



EUROPEISKA GEMENSKAPERNAS KOMMISSION

Bryssel den 1.9.2006
KOM(2006) 474 slutlig

GRÖNBOK

**om detektionstekniker i brottsförebyggande myndigheters, tullmyndigheters och andra
säkerhetsmyndigheters arbete**

(framlagt av kommissionen)

INNEHÅLLSFÖRTECKNING

Inledning.....	4
I. STANDARDISERING OCH SÄKERHETSFORSKNING.....	7
1. Standardisering.....	7
2. Säkerhetsforskning.....	8
II. BEHOV OCH LÖSNINGAR.....	9
1. Tekniska behov och lösningar.....	9
1.1 Mångsidiga lösningar.....	9
1.2 Bärbara och mobila lösningar.....	10
2. Driftskompatibilitet mellan system.....	10
3. Integration av information från olika detektionstekniker och förbättrad dataanalys.....	10
III. ANVÄNDNING OCH CERTIFIERING AV UTRUSTNING OCH VERKTYG.....	12
1. Bästa metoder och användning av befintliga verktyg och utrustning.....	12
2. Fastställande och spridning av bästa metoder och användning av nya verktyg och ny utrustning.....	12
3. Användning av verktyg för data- och textutvinning.....	13
4. Provning och certifiering av utrustningars och verktygs kvalitet.....	15
IV. UNDERSÖKNINGAR.....	16
V. GENOMFÖRANDE AV RESULTATEN AV SAMRÅDET.....	17
1. Bättre specifik dialog mellan den offentliga och den privata sektorn om detektionstekniker och relaterade tekniker.....	17
2. Handlingsplan.....	18
ANNEX.....	19
I. Background information on the preparation of the Green Paper.....	19
II. Standardisation and the exchange of personal data.....	20
III. Studies.....	20
1. Protection of mass events.....	20
2. Cooperation and information-sharing among forensic laboratories and security research institutes.....	21

3.	Law and specific detection technology	21
4.	Specific detection technology and its practical use.....	21
5.	Personal detection technologies and biometrics	21

GRÖNBOK

om detektionstekniker i brottsförebyggande myndigheters, tullmyndigheters och andra säkerhetsmyndigheters arbete

(Text av betydelse för EES)

INLEDNING

Säkerhet är en hörnsten i kommissionens politik. Bekämpning av brottslighet och terrorism är ett centralt inslag i säkerhetspolitiken. Kommissionen har redogjort för sin terroristbekämpningspolitik i meddelandet *Terroristattacker – förebyggande, beredskap och insatser* från oktober 2004. I meddelandet läggs tonvikten vid *säkerhetsdialogen mellan den offentliga och den privata sektorn* som ett redskap för dessa sektorer att inleda en meningsfull dialog om Europas säkerhetsbehov. *Haagprogrammet för stärkt frihet, säkerhet och rättvisa i Europeiska unionen*, som antogs av Europeiska rådet i november 2004 och för närvarande utgör EU:s politiska program på området för rättsliga och inre frågor, tar också upp vikten av samspelet mellan den offentliga och den privata sektorn i kampen mot organiserad brottslighet och terrorism. Denna grönbok syftar till att ge förutsättningarna för att inleda en sådan dialog angående detektionstekniker.

Säkerhetsmyndigheter använder sig i allt större utsträckning av detektionstekniker för att bekämpa terrorism och andra former av brottslighet. Detektionstekniker används i stor omfattning för att skydda passagerare när de går ombord på flygplan och publiken vid idrottsevenemang och för att upptäcka farliga ämnen i luft, vatten och livsmedel. Säkerhetsmyndigheter använder också sådan teknik för att skydda våra gränser och kontrollera varor som förs in på EU:s territorium. Sådan teknik är vidare av stor betydelse för att skydda privat egendom och viktig infrastruktur. Denna grönbok syftar till att ta reda på vilken roll EU skulle kunna spela när det gäller att främja användningen av detektionstekniker för att skydda dess medborgare. Å andra sidan innebär detektionstekniker till sin natur ett intrång i privatlivet eller kan utgöra ett hot mot fri- och rättigheter. Varje gång man överväger att förbättra och använda detektionstekniker måste man noggrant analysera denna aspekt och den grundläggande frågan om var gränserna för intrånget i privatlivet skall gå. Med det här initiativet vill kommissionen ge ett bidrag till båda dessa frågeställningar.

Den 28-29 november 2005 anordnade kommissionen en konferens i Bryssel – *Public-Private Security Dialogue: Detection Technologies and Associated Technologies in the Fight against Terrorism*¹. Över hundra företrädare för såväl stora europeiska företags- och branschorganisationer som den offentliga sektorn deltog, vilket vittnar om att berörda parter har ett intresse av en politik på detta område. Från den offentliga sektorn deltog företrädare för brottsbekämpande myndigheter, tullmyndigheter och andra säkerhetsmyndigheter.

EU har en klart fastställd roll på områden som säkerhetsforskning och standardisering. Även om ett avsevärt arbete har uppnåtts på vissa områden, i nära samarbete med medlemsstaterna, näringslivet och andra berörda parter, finns det fortfarande utrymme för en förbättrad EU-

¹ Se del I i bilagan för mer bakgrundsinformation.

politik om själva detektionsteknikerna. När det gäller luftfartsskydd innehåller både förordning (EG) nr 2320/2002 och förordning (EG) nr 622/2003² detaljerade krav i fråga om prestandan för den utrustning för säkerhetskontroll som används och i fråga om metoder. På detta område har standarder och testprotokoll fastställts i nära samarbete med Europeiska civila luftfartskonferensen, som består av experter från relevanta myndigheter i medlemsstaterna och andra länder i Europa. Kommissionen har dessutom regelbunden och nära kontakt med näringslivet och andra berörda parter (*Stakeholders Advisory Group on Aviation Security (SAGAS)* – Rådgivande grupp för berörda parter om luftfartssäkerhet).

I syfte att stärka den gemensamma strategin i fråga om detektionstekniker har kommissionen tagit detta initiativ för att ytterligare förbättra samspelet mellan den offentliga och den privata sektorn, i en strävan att fokusera investeringarna på standardisering, forskning, certifiering och driftskompatibilitet mellan detektionssystem och att omvandla forskningsresultat till nyttiga och användbara verktyg. Det måste skapas en ”god cirkel” där den privata sektorns forskningsarbete och utgifter styrs av en offentlig sektor som vet vad den vill och vad den privata sektorn har att erbjuda. Detta bör bidra till att utveckla en avancerad marknad för detektionsprodukter och säkerhetslösningar, som i sin tur bör öka utbudet av billigare produkter och tjänster.

För att detta mål skall kunna uppnås behövs det gemensamma insatser och bättre samordning och informationsutbyte mellan alla berörda parter i EU. Behoven måste definieras bättre och man måste finna lösningar som är tekniskt och ekonomiskt hållbara. Tanken är inte att denna grönbok skall överlappa annan verksamhet på nationell eller europeisk nivå. Kommissionen vill inte uppfinna hjulet på nytt, utan den vill få mer kunskaper om tillvägagångssätt och praxis som redan finns och stödja och sprida dem över hela unionen.

Kommissionen är angelägen om att denna grönbok ger så många tankeväckande svar och konkreta förslag om kommande åtgärder som möjligt. **Ett stort deltagande av medlemsstaterna, den privata sektorn och andra berörda parter är därför av avgörande betydelse.** Kommissionen är dock medveten om de sekretesskrav som finns inom såväl den offentliga som den privata sektorn av säkerhetsskäl och kommersiella skäl. De som svarar på grönboken ombeds därför att ange om ett svar är alltför känsligt för att offentliggöras och föreslå någon annan metod för att ta itu med detta problem.

Politiken i fråga om detektionstekniker och relaterade tekniker måste fullt ut överensstämma med de befintliga rättsreglerna, däribland EU:s stadga om de grundläggande rättigheterna, Europeiska konventionen om skydd för de mänskliga rättigheterna samt de principer och regler för uppgiftsskydd som föreskrivs i direktiv 95/46/EG. I detta sammanhang vill kommissionen betona att formgivning, tillverkning och användning av detektionstekniker, samt lagstiftning och andra åtgärder som har till syfte att reglera eller främja sådana tekniker, **fullt ut måste respektera de grundläggande rättigheterna** i EU:s stadga om de grundläggande rättigheterna och Europeiska konventionen om skydd för de mänskliga rättigheterna. Särskild uppmärksamhet måste fästas vid skyddet av personuppgifter och rätten till privatliv. Eftersom användning av detektionstekniker vanligtvis innebär ett intrång i den grundläggande rätten till privatliv och skydd av personuppgifter, måste alla sådana intrång vara i överensstämmelse med Europeiska konventionen om skydd för de mänskliga

² Europaparlamentets och rådets förordning (EG) nr 2320/2002 av den 16 december 2002 om införande av gemensamma skyddsregler för den civila luftfarten, EGT L 355, 30.12.2002, s. 1 och kommissionens förordning (EG) nr 622/2003 av den 4 april 2003 om åtgärder för att genomföra gemensamma grundläggande standarder avseende luftfartsskydd, EUT L 89, 5.4.2003, s. 9.

rättigheterna; de måste i synnerhet överensstämma med lagen och vara nödvändiga i ett demokratiskt samhälle för att skydda ett viktigt allmänt intresse samt stå i proportion till det allmänna intresse som skall skyddas.

I. STANDARDISERING OCH SÄKERHETSFORSKNING

1. STANDARDISERING

Det finns ett mycket stort utbud av tekniska möjligheter i fråga om detektionstekniker och säkerhetsmyndigheternas arbete. Det krävs därför minimistandarder. Med hänsyn till att det finns så många olika möjligheter måste man dock göra prioriteringar i standardiseringsprocessen, vilket endast är möjligt om det finns ett tillräckligt samspel mellan den offentliga sektorn (behov) och den privata sektorn (lösningar). Både den offentliga och den privata sektorn anser att detta samspel är otillräckligt på EU-nivå. Vidare håller en rad positiva åtgärder på att utvecklas på både nationell nivå och EU-nivå. Det saknas en allmän översikt över vad som händer, vilket behövs för att man skall kunna undvika dubbelarbete och förbättra prioriteringen. Det är naturligt att utvecklingen av standarder av säkerhetsskäl inte kan diskuteras öppet. Diskussionen kommer därför att inriktas främst på frågan om i vilken utsträckning det är önskvärt med gemensamma standarder.

Användning och hantering av uppgifter och information som inhämtas med hjälp av detektionsverktyg, till exempel som bevis i en rättegång, har också ett nära samband med standardisering. De relevanta myndigheterna skulle kunna dra nytta av att bästa metoder fastställs och utbyts på området. Det bör också övervägas om man skall skapa tekniska standarder för att se till att de inhämtade uppgifterna iakttar kraven i lagstiftning om användningen av sådana uppgifter i domstolsförfaranden³.

Frågor

Behövs det gemensamma standarder för de detektionstekniker som säkerhetsmyndigheter använder i sitt arbete? Vilka standarder anser ni bör ges prioritet?

Vilka standarder ges inte ekonomiskt stöd i skedet före standardisering?

För att undvika dubbelarbete och förbättra öppenheten, vore det användbart med en regelbundet uppdaterad förteckning/handbok/sökbar databas över tidigare, pågående och planerat standardiseringsarbete på området för detektionsteknik och nära relaterad teknik på nationell och europeisk nivå?

Skulle ni vara intresserade av att fastställa och utbyta bästa metoder för användning och hantering av uppgifter och information som samlats in med hjälp av detektionsverktyg, i ett försök att uppnå en fullständig överensstämmelse med lagstiftning och andra regler för användning av bevis i domstolsförfaranden?

Hur kan man bäst fastställa och utbyta bästa metoder?

³

Angående lagbestämmelser om utbyte av personuppgifter, se del II i bilagan.

2. SÄKERHETSFORSKNING

Säkerhetsforskning är ett annat område som är av vikt för utvecklingen av nya säkerhetslösningar och -produkter för medlemsstaternas säkerhetsmyndigheter. I detta sammanhang måste betydelsen av Europeiska säkerhetsforskningsrådet (ESRAB) framhävas. ESRAB har ett globalt och brett perspektiv på detta område och ger kommissionen råd i fråga om innehåll och genomförande av forskning som skall utföras och om ordningar för att övervaka relevant utveckling i andra program.

Det pågår en rad forskningsprojekt i fråga om säkerhet på Europainivå och i medlemsstaterna. Det finns dock inte någon mekanism för att samla ihop och sprida information om tidigare företagen, pågående och föreslagna säkerhetsforskning på EU-nivå, på nationell nivå eller inom den privata sektorn. En sådan mekanism skulle kunna säkra att de knappa resurserna inte slösas bort på dubbelarbete och överlappande projekt. Om det anses vara nödvändigt skulle man även kunna utforma en separat mekanism för att ge spridning åt sekretessbelagd säkerhetsforskning, som säkerställer att informationen endast kan åtkommas av dem som har rätt att få tillgång till den.

Efter över ett års arbete håller ESRAB på att färdigställa sin rapport, som kommer att offentliggöras i september 2006. I rapporten identifieras omkring 120 säkerhetsmöjligheter och 100 nyckeltekniker som kräver ytterligare forskning och utveckling på EU-nivå, medan en rad andra tekniker håller på att behandlas eller kommer att behandlas på nationell nivå.

Fråga

Hur kan man sprida information om säkerhetsforskning i Europa för att främja konkurrenskraften och samtidigt undvika slöseri av knappa resurser?

II. BEHOV OCH LÖSNINGAR

1. TEKNISKA BEHOV OCH LÖSNINGAR

Bra, effektiva och användbara lösningar och produkter kan endast utvecklas om tillverkarna har tillräcklig information om slutanvändarnas verkliga behov. Det verkar finnas ett behov av ett bättre samspel på EU-nivå mellan de som behöver tekniska lösningar (dvs. de relevanta säkerhetsmyndigheterna) och de som erbjuder lösningarna. Ett sådant samspel bör också innebära att man försöker identifiera behoven på kort, medellång och lång sikt. Å andra sidan bör de som tillhandahåller lösningar också ange inom vilka tidsramar de kommer att finnas tillgängliga.

I dialogen mellan producenter och användare bör man även ställa och besvara mera grundläggande frågor kring våra samhällens karaktär och betydelsen av detektionstekniker. En sådan debatt är också viktig när det gäller att bevara våra samhällens värderingar och karaktär.

Frågor

Är ni intresserade av en bredare debatt om detektionsteknikers roll och den påverkan användningen av dem kan ha på det europeiska samhället?

På vilka särskilda områden behöver de relevanta säkerhetsmyndigheterna tekniska förbättringar? Ange hur högt de särskilda behoven prioriteras.

Finns det ett glapp mellan behoven av detektionskapacitet och den teknik som för närvarande erbjuds på marknaden? Hur kan man lösa det problemet?

På vilka specifika områden erbjuder den privata sektorn redan, eller planerar att erbjuda, tekniska lösningar? Ange inom vilka tidsramar sådana lösningar kommer att finnas tillgängliga och vara kostnadseffektiva.

Skulle det vara användbart att upprätta en EU-omfattande sökbar förteckning eller databas över de specifika behoven hos de relevanta säkerhetsmyndigheterna och över de lösningar som erbjuds av den privata sektorn?

Om inte, vilken annan lösning skulle ni föreslå för att förbättra informationsflödet mellan de som behöver tekniska lösningar och de som erbjuder dem?

1.1 Mångsidiga lösningar

Dagens hot från brottslighet och terrorism är av olika slag. Hoten ändras hela tiden och förekommer i olika former och på olika nivåer i olika situationer. De kräver därför olika nivåer av skydd och reaktion vid olika tidpunkter, dvs. det behövs mångsidiga lösningar.

Frågor

Vilka befintliga verktyg och utrustningar skulle kunna göras mer mångsidiga och därmed mer användbara och effektiva?

Vilka nya mångsidiga verktyg och utrustningar behövs?

1.2 Bärbara och mobila lösningar

Hoten från terrorism och annan brottslighet inte bara ändras med tiden utan blir också allt mer mobila. Säkerhetsmyndigheter behöver därför bärbara lösningar. Sådana lösningar kan öka kostnadseffektiviteten och kan lätt flyttas från en plats till en annan där de behövs bäst, vilket är nödvändigt eftersom det helt enkelt inte är möjligt att täcka alla platser eller problemområden med samma nivå av säkerhet. Bärbara och mobila lösningar kan vidare erbjuda nya operativa strategier.

Frågor

Vilka befintliga verktyg och utrustningar skulle kunna användas bättre och effektivare i de relevanta säkerhetsmyndigheternas arbete om de vore mobila och bärbara?

Vilka nya bärbara och mobila verktyg och utrustningar behövs?

2. DRIFTSKOMPATIBILITET MELLAN SYSTEM⁴

EU:s medlemsstater och deras relevanta myndigheter har redan ett antal system som hjälper dem i kampen mot brottslighet och terrorism. Systemen kan dock ofta inte kommunicera med varandra. Detta kan vara ett hinder för arbetet med att bekämpa brottslighet och terrorism på nationell nivå och EU-nivå. Å andra sidan måste systemen iakttä gällande lagstiftning och andra riktlinjer (t.ex. om uppgiftsskydd och om detektionssystemers intrång i privatlivet).

Frågor

Vilka system behöver göras mer kompatibla sinsemellan?

Skulle det vara användbart med en studie över rättsliga och andra hinder för systemens kompatibilitet inom EU för att identifiera vilka begränsningar som finns?

3. INTEGRATION AV INFORMATION FRÅN OLIKA DETEKTIONSTEKNIKER OCH FÖRBÄTTRAD DATAANALYS

Detektionssystemen kan göras effektivare om uppgifter som erhålls med hjälp av olika detektionstekniker integreras i ett enda dataanalyssystem. Alla sådana åtgärder måste följa reglerna om uppgiftsskydd.

⁴ Även andra system än informationssystem.

Frågor

På vilka områden anser ni att det skulle förbättra det samlade resultatet om man integrerade information från olika detektionstekniker?

På vilka områden behövs det förbättrade tekniker för dataanalys?

III. ANVÄNDNING OCH CERTIFIERING AV UTRUSTNING OCH VERKTYG

1. BÄSTA METODER OCH ANVÄNDNING AV BEFINTLIGA VERKTYG OCH UTRUSTNING

Det behövs inte alltid helt nya tekniska lösningar för att effektivt bemöta befintliga eller nya hot. Staterna har ofta inte råd med sådana lösningar. Man bör därför också överväga hur befintliga och tidigare inköpta verktyg kan användas effektivare eller uppgraderas. Detta kan vara ett kostnadseffektivt sätt att öka deras effektivitet och tillförlitlighet och minska antalet falska alarm.

Det finns inte någon mekanism för att utbyta erfarenheter om sådana frågor mellan myndigheter i olika medlemsstater. Man skulle till exempel kunna utbyta information om förbättringar som uppnåtts genom ändringar i driftsmetoder eller kostnadseffektiva uppgraderingar.

Frågor

Vilket vore det bästa sättet att fastställa och utbyta bästa metoder på detta område?

Fastställande av bästa metoder

Skulle det bästa sättet vara inbördes utvärdering (*peer evaluation*) eller frågeformulär som skickas ut till medlemsstaterna?

Spridning av bästa metoder

Skulle det ske genom en säker och sökbar databas eller genom möten och seminarier?

Har ni några andra förslag om hur man på bästa sätt kan fastställa och sprida bästa metoder på detta område?

Om det bedöms nödvändigt att uppgradera ett verktyg eller utrustning och ingen myndighet i någon annan medlemsstat har företagit en sådan uppdatering, skulle det vara acceptabelt att rådgöra med den privata sektorn om det?

2. FASTSTÄLLANDE OCH SPRIDNING AV BÄSTA METODER OCH ANVÄNDNING AV NYA VERKTYG OCH NY UTRUSTNING

Nationella myndigheter kan också i sitt arbete ha nytta av ett system som skulle underlätta informationsutbytet om användning av nya verktyg och ny utrustning och ge dem möjlighet att lära av varandra och bygga vidare på varandras erfarenheter. Sådant utbyte av information, erfarenheter och bästa metoder om verktyg och utrustning skulle kunna vara en hjälp för myndigheterna att identifiera vilken utrustning de behöver för sina specifika behov.

Förutom detta skulle provning av ny eller experimentell utrustning kunna främjas genom samfinansiering från gemenskapsbudgeten och/eller av den privata sektorn. En mer

omfattande provning av ny och experimentell utrustning skulle kunna hjälpa det europeiska näringslivet att omvandla säkerhetsforskning till effektiva och konkurrenskraftiga produkter.

Frågor

Vilket vore det bästa sättet att fastställa och utbyta information och bästa metoder på detta område?

Fastställande av bästa metoder

Skulle det bästa sättet vara inbördes utvärdering (*peer evaluation*) eller frågeformulär som skickas ut till medlemsstaterna?

Spridning av information och bästa metoder

Skulle det ske genom en säker och sökbar databas eller genom slutna möten och seminarier?

Har ni några andra förslag om hur man kan fastställa och effektivt sprida bästa metoder på detta område?

Experimentella och nya verktyg

Är ni intresserade av provning av nya eller experimentella verktyg och utrustningar?

Om ja, utveckla svaret.

Skulle delvis finansiering av provning av nya eller experimentella verktyg och utrustningar av gemenskapen och/eller den privata sektorn vara av intresse?

3. ANVÄNDNING AV VERKTYG FÖR DATA- OCH TEXTUTVINNING

Nationella och europeiska säkerhetsmyndigheter står inför en ständig ökning av den mängd dokumentation och information de måste bearbeta. För att klara av denna utmaning på ett effektivare sätt finns det modern mjukvara för data- och textutvinning. Med sådan teknik kan man ta ut relevant information från enorma mängder dokument. Det är till exempel möjligt att på ett intelligent sätt filtrera text och dokument för att stödja navigering (gruppering av dokument), för automatisk kategorisering (kanalisering och prioritering av dokumentflödet inom utredningsgrupper) och för valideringskontroll av kodanvändning. Målen är följande:

- Snabb överblick över nyckelenheter i dokumentsamlingar.
- Föregående bearbetning för målinriktad dokumentsökning.
- Innehållsbaserad klassificering av dokument i syfte att bestämma inriktningen på vidare analyser.
- Automatisk informationsanalys via olika källor.

Dessa moderna verktygs potential utnyttjas inte i tillräcklig utsträckning i medlemsstaterna. När man verkar för användning av dessa tekniker måste man dock vara uppmärksam på att de när de används i vissa tillämpningar, t.ex. för att övervaka e-post, i sig själva utgör ett intrång

i medborgarnas grundläggande rätt till privatliv. E-post är korrespondens och omfattas därmed av den rätt till skydd för korrespondens som föreskrivs i Europeiska konventionen om skydd för de mänskliga rättigheterna. Användningen av olika tekniker för data- och textutvinning måste överensstämma med lagen och vara nödvändiga i ett demokratiskt samhälle för att skydda ett viktigt allmänt intresse samt stå i proportion till det allmänna intresse som skall skyddas. Sådana verktyg och användningen av dem bör alltid grunda sig på en överensstämmelse med de grundläggande rättigheterna och principerna för uppgiftsskydd. Denna verksamhet kommer slutligen att utföras under relevanta offentliga myndigheters kontroll och överinseende.

Frågor

Informationsinsatser

Skulle medlemsstaterna och de relevanta EU-organen vara intresserade av utbyte av bästa metoder och av de potentiella fördelarna av användningen av verktyg för data- och textutvinning?

Skulle de myndigheter i medlemsstaterna som använder denna teknik vara beredda att utbyta erfarenheter med sina kolleger?

Skulle det vara meningsfullt med slutna seminarier i denna fråga som organiseras av medlemsstaterna, Europol eller OLAF?

Ökning av EU:s kapacitet för data- och textutvinning

Skulle ett expertiscentrum på EU-nivå, som är alla medlemsstater och deras relevanta myndigheter får tillgång till, bidra till att man utnyttjade dessa verktygs potential i praktiken?

Om inte, vilka andra alternativ föreslår ni för att maximera dessa verktygs potential?

Fastställande och spridning av bästa metoder

Skulle inbördes utvärdering (*peer evaluation*) eller frågeformulär som skickas ut till medlemsstaterna vara användbart för att fastställa bästa metoder för användningen av dessa verktyg?

Om inte, på vilka andra sätt föreslår ni att man fastställer bästa metoder på detta område?

Ökning av den regionala kapaciteten för data- och textutvinning

Har medlemsstaternas och EU:s organ någon ledig kapacitet för att hjälpa medlemsstater som inte har denna teknik att arbeta med sina dokument?

Om det inte finns någon sådan ledig kapacitet, eller bara begränsad kapacitet, skulle det vara användbart och praktiskt med en EU-finansierad ökning av kapaciteten i medlemsstaterna eller på EU-nivå?

Skulle medlemsstater som saknar tillräcklig kapacitet för data- och textutvinning överväga att använda andra organs verktyg om de hölls tillgängliga?

Skulle det vara möjligt att skapa europeiska eller regionala centrum för data- och textutvinning som flera medlemsstater och deras myndigheter kan använda sig av?

Täcker de befintliga data- och textutvinningsverktygen i tillräcklig mån de olika språken i Europa?

Finns det lämpliga verktyg till hjälp för myndigheter som behandlar text och dokument som är skrivna på främmande språk?

Andra uppgifter

Om ni inte håller med om ett eller flera av de alternativ som föreslås ovan, hur skulle ni vilja lösa de problem som tagits upp i denna punkt?

4. PROVNING OCH CERTIFIERING AV UTRUSTNINGARS OCH VERKTYGS KVALITET

Det finns redan ett antal olika detektionsprodukter på marknaden. Det är dock ofta svårt att identifiera vilka verktyg och produkter som är bäst eller åtminstone uppfyller vissa minimikriterier. Detta problem skulle kunna lösas genom ett EU-omfattande system för certifiering och riktmärkning (*benchmarking*) av verktyg av god kvalitet, som är utformat för att förenkla förfarandet för att fastställa vilka verktyg eller utrustningar som kan tillgodose de specifika behoven för en viss myndighet. Det kan göra det lättare för nationella myndigheter att besluta vilka verktyg och vilken utrustning de skall köpa. Det kan också hjälpa myndigheterna att använda knappa resurser på bästa sätt.

Ett nätverk av *nationella* certifieringsmyndigheter som utbyter erfarenheter och kunskaper skulle kunna upprättas för att avhjälpa problemet att det saknas ett system för att avgöra verktygens kvalitet. Dessa myndigheter skulle också komma överens om standarder för riktmärkning och certifiering av högkvalitativa tekniska lösningar. Denna typ av certifiering kan användas inte bara för att hjälpa nationella myndigheter att avgöra om ett verktyg är bra eller inte, utan även för att göra reklam för europeiska lösningar på andra marknader. Det är naturligt att utvecklingen av testprotokoll av säkerhetsskäl inte kan diskuteras öppet.

Frågor

Skulle det vara användbart att skapa ett nätverk med nationella certifieringsmyndigheter som utbyter erfarenheter och kunskaper, och ett system för kvalitetscertifiering och riktmärkning?

Om inte, vilka andra lösningar föreslår ni för att lösa detta problem?

Skulle gemensamma standarder för certifiering och riktmärkning vara till nytta?

Om inte, hur anser ni att man kan garantera en öppen process med resultat som kan användas i hela EU?

IV. UNDERSÖKNINGAR⁵

Deltagarna i konferensen identifierade flera frågor som behöver undersökas ytterligare. Kommissionen föreslår således att det genomförs undersökningar om

- (1) teknik och skydd av masstillställningar,
- (2) hinder för samarbete och informationsutbyte bland kriminaltekniska laboratorier och institut för säkerhetsforskning,
- (3) lagbestämmelser som reglerar användningen av specifik detektionsteknik,
- (4) praktisk användning av specifik detektionsteknik,
- (5) den rättsliga ram som reglerar användningen av persondetektion (även övervakning) i hela EU,
- (6) graden av acceptans för persondetektion (även övervakning och användning av biometri) i hela EU.

Generellt är undersökningarnas syfte att man skall kunna använda dem för att öka de berörda parternas kunskaper och säkra att befintliga lagregler iakttas när detektionstekniker utarbetas eller används. I andra fall kan undersökningarna användas för att överväga olika policyalternativ och olika alternativ till fortsatta åtgärder.

Fråga

Skulle ni vara intresserade av att få ta del av undersökningar om dessa frågor som bygger på den bakgrundsinformation som finns i bilagan?

Om inte, ange skälen för det och föreslå hur man på annat sätt kan hantera de nämnda problemen.

⁵

För en närmare beskrivning av idéerna bakom behovet av dessa undersökningar, se del III i bilagan.

V. GENOMFÖRANDE AV RESULTATEN AV SAMRÅDET

1. BÄTTRE SPECIFIK DIALOG MELLAN DEN OFFENTLIGA OCH DEN PRIVATA SEKTORN OM DETEKTIONSTEKNIKER OCH RELATERADE TEKNIKER

Denna grönbok tar upp en rad möjliga verksamheter som kan bidra till att förbättra samspelet mellan den offentliga och den privata sektorn på området för detektionstekniker och därmed hjälpa säkerhetsmyndigheter i medlemsstaterna att få tillgång till bästa möjliga verktyg, lösningar och bästa metoder. Samtidigt kan dessa verksamheter hjälpa den privata sektorn att inrikta sina investeringar och svara mot den offentliga sektorns behov. Det är dock tydligt att detta kräver ett intensivt samarbete mellan den offentliga och den privata sektorn. Det finns därför ett behov av en större, specifik offentlig-privat dialog på detta område. Detta skulle kunna uppnås på olika sätt, bland annat genom att man upprättar ett specifikt organ eller en specifik grupp inom ramen för horisontellt arbete inom offentlig-privata partnerskap som avser säkerhet, vilka bör inledas inom en nära framtid.

Syftet med en sådan verksamhet skulle inte vara att konkurrera med befintliga organ utan att ta itu med luckor i samspelet mellan den offentliga och privata sektorn med deltagande av relevanta säkerhetsmyndigheter på EU-nivå. Det skulle inte heller vara ett permanent organ; det skulle ha klart definierade mål och det skulle upphöra att finnas när dessa mål har uppnåtts. Det skulle fungera som ett forum för experter från såväl den offentliga som den privata sektorn och bidra till att lösa de problem som har tagits upp i denna grönbok eller nya utmaningar som kan uppkomma under genomförandet av resultaten från det offentliga samrådet om grönboken.

Det står dock även klart att ett antal av de möjliga åtgärder som föreslås i detta dokument skulle kräva att medlemsstaterna vidtog åtgärder utan inblandning av den privata sektorn. Dessutom skulle den offentliga och den privata sektorn komma överens om definitionen av uppdragen i ett sådant samarbete, och medlemsstaterna skulle således genom sitt medlemskap kunna påverka dess roll och inriktning. Inom ramen för detta samarbete skulle man också behöva ta upp frågan om utbyte av sekretessbelagd information mellan den offentliga och den privata sektorn, även om det bör understrykas att den offentliga sektorn inte är ensam om att förvara känsliga uppgifter.

Frågor

Skulle ett verktyg som en förstärkt offentlig-privat dialog om detektionstekniker och relaterade tekniker vara till hjälp vid genomförandet av resultaten av det offentliga samrådet om denna grönbok?

Om ja, håller ni med om ovannämnda förslag eller har ni några andra idéer?

Om nej, vilka andra mekanismer skulle ni föreslå för att följa upp resultaten av det offentliga samrådet om denna grönbok?

Skulle ni vara intresserade av att bidra till detta arbete eller att delta i det direkt?

2. HANDLINGSPLAN

På nationell nivå och EU-nivå har handlingsplaner visat sig vara ett framgångsrikt redskap för att övervaka verksamheten på komplexa områden, t.ex. kampen mot terrorism och annan brottslighet. Både vid konferensen och i detta dokument har det ställts ett stort antal frågor om detektionstekniker och relaterade tekniker i de relevanta säkerhetsmyndigheternas arbete. För att övervaka framstegen på området och fastställa målsättningar skulle man kunna utarbeta en handlingsplan som bygger på svaren på frågorna och, om nödvändigt, på ytterligare samråd.

Fråga

Skulle en handlingsplan vara ett användbart verktyg för att genomföra de åtgärder som kommer att identifieras i svaren på denna grönbok?

Avslutande anmärkningar

Svaren på denna grönbok skall senast den 10 januari 2007 sändas elektroniskt till följande adress: **JLS-D1-Detection@ec.europa.eu**. Alla svar från både den offentliga och den privata sektorn kommer att offentliggöras på kommissionens webbplats, om inte de som svarar uttryckligen anger att de vill att viss information skall vara konfidentiell.

ANNEX

I. BACKGROUND INFORMATION ON THE PREPARATION OF THE GREEN PAPER

This Green Paper is based on the results of the conference and raises themes and issues that featured prominently in the discussions (e.g. standardisation, security research, improvement of technological solutions, protection of privacy, the legal framework and other guidelines by which technologies have to abide, etc.). Over one hundred participants from business, industry and the public sector engaged in the debate. The public sector was represented by the members of law enforcement, customs and other security authorities, by the Commission and by representatives of the Member States. The title of the conference suggests that it focused on the fight against terrorism. However, it became clear from the outset that a broader security approach was inevitable if important security concerns were not to be omitted. This broad approach was reaffirmed by the December 2005 Council decision to base European critical infrastructure protection on an 'all hazards' approach. Moreover, the conference took a holistic approach by bringing together stakeholders from different areas of expertise to discuss the following topics:

- Detection technologies in the protection of infrastructure
- Personal detection technologies and biometrics
- Detection of explosives and chemical, biological, radiological and nuclear (CBRN) substances.

All themes focused on the work of law enforcement, security and customs authorities. This approach enabled the conference to identify numerous areas of common concern for both public and private sectors (e.g. interaction between solution-providers and those who need solutions in the public sector). This is reflected throughout the document.

Definition of detection technologies and relevant categories

For the purposes of the consultation, the term 'detection technology' is used in the broadest sense. Detection technologies can be "in situ" or external and probably the more sophisticated means to deal with some of the security challenges in various scenarios are when integrated into the complex system (such as transport system). A detection technology can be almost anything used to detect something in a security or safety context, with the focus on law enforcement, customs or security authority. It is possible to identify several categories⁶ which, if taken into consideration when responding to the questions outlined in this document, may help to sharpen the answers:

- Hand-held detectors
- Detection portals
- Surveillance solutions

⁶ This is a non-exhaustive list of categories.

- Detection of biometrics
- Data- and text-mining tools
- Other software-based detection tools, etc.

Furthermore, respondents should also consider associated technologies when replying to the questions, as technologies which help humans to make sense of the data collected by the detectors are also important for effective solutions. Technology is needed to integrate solutions and to make systems interoperable. Despite having highlighted these categories, respondents should not feel constrained by them, and are encouraged to go beyond them.

II. STANDARDISATION AND THE EXCHANGE OF PERSONAL DATA

The Commission points out that, in terms of handling personal data, Directive 95/46/EC already provides the legal framework for exchange of information containing personal data in respect of activities relating to the "first pillar". As regards exchange of information as part of judicial and criminal cooperation, and under the principle of availability, the Commission has tabled a legislative proposal, which is under discussion.

III. STUDIES

1. Protection of mass events

Every year EU Member States organise several public mass events of national, European, but also of international importance. In today's security environment the costs of security for such events may take up a substantial part of their budgets. All Member States could benefit from a common approach to this problem.

To prepare the ground for eventual steps to be taken in this area, the Commission proposes to organise a study on the protection of mass events. The study would analyse what security tools, equipment and expertise applied in the protection of mass events are transferable from one event/site to another. The study would also consider the practicality and implications of Community-owned equipment, of Community-shared equipment, of developing a business model for services provided by the private sector or of a combination of all three approaches. This part of the study should determine which solution:

- is the most cost-effective and flexible enough to fit diverse needs of Member States;
- can ensure access to this solution by all Member States together with appropriate sharing of the costs by the Member States.

When the results of the study are ready, the Commission would consider further steps in this area in conjunction with the Member States and other relevant stakeholders.

2. Cooperation and information-sharing among forensic laboratories and security research institutes

The participants in the conference highlighted the fact that legal and other obstacles exist at national level which prevent effective cooperation and information-sharing among national forensic institutes at European level. Therefore, the Commission suggests conducting a study on the subject. This study could also address options for remedying the situation.

A similar concern was raised regarding cooperation and information exchange among security research institutes. A separate study addressing this issue could also be conducted.

3. Law and specific detection technology

Law enforcement, customs and other security authorities are often scrutinised for whether they comply with applicable legal standards. Even if the technology as such is not in breach of legal standards, the manner of its use may raise concerns. Accordingly, identifying the legal framework governing the use of, and setting limits for, technological solutions could help to raise greater awareness in both public and private sectors and facilitate compliance with existing standards. The private sector could also benefit from such a study when proposing and designing technological solutions and services for the public sector.

4. Specific detection technology and its practical use

Similarly, guidance and best practice in the use of technologies, particularly detection technologies, must take into account how users of these technologies actually use such tools in practice, and how they act in relation to persons subject to detection. A specific technology as such may not breach legal standards, but its real world use by an operator may raise concerns. In addition, the development of new technologies or the changing use of existing technologies may result in situations where a law regulating their use does not exist. Alternatively a particular use of a technology may not be in breach of the law, but it may run counter to best practice or codes of conducts developed to supplement legal provisions. Knowledge of regulations (instruments) in this area might provide guidance on whether they comply with the legal framework (in particular fundamental rights and data protection) and on what is acceptable or not in a situation where legal provisions have not been developed.

5. Personal detection technologies and biometrics

Personal detection (including surveillance) and biometrics are issues which affect individuals directly, and therefore a sensitive political debate is ongoing on the use of these tools for the purposes of improving security in Europe. The Commission suggests that a study should be undertaken to identify the legal framework governing personal detection technology and biometrics. This study would analyse the legal systems of the Member States and the EU and thereby establish what existing rules govern personal detection and biometrics. A study of this kind is particularly important when making technological solutions proposed by the private sector compliant with the law. In simple terms, it would help the private sector to understand the legal and other constraints on technological solutions they develop.

Special studies could also be drawn up on the levels of acceptance of surveillance and biometrics by the population in individual Member States and in the EU. The methodology of these studies would have to ensure that there is no confusion between the two subjects – surveillance and biometrics. Such studies could help the EU and national governments to deploy adequate communication strategies on these issues. In general, both studies would further contribute to the political debate in Europe on these important matters.