KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER

Bruxelles, den 1.9.2006
KOM(2006) 474 endelig

# GRØNBOG

## om detektionsteknologier i de retshåndhævende myndigheders, toldmyndighedernes og andre sikkerhedsmyndigheders arbejde

(forelagt af Kommissionen)

# INDHOLDSFORTEGNELSE

**GRØNBOG**

**om detektionsteknologier i de retshåndhævende myndigheders, toldmyndighedernes og andre sikkerhedsmyndigheders arbejde**

(EØS-relevant tekst)

## INDLEDNING

Sikkerhed er en hjørnesten i Kommissionens politik. Bekæmpelsen af kriminalitet og terrorisme er et afgørende aspekt af sikkerhedspolitikken. Kommissionen beskrev sin antiterrorpolitik i sin meddelelse "*Terrorangreb: forebyggelse, beredskab og reaktion*" fra oktober 2004. I denne meddelelse fremhæves *sikkerhedsdialogen mellem den offentlige og den private sektor* som et redskab, som den private og den offentlige sektor kan bruge til at indlede en meningsfuld dialog om Europas sikkerhedsbehov. *Haag-programmet til styrkelse af frihed, sikkerhed og retfærdighed i Den Europæiske Union*, som blev vedtaget af Det Europæiske Råd i november 2004, og som nu udgør EU's politiske program for retlige og indre anliggender, understreger også betydningen af samspillet mellem den offentlige og den private sektor i bekæmpelsen af organiseret kriminalitet og terrorisme. Denne grønbog sigter mod at tilvejebringe de ingredienser, som skal gøre det muligt at indlede en sådan dialog vedrørende detektionsteknologier.

Detektionsteknologier anvendes stadig mere i sikkerhedsmyndighedernes daglige arbejde til at bekæmpe terrorisme og andre former for kriminalitet. Detektionsteknologier anvendes i vidt omfang til at beskytte passagererne ved ombordstigningen i fly og sportsfans under sportsbegivenheder og til at afsløre farlige stoffer i luften, vandet eller maden. Sikkerhedsmyndighederne anvender også disse teknologier til at beskytte vores grænser og kontrollere varer, der ankommer til EU's område. Desuden er detektionsteknologier afgørende for beskyttelsen af privat ejendom og kritisk infrastruktur. Formålet med denne grønbog er at finde ud af, hvilken rolle EU kan spille med henblik på at fremme detektionsteknologier for at øge borgernes sikkerhed. På den anden side griber detektionsteknologier ifølge sagens natur ind i privatlivets fred eller kan udgøre en udfordring for friheder og rettigheder. Hver gang man overvejer forbedring og anvendelse af detektionsteknologier er det derfor nødvendigt at foretage en grundig analyse af dette aspekt og det grundlæggende spørgsmål om, hvilke grænser der bør være for deres indgriben i privatlivets fred. Kommissionen har til hensigt at bidrage til begge spørgsmål med dette initiativ.

Kommissionen afholdt en konference[1] - *Public-Private Security Dialogue: Detection Technologies and Associated Technologies in the Fight against Terrorism* – i Bruxelles den 28.-29. november 2005. Over hundrede repræsentanter for både større europæiske erhvervs- og industrisammenslutninger og den offentlige sektor deltog i konferencen, hvilket viser, at parterne er interesserede i en politik på dette område. Fra den offentlige sektor deltog repræsentanter for de retshåndhævende myndigheder, toldmyndighederne og andre sikkerhedsmyndigheder.

[1] Yderligere oplysninger kan findes i del I i bilaget.

EU's rolle på områder som sikkerhedsforskning og standardisering er klart fastlagt. Selv om der på visse områder er gjort et stort stykke arbejde i tæt samarbejde med medlemsstaterne, erhvervslivet og andre interesserede parter, er der stadig plads til en forbedret europæisk politik for detektionsteknologier som sådan. Med hensyn til luftfartssikkerhed indeholder både forordning (EF) nr. 2320/2002 og forordning (EF) nr. 622/2003[2] detaljerede krav til det anvendte screeningudstyrs ydelser og metoderne. På dette område er der fastsat standarder og forsøgsprotokoller i tæt samarbejde med Den Europæiske Konference for Civil Luftfart, som består af eksperter fra de relevante myndigheder i medlemsstaterne og andre europæiske stater. Desuden er Kommissionen jævnligt i tæt kontakt med erhvervslivet og andre berørte parter (Stakeholders Advisory Group on Aviation Security – SAGAS-gruppen).

Med henblik på at styrke den fælles strategi for detektionsteknologier iværksatte Kommissionen dette initiativ for at forbedre samspillet mellem den offentlige og den private sektor yderligere i en bestræbelse på at fokusere investeringerne på standardisering af, forskning i, certificering af og interoperabilitet mellem detektionssystemerne og omdanne forskningsresultaterne til nyttige og anvendelige værktøjer. Der skal skabes en god cirkel, hvor den private sektors forskningsindsats og udgifter styres af en offentlig sektor, som ved, hvad den ønsker, og hvad den private sektor kan tilbyde. Det vil bidrage til udviklingen af et avanceret marked for detektionsprodukter og sikkerhedsløsninger, hvilket igen vil øge udbuddet af billigere varer og tjenester.

**Det er vigtigt med en fælles indsats og bedre koordination og informationsudveksling mellem alle berørte parter i EU, hvis dette mål skal kunne nås. Behovene skal defineres bedre, og der skal findes løsninger, som er både teknisk og økonomisk holdbare.** Det er bestemt ikke meningen, at der skal være **overlapning mellem denne grønbog og andre aktiviteter på nationalt eller europæisk plan**. Kommissionen ønsker ikke at genopfinde hjulet, men blot at få større viden om de eksisterende gode strategier og former for praksis og at støtte dem og udbrede dem i hele EU.

Kommissionen ønsker, at denne grønbog skal resultere i så mange tankevækkende svar og konkrete forslag til kommende skridt som muligt. **Det er derfor helt afgørende at sikre stor deltagelse af medlemsstaterne, den private sektor og andre relevante parter.** Kommissionen er dog godt klar over, at der af både sikkerhedsmæssige og kommercielle grunde må tages hensyn til fortrolighedskravene i såvel den offentlige som den private sektor. Hvis et svar er for følsomt til at blive offentliggjort, bedes respondenterne derfor oplyse dette og foreslå en alternativ metode, som vil gøre det muligt at tage hensyn til sådanne problemer.

Politikkerne vedrørende detektion og tilknyttede teknologier skal fuldt ud overholde den eksisterende lovgivning, herunder Den Europæiske Unions charter om grundlæggende rettigheder, den europæiske menneskerettighedskonvention og de databeskyttelsesprincipper og –regler, som er fastsat i direktiv 95/46/EF. I den forbindelse skal Kommissionen understrege, at udformningen, fremstillingen og anvendelsen af detektionsteknologier og tilknyttede teknologier sammen med lovgivning og andre foranstaltninger, der sigter mod at regulere eller fremme dem, **fuldt ud skal overholde de grundlæggende rettigheder** som omhandlet i Den Europæiske Unions charter om grundlæggende rettigheder og den europæiske menneskerettighedskonvention. Der må lægges særlig vægt på overholdelse af reglerne om beskyttelse af personoplysninger og retten til privatlivets fred. Da anvendelsen af

---

[2] Europa-Parlamentets og Rådets forordning (EF) nr. 2320/2002 af 16. december 2002 om fastsættelse af fælles bestemmelser om sikkerhed inden for civil luftfart, EFT L 355 af 30.12.2002, s. 1, og Kommissionens forordning (EF) nr. 622/2003 af 4. april 2003 om foranstaltninger til gennemførelse af grundlæggende fælles normer for luftfartssikkerhed, EUT L 89 af 5.4.2003, s. 9.

detektionsteknologier som regel medfører et indgreb i den grundlæggende ret til privatlivets fred og beskyttelse af personoplysninger, skal ethvert indgreb i de grundlæggende rettigheder overholde den europæiske menneskerettighedskonvention; det skal specielt være i overensstemmelse med lovgivningen og være nødvendig i et demokratisk samfund for at beskytte en vigtig samfundsinteresse, og det skal stå i et rimeligt forhold til den samfundsinteresse, som skal beskyttes.

# I. STANDARDISERING OG SIKKERHEDSFORSKNING

## 1. STANDARDISERING

Der findes et meget stort antal teknologiske muligheder på områderne vedrørende detektion og tilknyttede teknologier og sikkerhedsmyndighedernes arbejde. Der er derfor behov for minimumsstandarder. Men i betragtning af det store antal muligheder skal standardiserings-processen prioriteres højt, hvilket kun er muligt, hvis der er et tilstrækkeligt samspil mellem den offentlige sektor (behov) og den private sektor (løsninger). På europæisk plan anser både den offentlige og den private sektor dette samspil for at være utilstrækkeligt. Desuden udvikles der en lang række positive aktiviteter på både nationalt og europæisk plan. Men der findes ikke noget generelt overblik over, hvad der foregår, og der er behov for et sådant overblik for at undgå dobbeltarbejde og forbedre prioriteringen. Det er klart, at udviklingen af standarder af sikkerhedshensyn ikke kan drøftes åbent. Drøftelserne vil derfor hovedsagelig komme til at dreje sig om spørgsmålet om, i hvilket omfang det er ønskeligt at have fælles standarder.

Anvendelsen og behandlingen af data og oplysninger, som er indsamlet af detektionsværktøjer, f.eks. som bevismidler i retssager, er også tæt knyttet til standardisering. De relevante myndigheder ville have fordel af, at man kortlagde og udvekslede bedste praksis på dette område. Det bør også overvejes at indføre tekniske standarder for at sikre, at de indsamlede data overholder lovkravene vedrørende anvendelse af sådanne data i retssager[3].

**Spørgsmål**

Er der behov for fælles standarder for detektionsteknologier og tilknyttede teknologier, som anvendes i sikkerhedsmyndighedernes arbejde? Hvilke standarder mener De skal gives høj prioritet?

Hvilke standarder mangler økonomisk støtte i førstandardiseringsfasen?

Ville det være nyttigt med en regelmæssigt opdateret liste/håndbog/søgbar database over tidligere, igangværende og planlagte standardiseringsbestræbelser inden for detektionsteknologier og nært tilknyttede teknologiske områder på nationalt og europæisk plan for at undgå dobbeltarbejde og forbedre gennemsigtigheden?

Ville De være interesseret i at kortlægge og udveksle bedre praksis inden for anvendelse og behandling af data og oplysninger, som indsamles af detektionsværktøjer, med henblik på fuld overholdelse af den relevante lovgivning og de relevante regler vedrørende anvendelse af bevismidler i retssager?

Hvordan kan man bedst kortlægge og udveksle disse former for praksis?

[3] Oplysninger om lovgivningen om udveksling af personoplysninger findes i del II i bilaget.

## 2. SIKKERHEDSFORSKNING

Sikkerhedsforskning er et andet område, som er afgørende for udviklingen af nye sikkerhedsløsninger og -produkter til medlemsstaternes sikkerhedsmyndigheder. I den forbindelse skal den rolle, som Det Europæiske Rådgivende Udvalg for Sikkerhedsforskning (ESRAB) spiller, fremhæves. ESRAB anlægger et overordnet, bredt perspektiv på dette område og rådgiver Kommissionen om indholdet og gennemførelsen af den forskning, som skal foretages, sammen med ordninger til overvågning af relevante udviklinger i andre programmer.

Der foregår en række aktiviteter vedrørende sikkerhedsforskning på europæisk plan og i medlemsstaterne. Der findes dog ingen ordning for aggregering og udbredelse af oplysninger om tidligere, igangværende og foreslået sikkerhedsforskning på europæisk og nationalt plan og i sidste ende i den private sektor. En sådan ordning kunne sikre, at der ikke spildes knappe ressourcer på dobbeltarbejde og overlappende projekter. Hvis det anses for nødvendigt, kan der desuden indføres en særskilt ordning til udbredelse af klassificerede aktiviteter inden for sikkerhedsforskning, så det sikres, at det kun er de personer, der har ret til at få adgang til oplysningerne, der rent faktisk kan få adgang til dem.

Efter mere end et års arbejde er ESRAB i gang med at færdiggøre sin rapport, som vil blive offentliggjort i september 2006. Rapporten peger på ca. 120 sikkerhedsforanstaltninger og 100 nøgleteknologier, som kræver yderligere forskning og udvikling på EU-plan, mens en række andre teknologier behandles eller vil blive behandlet på nationalt plan.

**Spørgsmål**

Hvordan bør oplysninger om sikkerhedsforskning i Europa udbredes for at fremme konkurrenceevnen og samtidig undgå spild af knappe ressourcer?

# II. BEHOV OG LØSNINGER

## 1. TEKNOLOGISKE BEHOV OG LØSNINGER

Der kan kun udvikles gode, effektive og brugbare løsninger og produkter, hvis producenterne af disse løsninger og produkter har tilstrækkelige oplysninger om slutbrugernes faktiske behov. På europæisk plan ser der imidlertid ud til at være behov for et bedre samspil mellem dem, der har behov for tekniske løsninger (dvs. de relevante sikkerhedsmyndigheder), og dem, der tilbyder sådanne løsninger. Et sådant samspil bør også sigte mod at finde frem til, hvad de kort-, mellem- og langsigtede behov er. På den anden side bør de, som tilvejebringer løsningerne, også angive en tidsplan for, hvornår løsningerne vil være til rådighed.

Desuden bør en række mere grundlæggende spørgsmål vedrørende vore samfunds egenart og detektionsteknologiernes rolle også stilles og besvares i dialog mellem producenterne og brugerne. En sådan debat er også vigtig for at beskytte vore samfunds værdier og egenart.

**Spørgsmål**

Er De interesseret i en bredere debat om detektionsteknologiernes rolle og den indflydelse, anvendelsen af dem kan få på de europæiske samfund?

På hvilke specifikke områder har de relevante sikkerhedsmyndigheder behov for teknologiske forbedringer? Angiv, hvor højt de specifikke behov prioriteres.

Er der et hul mellem behovene for detektionsforanstaltninger og den teknologi, som på nuværende tidspunkt tilbydes på markedet? Hvordan kan problemerne med disse huller løses?

Anfør specifikke områder, hvor den private sektor allerede tilbyder eller har planer om at tilbyde teknologiske løsninger. Angiv en tidsplan for, hvornår sådanne løsninger vil være til rådighed og omkostningseffektive.

Ville det være nyttigt at oprette en søgbar liste/database for hele EU, som indeholder specifikke behovsområder for de relevante sikkerhedsmyndigheder og samtidig de løsninger, som den private sektor tilbyder?

Hvis nej, hvilke andre løsninger vil De foreslå for at forbedre informationsstrømmen mellem dem, der har behov for teknologiske løsninger, og dem, der tilbyder sådanne løsninger?

### 1.1 Alsidige løsninger

I vore dage er truslerne fra kriminalitet og terrorisme forskelligartede, de ændrer sig hele tiden og forekommer i forskellige former og på forskellige niveauer i forskellige situationer. De kræver derfor forskellige niveauer af beskyttelse og reaktion på forskellige tidspunkter, dvs. alsidige løsninger.

**Spørgsmål**

Hvilke eksisterende værktøjer og former for udstyr ville kunne gøres mere anvendelige og effektive ved at gøre dem mere alsidige?

Hvilke nye alsidige værktøjer og former for udstyr er der behov for?

### 1.2 Bærbare og mobile løsninger

Truslen fra terrorisme og kriminalitet ændrer ikke blot karakter med tiden, den bliver også stadig mere mobil. Sikkerhedsmyndighederne har derfor brug for bærbare løsninger. Sådanne løsninger kan øge omkostningseffektiviteten og kan let overføres fra ét sted til et andet, hvor der er mest behov for dem, da det ganske enkelt er umuligt at dække alle indrejsesteder eller problemområder med samme sikkerhedsniveau. Desuden kan bærbare og mobile løsninger give mulighed for nye operative strategier.

**Spørgsmål**

Hvilke eksisterende værktøjer og former for udstyr ville kunne anvendes bedre og mere effektivt i de relevante sikkerhedsmyndigheders arbejde, hvis de var mobile og bærbare?

Hvilke nye bærbare og mobile værktøjer og former for udstyr er der behov for?

## 2. SYSTEMERNES INTEROPERABILITET[4]

EU-medlemsstaterne og deres relevante myndigheder har allerede et antal systemer, som hjælper dem med at bekæmpe kriminalitet og terrorisme. Disse systemer kan imidlertid ofte ikke kommunikere med hinanden. Det kan hæmme de fælles bestræbelser på at bekæmpe kriminalitet og terrorisme på nationalt og europæisk plan. På den anden side skal systemerne overholde den eksisterende lovgivning og andre retningslinjer (f.eks. databeskyttelse og detektionssystemernes indgriben i privatlivets fred).

**Spørgsmål**

Hvilke systemer har behov for bedre interoperabilitet?

Ville det være nyttigt med en undersøgelse vedrørende juridiske og andre hindringer for systemernes interoperabilitet i EU for at kortlægge begrænsningerne?

## 3. INTEGRERING AF OPLYSNINGER FRA FORSKELLIGE DETEKTIONSTEKNOLOGIER OG FORBEDRET DATAANALYSE

Integreringen af data fra forskellige detektionsteknologier i ét dataanalysesystem kan gøre detektionssystemerne mere effektive. De foranstaltninger, som vedtages på dette område, skal overholde databeskyttelsesreglerne.

[4] Andre systemer end informationssystemer bør også tages i betragtning.

**Spørgsmål**

På hvilke områder mener De, at integrering af oplysninger fra forskellige detektionsteknologier ville forbedre de samlede resultater?

På hvilke områder er der behov for bedre dataanalyseteknikker?

# III. ANVENDELSE OG CERTIFICERING AF UDSTYR OG VÆRKTØJER

## 1. BEDSTE PRAKSIS OG ANVENDELSE AF EKSISTERENDE VÆRKTØJER OG UDSTYR

Der er ikke altid behov for helt nye teknologiske løsninger for at håndtere eksisterende eller nye trusler effektivt. De offentlige budgetter har ofte ikke råd til sådanne løsninger. Man bør derfor også være opmærksom på, hvordan eksisterende og tidligere anskaffede værktøjer kan anvendes mere effektivt eller opgraderes. Det kan være en omkostningseffektiv måde at forbedre effektiviteten, øge pålideligheden og mindske antallet af falske alarmer.

Der mangler en ordning for udveksling af erfaringer om sådanne spørgsmål mellem myndighederne i de forskellige medlemsstater. For eksempel kunne man udveksle oplysninger om forbedringer, som er opnået gennem ændringer i den operationelle procedure, eller omkostningseffektive opgraderinger.

**Spørgsmål**

Hvordan kan man bedst kortlægge og udveksle bedste praksis på dette område?

*Kortlægning af bedste praksis*

Bør det ske gennem peer-evaluering eller spørgeskemaer, som sendes til medlemsstaterne?

*Udbredelse af bedste praksis*

Bør det ske gennem en sikker og søgbar database eller gennem møder og seminarer?

Kan De foreslå andre løsninger til, hvordan man bedst kortlægger og udbreder bedste praksis på dette område?

Hvis det blev anset for nødvendigt med en opgradering af et værktøj eller udstyr, og ingen myndighed i andre medlemsstater havde foretaget en sådan opgradering, ville det så være acceptabelt at høre den private sektor om spørgsmålet?

## 2. KORTLÆGNING OG UDBREDELSE AF BEDSTE PRAKSIS OG ANVENDELSE AF NYE VÆRKTØJER OG NYT UDSTYR

De nationale myndigheder kan også i deres arbejde have gavn af et system, som ville lette udvekslingen af oplysninger om anvendelsen af nye værktøjer og nyt udstyr og gøre det muligt for dem at lære af hinanden og bygge videre på andres erfaringer. Sådanne udvekslinger af oplysninger, erfaringer og bedste praksis om værktøjer og udstyr kunne hjælpe myndighederne med at finde ud af, hvilket udstyr der kan anvendes til at opfylde deres særlige behov.

Derudover kunne afprøvningen af nyt eller eksperimentelt udstyr fremmes gennem samfinansiering fra fællesskabsbudgettet og/eller den private sektor. En mere omfattende

afprøvning af nyt og eksperimentelt udstyr ville kunne hjælpe det europæiske erhvervsliv med at omdanne sikkerhedsforskning til effektive og konkurrencedygtige produkter.

**Spørgsmål**

Hvordan kan man bedst finde frem til og udveksle oplysninger og bedste praksis på dette område?

*Kortlægning af bedste praksis*

Bør det ske gennem peer-evaluering eller spørgeskemaer, som sendes til medlemsstaterne?

*Udbredelse af oplysninger og bedste praksis*

Bør det ske gennem en sikker og søgbar database eller gennem møder og seminarer med begrænset deltagerkreds?

Har De andre forslag til, hvordan man bedst kan kortlægge bedste praksis på dette område og udbrede den effektivt?

*Eksperimentelle og nye værktøjer*

Er De interesseret i afprøvning af nye eller eksperimentelle værktøjer og former for udstyr?

Hvis ja/nej, forklar nærmere.

Ville en delvis finansiering af afprøvningen af nye eller eksperimentelle værktøjer og former for udstyr fra Fællesskabets og/eller den private sektors side være af interesse?

## 3. ANVENDELSE AF DATA MINING- OG TEXT MINING-VÆRKTØJER

De nationale og europæiske sikkerhedsmyndigheder står over for en konstant stigning i den mængde dokumentation og oplysninger, de skal behandle. Moderne softwareværktøjer til data mining og text mining gør det muligt at håndtere denne udfordring mere effektivt. Denne teknologi kan hjælpe med at udtrække relevante oplysninger fra et enormt antal dokumenter. For eksempel er det muligt at filtrere tekst og dokumenter på en intelligent måde for at støtte navigationen (gruppering af dokumenter) og med henblik på automatisk kategorisering (kanalisering og prioritering af dokumentstrømmen inden for efterforskningsholdene) og kontrol af, om kodeanvendelsen er gyldig. Målene er:

- et hurtigt overblik over nøgleenheder i dokumentsamlingerne
- forbehandling med henblik på målrettet dokumentsøgning
- indholdsbaseret klassificering af dokumenterne med henblik på at målrette yderligere analyser
- automatisk informationsanalyse på tværs af forskellige kilder.

De muligheder, som disse moderne værktøjer giver, udnyttes ikke tilstrækkeligt i medlemsstaterne. Men når man fremmer brugen af disse teknologier, må man være meget

opmærksom på, at anvendelsen i visse applikationer, f.eks. overvågning af e-mails, i sig selv er en indgriben i borgernes grundlæggende ret til privatlivets fred. E-mails er korrespondance og dermed omfattet af den ret til kommunikationshemmelighed, som er fastlagt i den europæiske menneskerettighedskonvention. Anvendelsen af teknikker til data mining og text mining skal derfor ske i overensstemmelse med loven, være nødvendig i et demokratisk samfund for at beskytte en vigtig samfundsinteresse og stå i et rimeligt forhold til den pågældende samfundsinteresse. Sådanne værktøjer og anvendelsen heraf bør automatisk omfatte støtte til overholdelse af de grundlæggende rettigheder og databeskyttelsesprincipperne. Endelig vil disse aktiviteter blive gennemført under de relevante offentlige myndigheders kontrol og overvågning.

**Spørgsmål**

*Oplysningsindsats*

Ville medlemsstaterne og de relevante europæiske organer være interesseret i at udveksle bedste praksis og i de mulige fordele, som følger af anvendelsen af data mining- og text mining-værktøjer?

Ville de myndigheder i medlemsstaterne, som anvender denne teknologi, være villige til at udveksle erfaringer med deres kolleger?

Ville det være nyttigt med seminarer med begrænset deltagerkreds om emnet, som blev afholdt af medlemsstaterne, Europol eller OLAF?

*Forbedring af EU's data mining- og text mining-kapacitet*

Ville et ekspertisecenter på europæisk plan, som alle medlemsstaterne og deres relevante myndigheder havde adgang til, gøre det lettere at udnytte disse værktøjers muligheder i praksis?

Hvis nej, hvilke andre muligheder vil De foreslå for at maksimere disse værktøjers muligheder?

*Kortlægning og udbredelse af bedste praksis*

Ville en peer-evaluering eller et spørgeskema, som sendes til medlemsstaterne, være nyttigt med henblik på at kortlægge bedste praksis for anvendelsen af disse værktøjer?

Hvis nej, hvilke andre metoder vil De foreslå til at kortlægge bedste praksis på dette område?

*Forbedring af den regionale data mining- og text mining-kapacitet*

Ville der være ledig kapacitet i medlemsstaterne og de europæiske organer til at hjælpe de medlemsstater, som ikke har denne teknologi, med at arbejde med deres dokumenter?

Hvis der ikke var ledig kapacitet eller kun begrænset kapacitet, ville en EU-finansieret forøgelse af kapaciteten i medlemsstaterne eller på europæisk plan så være nyttig og praktisk?

Ville de medlemsstater, der ikke har tilstrækkelig data mining- og text mining-kapacitet, overveje at anvende andre organers værktøjer, hvis de blev stillet til rådighed?

Ville det være muligt at oprette europæiske eller regionale centre for data mining og text mining, som en række medlemsstater og deres myndigheder kunne bruge til data mining og text mining?

Dækker de eksisterende data mining- og text mining-værktøjer i tilstrækkelig grad de forskellige sprog i Europa?

Findes der passende værktøjer til støtte for myndigheder, der behandler tekst og dokumenter på fremmede sprog?

*Andet*

Hvis De er uenig i en eller flere af ovenstående muligheder, hvad ville De så gøre ved de problemer, som er nævnt under dette punkt?

## 4. AFPRØVNING OG CERTIFICERING AF UDSTYRETS OG VÆRKTØJERNES KVALITET

Markedet tilbyder allerede en række detektionsprodukter. Det er dog meget ofte vanskeligt at finde ud af, hvilke værktøjer og produkter der er bedst eller i hvert fald opfylder visse minimumskrav. Et EU-system for certificering og benchmarking af værktøjer af god kvalitet, der er udformet sådan, at det forenkler arbejdet med at finde ud af, hvilke værktøjer eller hvilket ustyr der kan opfylde en bestemt myndigheds særlige behov, ville kunne løse dette problem. Det kan gøre det lettere for de nationale myndigheder at beslutte, hvilket udstyr og hvilke værktøjer de skal købe. Det kan også hjælpe myndighederne med at udnytte de knappe ressourcer bedst muligt.

Der kunne oprettes et netværk af *nationale* certificeringsmyndigheder, som udveksler erfaringer og viden, for at løse problemet med, at der ikke findes et system til at fastslå værktøjernes kvalitet. Disse myndigheder ville også kunne fastlægge standarder for benchmarking og certificering af teknologiske løsninger af god kvalitet. Denne form for certificering ville ikke blot kunne bruges til at hjælpe de nationale myndigheder med at afgøre, om et værktøj er godt eller ej, men også til at gøre reklame for europæiske løsninger på andre markeder. Det er klart, at udviklingen af forsøgsprotokoller af sikkerhedshensyn ikke kan drøftes åbent.

**Spørgsmål**

Ville det være nyttigt at etablere et netværk af nationale certificeringsmyndigheder, som udveksler erfaringer og viden, og et system for kvalitetscertificering og benchmarking?

Hvis nej, hvilken anden løsning foreslår De på det nævnte problem?

Ville det være nyttigt med fælles standarder for certificering og benchmarking?

Hvis nej, hvordan ville De sikre, at denne proces er gennemsigtig, og at resultaterne kan bruges i hele EU?

# IV. UNDERSØGELSER[5]

Deltagerne i konferencen pegede på flere forskellige emner, hvor der er behov for yderligere undersøgelser. Kommissionen foreslår derfor, at der gennemføres undersøgelser om:

(1) teknologi og beskyttelse af store arrangementer med mange deltagere

(2) hindringer for samarbejde og informationsudveksling mellem retsmedicinske laboratorier og sikkerhedsforskningsinstitutter

(3) lovbestemmelser, som regulerer brugen af specifik detektionsteknologi

(4) praktisk brug af specifik detektionsteknologi

(5) lovgivningen vedrørende brugen af persondetektion (herunder overvågning) i hele EU

(6) graden af accept af persondetektion (herunder overvågning og brug af biometri) i hele EU.

Generelt er formålet med undersøgelserne at bruge dem som et redskab, der kan øge de relevante parters viden og sikre, at den eksisterende lovgivning overholdes under udviklingen eller anvendelsen af detektionsteknologier. I andre tilfælde kan undersøgelserne bruges til at overveje politikmuligheder og muligheder for yderligere praktiske skridt.

**Spørgsmål**

Ville De være interesseret i at modtage undersøgelser om disse spørgsmål baseret på de baggrundsoplysninger, som er anført i bilaget?

Hvis nej, angiv hvorfor og foreslå alternative måder at håndtere de nævnte problemer på.

[5] Der gives en mere indgående beskrivelse af idéerne bag behovet for disse undersøgelser i del III i bilaget.

# V. GENNEMFØRELSE AF RESULTATERNE AF HØRINGEN

## 1. EN BEDRE SPECIFIK DIALOG MELLEM DEN OFFENTLIGE OG DEN PRIVATE SEKTOR OM DETEKTIONSTEKNOLOGIER OG TILKNYTTEDE TEKNOLOGIER

Denne grønbog afspejler en række mulige aktiviteter, som kan være med til at forbedre samspillet mellem den offentlige og den private sektor vedrørende detektionsteknologier og dermed hjælpe medlemsstaternes sikkerhedsmyndigheder med at få adgang til de bedst mulige værktøjer, løsninger og former for bedste praksis. Omvendt kan disse aktiviteter hjælpe den private sektor med at målrette sine investeringer og matche den offentlige sektors behov. Det er dog klart, at dette kræver et intensivt samarbejde mellem den offentlige og den private sektor. Der er derfor behov for en bedre specifik dialog mellem den offentlige og den private sektor på dette område. Dette kan ske på forskellige måder, bl.a. ved at etablere et særligt organ eller oprette en specifik gruppe inden for rammerne af horisontale partnerskabsøvelser med deltagelse af den offentlige og den private sektor, som bør iværksættes i den nærmeste fremtid.

Formålet med denne aktivitet ville ikke være at konkurrere med eksisterende organer, men snarere at tage sig af mangler i samspillet mellem den offentlige og den private sektor med deltagelse af de relevante sikkerhedsmyndigheder på europæisk plan. Der bør heller ikke være tale om et permanent organ; det skal have klart fastsatte mål, men når disse er nået, skal det nedlægges. Det skal bruges som et forum for eksperter fra både den private og den offentlige sektor og hjælpe med at behandle de spørgsmål, som tages op i dette dokument, eller nye udfordringer, der opstår under gennemførelsen af resultaterne af den offentlige høring om dette dokument.

På den anden side er det klart, at en række af de mulige foranstaltninger, som foreslås i dette dokument, ville kræve en indsats fra medlemsstaternes side uden deltagelse af den private sektor. Desuden skal både den offentlige og den private sektor være enige om fastlæggelsen af opgaverne for et sådant samarbejde, og medlemsstaterne vil dermed gennem deres medlemskab kunne få indflydelse på dets rolle og fokus. Det skal også behandle spørgsmålene om udveksling af fortrolige oplysninger mellem den offentlige og den private sektor, selv om det skal understreges, at det ikke kun er den offentlige sektor, der ligger inde med følsomme oplysninger.

**Spørgsmål**

Ville et værktøj som en bedre specifik dialog mellem den offentlige og den private sektor om detektion og tilknyttede teknologier være nyttigt med henblik på at gennemføre resultaterne af den offentlige høring om dette dokument?

Hvis ja, er De enig i ovenstående forslag, eller har De andre idéer?

Hvis nej, hvilke andre ordninger vil De foreslå til opfølgning af resultaterne af den offentlige høring om dette dokument?

Ville De være interesseret i at bidrage til dets arbejde eller i at deltage direkte i det?

## 2. HANDLINGSPLAN

På nationalt og europæisk plan har handlingsplaner vist sig at være et nyttigt redskab til at overvåge indsatsen på komplekse områder som bekæmpelse af terrorisme eller kriminalitet. Både konferencen og dette dokument har givet anledning til et stort antal spørgsmål vedrørende detektionsteknologier og tilknyttede teknologier i de relevante sikkerhedsmyndigheders arbejde. Med henblik på at overvåge fremskridtene på dette område og fastsætte en række mål kan der udarbejdes en handlingsplan på grundlag af svarene på disse spørgsmål og om nødvendigt yderligere høringer.

| **Spørgsmål** |
| --- |
| Ville en handlingsplan være et nyttigt redskab til gennemførelse af de foranstaltninger, som er nævnt i svarene på dette dokument? |

**Afsluttende bemærkning**

Svarene på dette dokument skal senest den 10. januar 2007 sendes elektronisk til følgende e-mail-adresse: **JLS-D1-Detection@ec.europa.eu**. Alle svar fra både den offentlige og den private sektor vil blive offentliggjort på Kommissionens website, medmindre respondenterne udtrykkeligt anfører, at de ønsker, at bestemte oplysninger hemmeligholdes.

# BILAG

## I. BAGGRUNDSOPLYSNINGER OM UDARBEJDELSEN AF GRØNBOGEN

Denne grønbog er baseret på resultaterne af konferencen og rejser en række emner og spørgsmål, som indtog en fremtrædende plads i diskussionerne (f.eks. standardisering, sikkerhedsforskning, forbedring af teknologiske løsninger, beskyttelse af privatlivets fred og den lovgivning og andre retningslinjer, som teknologierne skal overholde). Over 100 deltagere fra erhvervslivet, industrien og den offentlige sektor deltog i debatten. Den offentlige sektor var repræsenteret af medarbejdere fra de retshåndhævende myndigheder, toldmyndighederne og andre sikkerhedsmyndigheder, af Kommissionen og af repræsentanter for medlemsstaterne. Konferencens titel antyder, at den fokuserede på bekæmpelse af terrorisme. Det stod imidlertid klart fra starten, at det var nødvendigt med en bredere sikkerhedsstrategi, hvis man ikke skulle udelade en række vigtige sikkerhedsproblemer. Denne brede strategi blev bekræftet af den beslutning, som Rådet traf i december 2005 om at basere beskyttelsen af de kritiske europæiske infrastrukturer på en strategi, som omfatter alle risici. Desuden valgte konferencen en helhedsorienteret fremgangsmåde ved at bringe parter fra forskellige ekspertiseområder sammen for at drøfte følgende emner:

- Detektionsteknologier og beskyttelse af infrastruktur
- Persondetektionsteknologier og biometri
- Detektion af sprængstoffer og kemiske, biologiske, radiologiske og nukleare stoffer.

Alle emnerne fokuserede på de retshåndhævende myndigheders, sikkerhedsmyndighedernes og toldmyndighedernes arbejde. Denne fremgangsmåde gjorde det muligt at finde frem til en lang række områder, som både den offentlige og den private sektor lagde vægt på (f.eks. samspillet mellem dem, som tilbyder løsninger, og dem, som har brug for løsninger i den offentlige sektor). Dette er afspejlet i hele dokumentet.

*Definition af detektionsteknologier og relevante kategorier*

I forbindelse med høringen anvendes termen "detektionsteknologi" i den bredest mulige betydning. Detektionsteknologier kan være "in situ" eller eksterne, og formodentlig får man de mest sofistikerede midler til at håndtere nogle af sikkerhedsudfordringerne i forskellige scenarier, når de integreres i det komplekse system (såsom et transportsystem). En detektionsteknologi kan være næsten hvad som helst, der anvendes til at detektere noget i en sikkerhedskontekst, med fokus på retshåndhævende myndigheder, toldmyndigheder eller sikkerhedsmyndigheder. Det er muligt at finde frem til en række kategorier[6], som, hvis der tages hensyn til dem ved besvarelsen af spørgsmålene i dette dokument, kan være med til at præcisere svarene:

- Håndholdte detektorer
- Detektorkarme

[6] Listen over kategorier er ikke udtømmende.

- Overvågningsløsninger
- Detektion af biometriske identifikatorer
- Data mining- og text mining-værktøjer
- Andre softwarebaserede detektionsværktøjer.

Desuden bør respondenterne også overveje tilknyttede teknologier, når de besvarer spørgsmålene, da teknologier, som hjælper mennesker med at forstå de data, som detektorerne indsamler, også er vigtige for effektive løsninger. Der er behov for teknologi for at integrere løsningerne og gøre systemerne interoperable. Selv om respondenterne har fremhævet disse kategorier, bør de ikke føle sig forpligtet til at holde sig til dem, men opfordres til at tage andre spørgsmål op.

## II. STANDARDISERING OG UDVEKSLING AF PERSONOPLYSNINGER

Med hensyn til persondata skal Kommissionen påpege, at direktiv 95/46/EF allerede udgør den juridiske ramme for udveksling af information, der indeholder personoplysninger, i forbindelse med aktiviteter under "søjle 1". For så vidt angår udveksling af oplysninger som led i det retlige samarbejde har Kommissionen i overensstemmelse med tilgængelighedsprincippet fremlagt et forslag til lovgivning, som er under drøftelse.

## III. UNDERSØGELSER

### 1. Beskyttelse af store arrangementer

Hvert år organiserer EU's medlemsstater en række store offentlige arrangementer med mange deltagere af national og europæisk, men også international betydning. I vore dages sikkerhedsmiljø kan sikkerhedsomkostningerne i forbindelse med sådanne arrangementer sluge en betydelig del af deres budgetter. Alle medlemsstaterne ville have gavn af en fælles strategi for håndtering af dette problem.

For at bane vej for senere skridt på dette område foreslår Kommissionen, at der iværksættes en undersøgelse om beskyttelse af store arrangementer. Det vil blive undersøgt, hvilke sikkerhedsværktøjer, hvilket udstyr og hvilken ekspertise, som anvendes til at beskytte store arrangementer, der kan overføres fra ét arrangement/sted til et andet. Undersøgelsen vil også komme til at omfatte gennemførligheden og implikationerne af udstyr, som ejes af Fællesskabet, af udstyr, som deles på fællesskabsplan, af at udvikle en forretningsmodel for tjenesteydelser, der leveres af den private sektor, eller en kombination af de tre metoder. Denne del af undersøgelsen bør fastslå, hvilken løsning:

- der er mest omkostningseffektiv og er smidig nok til at passe til medlemsstaternes forskellige behov
- der kan sikre, at alle medlemsstaterne får adgang til denne løsning, og en passende omkostningsfordeling mellem medlemsstaterne.

Når resultaterne af undersøgelsen foreligger, vil Kommissionen overveje yderligere skridt på dette område i samarbejde med medlemsstaterne og andre relevante parter.

## 2. Samarbejde og informationsudveksling mellem retsmedicinske laboratorier og sikkerhedsforskningsinstitutter

Deltagerne i konferencen understregede, at der findes en række juridiske og andre hindringer på nationalt plan, som forhindrer et effektivt samarbejde og en effektiv informationsudveksling mellem de nationale retsmedicinske institutter på europæisk plan. Kommissionen foreslår derfor, at der gennemføres en undersøgelse om spørgsmålet. Denne undersøgelse kan også se nærmere på mulighederne for at rette op på situationen.

Tilsvarende problemer blev nævnt vedrørende samarbejde og informationsudveksling mellem sikkerhedsforskningsinstitutter. Der kan også gennemføres en særskilt undersøgelse om dette spørgsmål.

## 3. Lovgivning og specifik detektionsteknologi

Det undersøges tit, om de retshåndhævende myndigheder, toldmyndighederne og andre sikkerhedsmyndigheder overholder de gældende retlige standarder. Selv om teknologien som sådan ikke overtræder de retlige standarder, kan den måde, den bruges på, give anledning til bekymring. Ved at finde frem til den lovgivning, som regulerer anvendelsen af og sætter grænser for tekniske løsninger, kan man således øge bevidstheden i både den offentlige og den private sektor og lette overholdelsen af de eksisterende standarder. Den private sektor kan også have gavn af en sådan undersøgelse, når den foreslår og udformer teknologiske løsninger og tjenester for den offentlige sektor.

## 4. Specifik detektionsteknologi og den praktiske brug heraf

Tilsvarende må retningslinjerne og bedste praksis for anvendelsen af teknologier og specielt detektionsteknologier tage hensyn til, hvordan brugerne af disse teknologier rent faktisk anvender sådanne værktøjer i praksis, og hvordan de virker i forhold til de personer, som underkastes detektion. En specifik teknologi som sådan overtræder måske ikke de retlige standarder, men en operatørs anvendelse af teknologien i praksis kan give anledning til bekymring. Desuden kan udviklingen af nye teknologier eller en ændret anvendelse af eksisterede teknologier medføre situationer, hvor der ikke er nogen lovgivning, som regulerer anvendelsen af dem. I andre tilfælde er en bestemt anvendelse af en teknologi måske ikke i strid med lovgivningen, men den kan være i modstrid med bedste praksis eller de adfærdskodekser, der er udviklet som et supplement til de juridiske bestemmelser. Viden om forskrifterne (instrumenterne) på dette område kan gøre det muligt at vurdere, om de overholder lovgivningen (specielt de grundlæggende rettigheder og databeskyttelsesreglerne), og hvad der er acceptabelt eller uacceptabelt i en situation, hvor der ikke er udviklet retlige bestemmelser.

## 5. Persondetektionsteknologier og biometri

Persondetektion (herunder overvågning) og biometri er spørgsmål, som berører personer direkte, og der foregår derfor en følsom politisk debat om anvendelsen af disse værktøjer med henblik på at forbedre sikkerheden i Europa. Kommissionen foreslår, at der gennemføres en undersøgelse for at finde frem til den lovgivning, der gælder for persondetektionsteknologi og biometri. Denne undersøgelse skal analysere medlemsstaternes og EU's retssystemer og dermed fastslå, hvilke eksisterende regler der gælder for persondetektion og biometri. En undersøgelse af denne slags er særlig vigtig, når man skal sikre, at de teknologiske løsninger, som tilbydes af den private sektor, overholder lovgivningen. Den vil kort fortalt hjælpe den

private sektor med at forstå de retlige og andre begrænsninger for de teknologiske løsninger, den udvikler.

Der kan også udarbejdes særlige undersøgelser om, i hvilket omfang befolkningen i de enkelte medlemsstater og i EU accepterer overvågning og biometri. Metoden for disse undersøgelser skal sikre, at de to spørgsmål – overvågning og biometri – ikke blandes sammen. Sådanne undersøgelser kan hjælpe EU og de nationale regeringer med at iværksætte passende kommunikationsstrategier for disse spørgsmål. Generelt vil begge undersøgelserne bidrage yderligere til den politiske debat i Europa om disse vigtige emner.