waarin het stelsel functioneert wordt geconfronteerd met veranderingen van de dreiging, de modus operandi van daders en maatschappelijke en technologische ontwikkelingen. Welke van deze ontwikkelingen zijn het meest relevant voor de doorontwikkeling van het stelsel en welke aanpassingen en innovaties zijn nodig om het stelsel toekomstbestendig te houden? Denk aan ontwikkelingen op het gebied van *artificial intelligence*(AI), robotica en informatietechnologie in het algemeen? Welke nieuwe inzichten uit andere wetenschappelijke domeinen, denk aan victimologie, criminologie, psychologie, veiligheidskunde en crisismanagement kunnen helpen bij het ontwikkelen van nieuwe beveiligingsconcepten of de verdere ontwikkeling van preventief en repressief beleid?

Implementatie van innovaties

Voor een toekomstbestendig stelsel bewaken en beveiligen is zicht hebben op relevante technologische en wetenschappelijke ontwikkelingen van groot belang. De vraag rijst hoe nieuwe kennis en inzichten hun weg vinden in de dagelijkse praktijk en welke praktische, juridische en ethische zaken een snelle implementatie in het stelsel en adaptatie in de uitvoering in de weg staan. En hoe stimuleer je de innovatie- en ontwikkelkracht van de stelselpartners en zet je de wetenschappelijke schil rond het stelsel optimaal in? Wat zijn goede praktijkervaringen op dit gebied en wat kunnen we leren van andere overheidssectoren, de private sector en ervaringen in het buitenland als het gaat om innovaties en de implementatie daarvan?

Universiteit Leiden