Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2006–2007

# 22 112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

**Nr. 484**

## BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 12 januari 2007

Op 25 september 2006 heeft de Europese Commissie het «Groenboek betreffende detectietechnologieën bij werkzaamheden van wetshandhavings-, douane- en andere veiligheidsdiensten» gepubliceerd (COM(2006) 474).
De lidstaten is gevraagd een reactie op de vragen uit het Groenboek op te stellen en deze voor 10 januari 2007 aan de Commissie aan te bieden. Hierbij treft u ter behandeling aan het Groenboek en de kabinetsreactie op de in het Groenboek gestelde vragen.

### Aanleiding

De Commissie heeft veiligheid benoemd als een hoeksteen van haar beleid. De bestrijding van criminaliteit en terrorisme is voor de Commissie een belangrijk aspect van het veiligheidsbeleid. In haar mededeling «*Terreuraanslagen – Preventie, paraatheid en reactie*» van oktober 2004 heeft de Commissie haar antiterrorismebeleid uiteengezet. In deze mededeling is de *publiek-private veiligheidsdialoog* naar voren gebracht als instrument waarmee de publieke en de private sector met elkaar constructief overleg kunnen plegen over de veiligheidsbehoeften van Europa. Ook in het *Haags programma – Versterking van vrijheid, veiligheid en recht in de Europese Unie*, dat in november 2004 door de Europese Raad is aangenomen en dat momenteel het politiek programma van de Unie op het gebied van Justitie en Binnenlandse Zaken vormt, is het belang beklemtoond van publiek-private samenwerking in de bestrijding van georganiseerde criminaliteit en terrorisme.

Met het uitbrengen van dit Groenboek heeft de Commissie tot doel de elementen aan te reiken die de aanzet kunnen vormen van een dergelijke dialoog op het gebied van detectietechnologieën bij werkzaamheden van wetshandhavings-, douane- en andere veiligheidsdiensten.

KST104349
0607tkkst22112-484
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2007

De Commissie heeft op 28 en 29 november 2005 in Brussel een conferentie georganiseerd met als thema *Publiek-private veiligheidsdialoog: detectie- en aanverwante technologieën in de bestrijding van terrorisme.* Dit Groenboek is gebaseerd op de resultaten van die conferentie en stelt thema's en kwesties aan de orde die in de discussies naar voren kwamen. Door middel van dit Groenboek vindt een tweede consultatie plaats van de lidstaten.

**Inhoud Groenboek**

In het Groenboek worden verschillende vragen gesteld over de wenselijkheid en vorm waarmee de Commissie haar beleid kan inrichten op het gebied van detectietechnologieën bij werkzaamheden van wetshandhavings-, douane- en andere veiligheidsdiensten. Het Groenboek bevat de volgende onderdelen:

- standaardisering en veiligheidsonderzoek;
- behoeften en oplossingen;
- gebruik en certificering van apparaten en instrumenten studies en
- toepassing van de resultaten van de raadpleging.

**Hoofdlijnen kabinetsreactie**

Ook in Nederland is er behoefte aan detectietechnologieën bij werkzaamheden van wetshandhavings-, douane- en andere veiligheidsdiensten. De prioritering van de behoeftestelling ten aanzien van o.a. nieuwe detectietechnologieën bij werkzaamheden van deze diensten zal in Nederland plaatsvinden in de zgn. «Arena maatschappelijke veiligheid». In deze arena wordt aan de hand van kennis- en innovatiebehoeftes van eindgebruikers (de operationele diensten) in samenspraak met de industrie en kennisinstituten een nationaal onderzoeks- en ontwikkelingsprogramma maatschappelijke veiligheid ingericht. De verwachting is dat begin 2007 de eerste contouren van een vraaggestuurd onderzoeks- en ontwikkelingsprogramma gereed zullen zijn. In 2008 zal naar verwachting een voldragen onderzoeks- en ontwikkelingsprogramma op het gebied van innovatieve technologieën voor veiligheidstoepassingen gereed zijn. De behoeftestelling van de maatschappelijke partners in veiligheid is tevens relevant voor het European Security Research Programme.

Het kabinet vindt de behoeftebepaling uit de «Arena Maatschappelijke Veiligheid» richtinggevend. Bij de beoordeling van de voorstellen van de Commissie in het Groenboek is daarom ook rekening gehouden met de prioritering,voor zover deze momenteel bekend is, die in deze arena zal worden aangebracht.

Het kabinet is zich ervan bewust dat detectietechnologieën inbreuk kunnen maken op de persoonlijke levenssfeer van burgers en is van mening dat beginselen als doelbinding, noodzaak en proportionaliteit leidend moeten zijn bij de beoordeling van de inzet van dergelijke middelen. De toepassing van nieuwe technologieën kan ook leiden tot meer dataverwerking van (persoons)gegevens. Bij de ontwikkeling dient de integriteit en beveiliging van d.m.v. technologie verkregen persoonsgebonden gegevens meegenomen te worden. Bij het onderzoek naar de ontwikkeling en ingebruikname van detectietechnologieën dienen de privacyaspecten bij de beoordeling zo vroeg mogelijk mee te worden genomen.

Ik verzoek u mij, conform de bestaande gedragslijn, binnen één maand na dagtekening uw reactie op dit kabinetsstandpunt mede te delen. Om tegemoet te komen aan de in de aanhef genoemde dead line voor inzending aan de Europese Commissie, is het kabinetsstandpunt, na goedkeuring in

de Ministerraad van 15 december 2006, onder voorbehoud van parlementaire goedkeuring aan de Europese Commissie gezonden.

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

**Kabinetsreactie op het Groenboek van de Europese Commissie (CIE) betreffende detectietechnologieën bij de werkzaamheden van wetshandhavings-, douane- en andere veiligheidsdiensten (COM (2006) 474**

## Inleiding

De wereld is de afgelopen jaren sterk veranderd. Veranderingen en technologische ontwikkelingen volgen elkaar in een steeds sneller tempo op. De dreiging van terroristische aanslagen is nog steeds aanwezig en leidt tot een grote veiligheidsbehoefte. Globalisering leidt tot steeds intensievere verkeersstromen van mensen en goederen en (persoons)gegevens. Veranderde productiemethoden, waarbij op veel meer locaties dan voorheen deelproductie plaatsvindt, gaat gepaard met het ontwerpen van geavanceerde logistieke processen. Veiligheid is daarmee een thema geworden dat over landsgrenzen en regionale samenwerkingsverbanden heen strekt.

Nieuwe, innovatieve detectietechnologieën kunnen een bijdrage leveren aan veiligheid, waarbij onmiddellijk opgemerkt moet worden dat nieuwe technologieën alleen niet de veiligheid kunnen borgen. Ze moet passen in een samenstel van maatregelen die de veiligheid kunnen verbeteren, waarbij internationale samenwerking essentieel is.

Nederland vindt het belangrijk dat het borgen van de veiligheid zoveel mogelijk gepaard gaat met respect voor de privésfeer van de burger en dat de lasten voor het bedrijfsleven gereduceerd worden. We kunnen dat bereiken door er zoveel mogelijk voor te zorgen dat het ingrijpen van overheidswege niet ingrijpender is en niet vaker geschiedt dan noodzakelijk. Dit kan bijvoorbeeld door in het kader van internationale samenwerking te vertrouwen op controles die ergens anders al zijn verricht. Als er geen aanwijzingen zijn dat een verandering in de situatie is opgetreden is een nieuwe controle dan ook niet nodig, met uitzondering van wellicht steekproeven. Hiervoor is het noodzakelijk dat overheden, ook in de internationale omgeving, vertrouwen op controles die elders zijn uitgevoerd. Dat vertrouwen kan gestimuleerd worden doordat men weet dat de controles op hetzelfde niveau zijn uitgevoerd, bijvoorbeeld omdat de apparatuur voldoet aan internationaal aanvaarde standaarden. Verder zou het mogelijk moeten zijn om personen en bedrijven die aantoonbaar betrouwbaar zijn, doordat zij zelf veiligheidsmaatregelen hebben genomen en daar ook op toezien, tegemoet te komen met faciliterende maatregelen.

Om in Europees verband te komen tot een versterking van de gemeenschappelijke aanpak van detectie technologieën heeft de Europese Commissie het initiatief genomen om de interactie tussen de publieke en de private sector verder te versterken, de investeringen te concentreren op standaardisering, onderzoek, certificering en interoperabiliteit van detectiesystemen, en de onderzoeksresultaten om te zetten in nuttige en praktische instrumenten.
Op 28 en 29 november 2005 heeft de Commissie in Brussel een conferentie georganiseerd met als thema *Publiek-private veiligheidsdialoog: detectie- en aanverwante technologieën in de bestrijding van terrorisme.* Door middel van het onderhavige Groenboek betreffende detectietechnologieën bij de werkzaamheden van wetshandhavings-, douane- en andere veiligheidsdiensten dat de Europese Commissie heeft opgesteld, vindt een tweede consultatie plaats van de lidstaten en de private sector plaats. Hiermee wordt nader onderzocht de publieke en private behoeftestelling op het gebied van detectietechnologieën. Ook wordt voorgesteld te onder-

zoeken welke nationale mogelijkheden er al bestaan op het terrein van detectietechnologieën en wat er internationaal wenselijk is.

Door middel van ruim 50 vragen worden lidstaten gevraagd de gewenste invulling vooraf aan te geven. De vragen hebben betrekking op de bovengenoemde aspecten.

Alvorens op de afzonderlijke vragen in het Groenboek in te gaan, hecht het kabinet er belang aan te onderstrepen dat de vragen algemeen van aard zijn. In verband met de vraagstellingen rond Europese samenwerking op het gebied van detectietechnologieën zijn een aantal aspecten van belang. Nederland hecht eraan deze algemene overwegingen rond dit vraagstuk te benadrukken, omdat leidend zijn voor eventueel te ondernemen initiatieven. Deze voor Nederland belangrijke onderwerpen zijn in de samenvatting verwoord.

De reikwijdte van de technologieën die het Groenboek beslaat is zeer breed. Zij beslaat het detecteren van (risicostoffen), ongewenste goederen, persoonskenmerken, bewegingen en opsporingsinformatie in data en text (data en textmining). Ook het doel is breed en varieert van het beschermen van burgers, bewaken van vitale infrastructuur en personen, voorkomen van aanslagen maar ook de mogelijkheid van het opsporen van daders na een incident. Er is geen duidelijke prioriteit aangegeven aan één welomschreven doel.

In Nederland is er behoefte aan detectietechnologieën voor alle bovengenoemde doelen De prioritering van de behoeftestelling ten aanzien van o.a. nieuwe detectietechnologieën vindt in Nederland plaats in de zogenaamde «Arena maatschappelijke veiligheid». In deze arena wordt aan de hand van de behoefte aan innovatie van de eindgebruikers (de operationele diensten) in samenspraak met de industrie en kennisinstituten een nationaal onderzoeks- en ontwikkelingsprogramma maatschappelijke veiligheid ingericht. Wegens de omvang van het thema maatschappelijke veiligheid is de arena verdeeld in acht thema's, de zogenaamde subarena's, bijvoorbeeld de subarena radicalisering en terrorisme en de subarena overlast en kleine criminaliteit. De verwachting is dat eind 2006, begin 2007 de eerste contouren van een vraaggestuurd onderzoeks- en ontwikkelingsprogramma gereed zullen zijn. In 2008 zal naar verwachting een voldragen onderzoeks- en ontwikkelingsprogramma op het gebeid van innovatieve technologieën voor veiligheidstoepassingen gereed zijn. De behoeftestelling van de maatschappelijke partners in veiligheid die uit het programma volgen worden – waar van toepassing – middels het nationale programma door Nederland ingebracht in het eerder genoemde European Security Research Programme.

Bij de beoordeling van de voorstellen van de Commissie in het Groenboek zal daarom ook rekening gehouden moeten worden met de prioritering die in de arena maatschappelijke veiligheid uiteindelijk zal worden aangebracht.

Hierbij dient te worden aangetekend dat vele technologieën multi-inzetbaar zijn en daardoor meerdere doelen kunnen dienen.

De reactie op het Groenboek geeft de visie van Nederland op het gebruik en ontwikkeling detectietechnologieën bij de werkzaamheden van wetshandhavings-, douane- en andere veiligheidsdiensten en de vragen uit het Groenboek worden beantwoord.

De belangrijkste punten uit het Nederlandse standpunt zijn:

– Nederland is er in beginsel voorstander van dat de verdere ontwikkeling van detectie en aanverwante technologieën in een brederinternationaal- verband wordt onderzocht. De behoefte van de eindgebruiker staat hierbij voorop. De markt kan hier vervolgens op inspelen. Op korte termijn is de verwachting dat de Nederlandse behoefte zal bestaan uit het effectiever en efficiënter maken van de bestaande detectoren en het mobiel kunnen inzetten van apparatuur om de onveiligheid effectiever en efficiënter te bestrijden.
– Bij bespreking van dit vraagstuk is het van belang om een onderscheid te maken tussen mogelijkheden en beperkingen van technische mogelijkheden, doel van de inzet van technologieën, gebruik, omgang met data die deze systemen genereren en vragen rond opslag en doorgifte.
– Nederland is zich ervan bewust dat detectietechnologieën inbreuk kunnen maken op de persoonlijke levenssfeer van burgers en is van mening dat beginselen als doelbinding, noodzaak en proportionaliteit leidend moeten zijn bij de beoordeling van de inzet van dergelijke middelen. De toepassing van nieuwe technologieën kan leiden tot meer verwerking van (persoons)gegevens. Bij de ontwikkeling dient de integriteit en beveiliging van middels technologie verkregen gegevens meegenomen te worden. Bij het onderzoek naar de ontwikkeling en ingebruikname van detectietechnologieën dienen de privacy aspecten bij de beoordeling zo vroeg mogelijk mee te worden genomen.
– Bij de inzet van detectietechnologieën en mogelijke Europese samenwerking is een kosten-baten analyse van groot belang.
– Nederland dringt aan op het rekening houden met bestaande systemen en gedane investeringen bij beoordeling van Europese initiatieven, onder meer op standaardisering.
– Nederland legt nadruk op het belang om andere Europese initiatieven op het terrein van detectietechnologieën bij de thematiek van dit groenboek te betrekken. Enkele belangrijke zijn, het European Security Research Programma (ESRP, reeds genoemd in Groenboek).
– Nederland vraagt aandacht voor de mogelijkheid dat de te ontwikkelen systemen en apparatuur breed inzetbaar zijn en dat ze worden opgenomen in ketens van beschermende maatregelen.
– Nederland vraagt daarom aandacht voor de ontwikkeling van protocollen en interfaces die het mogelijk maakt detectiesystemen en detectieapparatuur zonder problemen aan elkaar te koppelen en gegevens overdracht van het ene systeem naar het andere systeem probleemloos te laten verlopen.
– Nederland vraagt aandacht voor ergonomische en gebruiksaspecten van detectieapparatuur en mogelijke gezondheidsrisico's die gebruik van apparatuur met zich mee kan brengen.
– Vanuit efficiency overwegingen dient het gebruik van apparatuur zoveel mogelijk universeel te zijn, zodat onder meer opleidingskosten voor personeel laag kunnen worden gehouden. Nu is het vaak het geval dat het gebruik van verschillende detectieapparatuur verschillende training noodzakelijk maakt.
– Daarnaast is het wenselijk de mate van verplichting tot het gebruik van standaarden binnen de EU overeen te komen, zodat dat inspanningen die door private organisaties geleverd worden of die van deze organisaties gevraagd worden binnen Europa in grote mate overeen komen.
– Nederland is voorstander van het toepassen van goede praktijken, onder meer als basis voor verdere kennisontwikkeling.
– Nederland constateert dat op het werkterrein van detectietechnologieën door de commissie al meerdere initiatieven zijn genomen, De samenhang tussen de initiatieven is onduidelijk. Nederland vraagt de commissie stroomlijning en coherentie tussen de initiatieven te bewerkstelligen waarbij in ieder geval de onderlinge relatie en het beoogde doel van deze initiatieven beter naar voren komt. Nederland

spreekt ook de wens uit om rekening houden met lopende internationale initiatieven van onder andere VS.
– Enkele andere initiatieven van de Commissie die raakvlakken hebben zijn:
  1. De vragenlijst die de Commissie recentelijk in de werkgroep terrorisme heeft uitgedeeld over surveillance systemen, met als doel meer inzicht te krijgen in de systemen in diverse Lidstaten. Deze informatie heeft onder als doel om te bezien hoe de samenwerking mogelijkerwijs versterkt kan worden.
  2. De workshop op 23–24 november 2006 over preventing radialogical en nuclear terrorisme en vragenlijst.
  3. De voortgang van de public-private partnership dialogue.
– Enkele andere initiatieven van de VS die raakvlakken hebben zijn:
  1. Het Container Security Initiative (CSI): extra controle van containers die bestemd zijn voor de VS. Het gaat om het vroegtijdig verstrekken van de ladingsgegevens, controle op basis van risico-indicatoren en eventuele fysieke cointrole (met scanners e.d.)
  2. Het Megaport Initiative: controle van containers op radioactiviteit. Uiteraard bedoeld voor de containers die bestemd zijn voor de VS, maar in Nederland worden alle containers gecontroleerd die via de haven van Rotterdam gaan.
  3. De Customs and Trade Partnership against terrorism (CT–PAT): een soort certificeringssysteem van de Amerikaanse overheid voor bedrijven die goederen leveren aan de VS.
  4. Het Advanced Passenger Information: het vroegtijdig verstrekken van gegevens over passagiers die naar de VS reizen.
– Bij vraagstukken rond goederenvervoer en douanecontroles is een bredere inbedding van Europese initiatieven in internationaal perspectief van belang.

## BEANTWOORDING VAN DE VRAGEN UIT HET GROENBOEK

De vragen zijn in het Groenboek per (sub)paragraaf aangegeven. De paragraaf indeling is bij de beantwoording aangehouden.

## I. STANDAARDISERING EN VEILIGHEIDSONDERZOEK

### 1. Standaardisering (pagina 7)

Vraag:
Zijn er gemeenschappelijke normen nodig voor de opsporings- en aanverwante technologieën die worden gebruikt bij de werkzaamheden van veiligheidsdiensten? Welke normen acht u prioritair?
Antwoord:
Ja, gemeenschappelijke functionele normen zijn nodig.
- Ten eerste op het gebied van grensoverschrijdende vraagstukken zodat de verkregen resultaten uit de detectie en opsporingstechnologie eenduidigheid opleveren ten aanzien van de betrouwbaarheid en aanvaardbaarheid waardoor zij over en weer door staten worden erkend.
- Ten tweede op interoperabiliteit zodat verschillende apparatuur van verschillende leveranciers die een detectieketen vormen zonder problemen op elkaar kunnen worden aangesloten.
- Ten derde de data uit detectieapparatuur/ketens in een standaard format kunnen worden uitgelezen, zodat deze eventueel zonder aanpassingen voor nader onderzoek kan worden ingelezen (plug and play) in analyse- en opsporingsapparatuur.

Vraag:
Welke normen ontbreekt het aan financiële steun in de pre-standaardiseringsfase?
Antwoord:
De overheid moet aangeven welke apparatuur zij wenst, maar daarmee is nog niet gezegd dat de overheid mede-investeerder zou moeten zijn. Voor detectieapparatuur geldt hetzelfde als voor andere producten als het aankomt op investeringen en het terugverdienen ervan.

Vraag:
Teneinde dubbel werk te voorkomen en de transparantie te verbeteren, zou een regelmatig bijgewerkte lijst/handboek/databank met zoekfunctie van voorbije, lopende en geplande inspanningen voor de standaardisering op het gebied van opsporing en nauw verwante technologische terreinen op nationaal en Europees niveau nuttig zijn?
Antwoord:
Op termijn lijkt ons dat nuttig. Eerst moet echter de standaardisering worden gerealiseerd. De databank met standaarden dient te worden ondergebracht bij de Europese Standaardisatie Instituten zoals SELENEC en ETSI. Nationale overheden zullen deze standaarden in moeten voeren in hun regelgeving en aankoopbeleid voor hun eigen organisaties.

Vraag:
Zou u geïnteresseerd zijn in het vaststellen en uitwisselen van goede praktijken op het gebied van het gebruik en de verwerking van gegevens en informatie die met behulp van opsporingsinstrumenten zijn verzameld, zodat u volledig kan voldoen aan de relevante wet- en regelgeving in verband met de toelaatbaarheid van bewijs in gerechtelijke procedures?
Antwoord:
We zijn daarin geïnteresseerd, te meer om van opgedane ervaringen te kunnen leren. Ook bieden best practices aanknopingspunten voor Europese samenwerking.

Vraag:
Wat zou de beste manier zijn om deze praktijken vast te stellen en uit te wisselen?
Antwoord:
In de op te richten Europese onderzoeksarena maatschappelijke veiligheid (denk bijvoorbeeld aan de ESRP) moet dit worden uitgewisseld.

Het is wenselijk om zoveel mogelijk aansluiting te zoeken bij bestaande structuren. Zo is bestaat er op het niveau van de Wereld Douane Organisatie er al een gegevensbank voor geavanceerde technologie (inclusief detectietechnologie) die voor de leden van de WDO toegankelijk is en waarop producenten hun producten kunnen aanbieden. Ook nuttig is direct contact tussen uitvoerende diensten, zoals geschied bij het programma Douane 2007 van de Europese Commissie (DG TAXUD). Ook kan gedacht worden aan de werkgroepen samenwerking politie en samenwerking douane.

## 2. Veiligheidsonderzoek

Vraag:
Hoe zou informatie over veiligheidsonderzoek in Europa moeten worden verspreid om het concurrentievermogen te bevorderen en de verspilling van schaarse middelen te voorkomen?
Antwoord:
In de Europese arena. Opgemerkt dient te worden dat het European Security Research Programme vanaf 2007 Europees onderzoek naar opsporingstechnieken zal stimuleren door door Lidstaten ingediende project-

voorstellen op dit terrein te subsidiëren. Afstemming en delen van resultaten staat centraal bij het ESRP.

In ieder geval zou het al een stap voorwaarts zijn als de verschillende initiatieven en lopende programma's binnen de EU in kaart gebracht worden en op elkaar worden afgestemd.

## II. BEHOEFTEN EN OPLOSSINGEN

### 1. Technologische behoeften en oplossingen

Vraag:
Bent u geïnteresseerd in een ruimer debat over de rol van detectietechnologieën en de mogelijke invloed van hun gebruik op Europese samenlevingen?
Antwoord:
Ja, we zijn daarin geïnteresseerd; ook mogelijkheden en beperkingen moeten daarbij aan de orde komen. Een dergelijk debat dient echter binnen de bestaande structuren plaats te vinden.

Vraag:
Op welke specifieke gebieden hebben de bevoegde veiligheidsdiensten technologische verbeteringen nodig? Geef voor elke specifieke behoefte het prioriteitsniveau aan.
Antwoord:
Voor zover ons thans bekend is dat apparatuur op elkaar moet kunnen aansluiten om in een keten te gebruiken. Universele apparatuur, zowel in toepassing als in bediening. Meer kunstmatige intelligentie toepassen zodat de mens effectiever en efficiënter met de apparatuur kan werken. Als we het bij de douane over een keten hebben denken we aan logistieke ketens. Om ervoor te zorgen dat uitgevoerde controles in andere landen geaccepteerd worden zou het behulpzaam zijn dat de uitkomsten ongeacht de apparatuur hetzelfde is.

Vraag:
Bestaat er een kloof tussen vereisten voor detectiecapaciteiten en de technologie die momenteel op de markt beschikbaar is? Wat zijn de mogelijke oplossingen om die kloof te dichten?
Antwoord:
Er is een kloof tussen de vereiste en de beschikbare technologie. De huidige apparatuur voor bijvoorbeeld datamining in opgenomen beeldmateriaal is in het gebruik zeer tijdrovend. Met name bij het opzoeken en beoordelen van data (camerabeelden, sporen, etc.). Een vraag-gestuurd onderzoeksprogramma waarin de behoeftes van de veiligheidsdiensten worden geprioriteerd kan een oplossing bieden. De behoeften kunnen per dienst verschillen. Bij de douane wordt bijvoorbeeld de detectieapparatuur zoveel mogelijk ingepast in het logistieke proces van de stakeholders waarbij verspilling van tijd wordt voorkomen. Hierin voorziet zowel de arena Maatschappelijke Veiligheid (zie hierboven voor een toelichting) en het ESRP, waarin de behoeftes eindgebruiker zeer centraal staan.

Vraag:
Op welke specifieke gebieden biedt de private sector reeds technologische oplossingen aan of is hij van plan die aan te bieden? Geef de termijn aan waarbinnen die oplossingen beschikbaar zullen zijn tegen een kosteneffectieve prijs.

Antwoord:
Over de private sector kunnen op dit terrein geen uitspraken doen. In de arena maatschappelijke veiligheid zal vraag een aanbod op elkaar worden aangesloten.

Vraag:
Zou het nuttig zijn om op Europees niveau een lijst/databank met zoekfunctie op te stellen van de specifieke gebieden waarop de bevoegde veiligheidsdiensten behoeften hebben én de door de private sector aangeboden oplossingen?
Antwoord:
Hierin voorziet naar onze smaak het ESRP. Zoals al eerder gemeld heeft de Wereld Douane Organisatie een gegevensbank voor geavanceerde technologie

Vraag:
Indien niet, welke andere oplossingen zou u voorstellen om de informatiestroom tussen degenen die technologische oplossingen nodig hebben en de aanbieders daarvan te verbeteren?
Antwoord:
Zie hierboven.

*1.1 Soepele oplossingen*

Vraag:
Van welke bestaande instrumenten en apparaten kunnen de toepasbaarheid en de doeltreffendheid worden verbeterd door hun soepelheid te versterken?
Antwoord:
Van belang is dat verschillende toepassingen in een apparaat worden geïntegreerd. Verschillende apparatuur (van verschillende leveranciers bijv) moet inter-operabel zijn. Ook een universele bediening is uit overwegingen van flexibele personeelsinzet wenselijk.

Vraag:
Welke nieuwe soepele instrumenten en apparaten zijn nodig?
Antwoord:
We verwijzen hier ook naar de uitkomsten van de arena Maatschappelijke Veiligheid. De verwachting op dit moment is dat er behoefte is aan apparatuur die klein, draagbaar, eenvoudig te bedienen en multidisciplinair kan worden gebruikt. Het betreft hier een breed scala aan detectieapparatuur.

*1.2 Draagbare en mobiele oplossingen*

Vraag:
Welke bestaande instrumenten en apparaten zouden beter en doeltreffender bij de werkzaamheden van de bevoegde veiligheidsdiensten kunnen worden gebruikt, indien zij mobiel en draagbaar waren.
Antwoord:
Alle apparatuur om mensen, goederen en documenten te screenen. En apparatuur die ingezet kan worden bij mobiel toezicht. Alle apparatuur die ingezet wordt bij evenementen zoals wereldkampioenschappen, popconcerten en belangrijke politiek bijeenkomsten.

Vraag:
Welke nieuwe draagbare en mobiele instrumenten en apparaten zijn nodig?
Antwoord:
Dit vraagt om een uitvoerige inventarisatie van de uitvoerende diensten. Daar kan nu geen goed antwoord op gegeven worden. Vermoedelijk

zullen de uitkomsten van de arena maatschappelijke veiligheid op termijn richtinggevend kunnen zijn.

### 2. Interoperabiliteit van systemen

Vraag:
Van welke systemen moet de interoperabiliteit worden verbeterd?
Antwoord:
Alle sensorsystemen (beeld, geluid, reuk) en communicatiesystemen en personeelsbeschermingssystemen zouden inter-operabel moeten zijn. Zie antwoorden bij 1.1 en 1.2.

Vraag:
Zou een studie van de wettelijke en andere beperkingen voor de interoperabiliteit van de systemen in de EU nuttig zijn?
Antwoord:
Een dergelijke studie kan nuttig zijn. het is echter van belang daarbij aan te sluiten op andere EU initiatieven over dit vraagstuk, zoals interoperabiliteit voor opsporing – en wetshandhavingdatabanken.

### 3. Integratie van informatie die met verschillende opsporingstechnologieën is verkregen en verbetering van gegevensanalyse

Vraag:
Op welke gebieden denkt u dat de integratie van informatie uit verschillende opsporingstechnologieën de globale prestaties zou kunnen verbeteren?
Antwoord:
Het gaat niet om de integratie van de informatie maar om een integrale verwerking van de informatie.

Vraag:
Op welke gebieden moeten de technieken voor gegevensanalyse worden verbeterd?
Antwoord:
Bij allen. Technologische ontwikkelingen gaan voortdurend door.

## III. GEBRUIK EN CERTIFICERING VAN APPARATEN EN INSTRUMENTEN

### 1. Goede praktijken en het gebruik van bestaande instrumenten en apparaten

*Vaststellen van goede praktijken*

Vraag:
Wat zou de beste manier zijn om goede praktijken op dit gebied vast te stellen en te delen?
Zou dit moeten gebeuren door middel van wederzijdse evaluatie of door middel van vragenlijsten die aan de lidstaten worden toegezonden?
Antwoord:
Zie onze eerdere antwoorden voor verspreiden van kennis (arena MV/ ESRP) Een arena kan worden vormgegeven door middel van een onderzoeksprogramma, pilots, congressen, seminars, weblog, website, databank, etc. etc. Het een sluit het ander vooral niet uit.

*Verspreiden van goede praktijken*

Vraag:
Zou dit moeten gebeuren via een veilige databank met zoekfunctie of via bijeenkomsten en seminars?
Antwoord:
Zie onze eerdere antwoorden voor verspreiden van kennis (de arena Maatschappelijke Veiligheid en het ESRP).

Vraag:
Hebt u suggesties voor andere opties om goede praktijken op dit gebied zo goed mogelijk vast te stellen en te verspreiden?
Antwoord:
Zie antwoord op de vorige vraag.

Vraag:
Indien een aanpassing van een instrument of apparaat noodzakelijk wordt geacht en geen enkele lidstaat een dergelijke aanpassing zou hebben uitgevoerd, zou overleg met de private sector dienaangaande aanvaardbaar zijn.
Antwoord:
Ja.

**2. Vaststellen en verspreiden van goede praktijken en het gebruik van nieuwe instrumenten**

Vraag: Wat zou de beste manier zijn om informatie en goede praktijken op dit gebied vast te stellen en te delen?
Antwoord:
Zie antwoord op III,1 hierboven.

*Vaststellen van goede praktijken*
*Verspreiden van informatie en goede praktijken*

Vragen:
Zou dit moeten gebeuren door middel van wederzijdse evaluatie of door middel van vragenlijsten die aan de lidstaten worden toegezonden?
Zou dit moeten gebeuren via een veilige databank met zoekfunctie of via besloten bijeenkomsten en seminars?
Hebt u andere suggesties voor de manier om goede praktijken op dit gebied vast te stellen en deze doeltreffend te verspreiden?
Antwoord:
Zie ook programma ESRP. Met name bij potentieel marktfalen zou dit van belang kunnen zijn.

*Experimentele en nieuwe instrumenten*

Vraag:
Bent u geïnteresseerd in het testen van nieuwe of experimentele instrumenten en apparaten?
Antwoord:
Ja.

Vraag:
Zou gedeeltelijke financiering van tests van nieuwe of experimentele instrumenten en apparaten door de Gemeenschap en/of de private sector van belang zijn?
Antwoord:
Financiering van experimentele instrumenten past goed in de strategie om de Europese kenniseconomie te bevorderen, overeenkomstig de

Lissabon akkoorden en het daaruit voortvloeiende Zevende Kaderprogramma. De budgetdiscipline van het Zevende Kaderprogramma is hier geldig. Hierin is voorzien in het uitvoeren van pilotprojecten.

**3. Gebruik van instrumenten voor datamining en textmining.**

Opmerking: Datamining is niet alleen ontworpen om documenten te screenen, maar ook andere bronnen, zoals opgenomen beelden, telefoongesprekken, financiële stromen en internet- en e-mailverkeer en gegevens over mobiliteit van personen en goederen.
Door de toenemende digitalisering van de samenleving zijn en komen inderdaad zeer veel gegevens elektronisch beschikbaar, waardoor rechercheren met technische hulpmiddelen zoals datamining mogelijk is. Door de grote omvang van beschikbare gegevens zijn technische hulpmiddelen voor effectief onderzoek in deze bronnen ook onmisbaar. Uitzonderingen blijven bestaan, het uitluisteren van telefoontaps en het terugkijken van videobewakingsbeelden blijft, ondanks reeds bestaande technische hulpmiddelen, bewerkelijk.

*Bewustmakingscampagne*

Vraag:
Zouden de lidstaten en de bevoegde Europese organen geïnteresseerd zijn in het delen van goede praktijken en in de mogelijke voordelen van het gebruik van instrumenten voor datamining en textmining?
Antwoord:
Er bestaat interesse voor het uitwisselen van best practices en de voordelen van datamining en textmining.

Vraag:
Zouden de autoriteiten van de lidstaten die deze technologie gebruiken bereid zijn hun ervaring te delen met hun collega's?
Antwoord:
De inschatting is dat de autoriteiten daartoe bereid zijn en al in hoge mate ervaringen en kennis uitwisselen. Denk aan Europol en de samenwerking van douane en de veiligheidsdiensten.

Vraag:
Zou het nuttig zijn dat de lidstaten, Europol of OLAF besloten seminars over dit onderwerp organiseren?
Antwoord:
In het geval er sprake is van geheimhouding zouden besloten seminars wenselijk zijn. In andere gevallen dient zoveel mogelijk openheid betracht te worden. De private markt maakt ook veelvuldig gebruik van detectietechnologieën en wordt in voorkomende gevallen (luchthavens) zelfs verplicht detectietechnologieën toe te passen.

*Versterking van de capaciteit van de EU voor datamining en textmining*

Vragen:
Zou een expertisecentrum op Europees niveau dat voor alle lidstaten en hun bevoegde autoriteiten toegankelijk is, ertoe bijdragen dat het potentieel van deze instrumenten in de praktijk wordt benut?
Indien niet, welke andere opties zou u voorstellen om het potentieel van deze instrumenten ten volle te benutten?
Antwoord:
Waarom zou data-en textmining anders benaderd dienen te worden dan andere technologieën. We zijn voorstander om de bestaande structuren te gebruiken.

*Vaststellen en verspreiden van goede praktijken*

Vragen:
Zou een wederzijdse beoordeling of een aan de lidstaten toegezonden vragenlijst nuttig zijn bij het vaststellen van goede praktijken bij het gebruik van deze instrumenten?
Indien niet, welke andere benaderingswijzen zou u voorstellen om goede praktijken op dit gebied vast te stellen?
Antwoord:
Zie eerdere antwoorden op dit punt.

*Versterking van de regionale capaciteit voor datamining en textmining*

Vraag:
Zou er bij de lidstaten en de Europese organen capaciteit beschikbaar zijn om de lidstaten die hun documenten niet met behulp van deze technologie kunnen bewerken, te helpen?
Antwoord
De Lidstaten moeten elkaar helpen waar en wanneer mogelijk. Zoals bijvoorbeeld twinning programma's. Een nieuw Europees orgaan lijkt niet nodig.

Vraag:
Indien er geen of slechts beperkte capaciteit beschikbaar is, zou de versterking van de capaciteit in de lidstaten met middelen van de EU of op Europees niveau nuttig en praktisch zijn?
Antwoord:
Het in eerste de verantwoordelijkheid van een Lidstaat zelf zijn opsporingsapparaat op orde te hebben. EU is aanvullend, zie ook ESRP.

Vraag:
Zouden de lidstaten die niet over voldoende capaciteit voor datamining en textmining beschikken, het gebruik van de instrumenten van andere organen overwegen, indien zij daartoe de gelegenheid zouden krijgen?
Antwoord:
Ja, als tijdelijk meer capaciteit nodig is. Hierbij zal wel rekening moeten worden gehouden met de juridische mogelijkheden binnen de nationale wetgeving om capaciteit van andere organen te gebruiken.

Vragen:
Zou het mogelijk zijn Europese of regionale centra voor datamining en textmining op te richten waarop verschillende lidstaten en hun autoriteiten een beroep kunnen doen?
Zijn de bestaande instrumenten voor datamining en textmining voldoende afgestemd op de diverse talen in Europa?
Antwoord:
Europese en regionale centra voor data- en textmining? Lijkt ons niet nodig. Onderlinge samenwerking nader stimuleren waarbij wel op Europees niveau kan worden afgesproken dat verschillende expertise wordt opgebouwd op het gebied van verschillende data en talen.

Vraag:
Zijn er afdoende instrumenten om de autoriteiten die te maken krijgen met teksten en documenten in vreemde talen, te ondersteunen?
Antwoord:
Bij textming ja, indien nodig kunnen de door Nederland erkende nationale en internationale taalinstituten worden ingeschakeld.

In de uitvoering van taken – het horen van vreemdelingen – in zake de vreemdelingenwet ondervindt men in de praktijk wel beperkingen ten aanzien van parate beschikbaarheid van erkende gerechtstolken en vertalers.

### 4. Testen en certificeren van de kwaliteit van apparaten en instrumenten

Opmerking: kwaliteitsbeoordeling door middel van certificering wordt voorafgegaan door het vaststellen van normen en beoordelingsrichtlijnen. Zie hiervoor de antwoorden uit hoofdstuk 1 «standaardisering».
Vraag:
Zou het nuttig zijn om een netwerk van nationale certificeringsinstanties die kennis en ervaring delen op te richten en een systeem van kwaliteitscontrole in te voeren?
Antwoord:
Ja, zelfs in breder (Europees) verband. Een kanttekening is wel dat apparatuur welke zeer vertrouwelijke informatie bevat of an sich geheim is, niet via certificering kan worden beoordeeld, maar door een door de overheid gecontroleerd inspectie-orgaan.
De coördineren van het netwerk kan worden opgepakt door de controlegroep van de europeese rekenkamer CEAD (coördinatie,evaluatie, certificering en ontwikkeling).

Vraag:
Zouden gemeenschappelijke normen voor certificering en benchmarking nuttig zijn?
Antwoord:
Ja, deze zijn nuttig, maar ook de BRL's dienen daarbij te worden meegenomen.
Een uitzondering bestaat voor strikt geheime en uiterst gevoelige informatie en systemen.

## IV STUDIES

Vraag:
Zou u geïnteresseerd zijn in studies over deze thema's die gebaseerd zijn op de in bijlage uiteengezette achtergrondinformatie ?
Antwoord:
We zijn geïnteresseerd in deze studies. Ook hier moet niet het mondiale aspect uit het oog worden verloren.

## V TOEPASSING VAN DE RESULTATEN VAN DE RAADPLEGING

### 1. Versterkte specifieke publiek-private dialoog over opsporingstechnologieën en aanverwante technologieën

Vragen:
Zou een instrument als een versterkte specifieke publiek-private dialoog over opsporings- en aanverwante technologieën nuttig zijn bij de toepassing van de resultaten van de publieke raadpleging over dit groenboek? Indien ja, stemt u in met bovenstaande suggesties of hebt u andere ideeën?
Antwoord:
Ja, in Nederland hebben wij hiervoor de Arena Maatschappelijke Veiligheid opgericht. Zie voor een uitleg van deze arena hierboven.

Vraag:
Zou u geïnteresseerd zijn in een bijdrage of een rechtstreekse deelname aan de werkzaamheden?
Antwoord:
We zijn zeker geïnteresseerd in deelname. Op nationaal niveau zijn we al goed op weg met deze arena.

## 2. Actieplan

Vraag:
Zou een actieplan een nuttig instrument zijn voor het nemen van de maatregelen die in de antwoorden op dit groenboek worden voorgesteld?
Antwoord:
Het lijkt ons voor de hand te liggen dat, als men antwoorden verzameld, er actie op moet volgen.
Het is nuttig de resultaten van de raadpleging te bestuderen en te leggen naast andere activiteiten op dit terrein onder de hoede van andere directoraten binnen de EU. Als er dan terreinen zijn waarop nog geen actie wordt ondernomen zou een actieplan wellicht nuttig kunnen zijn.