RAT DER EUROPÄISCHEN UNION

Brüssel, den 25. September 2006 (28.09) (OR. fr)

13183/06

JAI 464
ENFOPOL 160
MI 166

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission
Eingangsdatum:	4. September 2006
Empfänger:	der Generalsekretär/Hohe Vertreter, Herr Javier SOLANA
Betr.:	Grünbuch über Detektionstechnologien und ihre Anwendung durch Strafverfolgungs-, Zoll- und andere Sicherheitsbehörden

Die Delegationen erhalten in der Anlage das Kommissionsdokument - KOM(2006) 474 endgültig

---

Anl.: KOM(2006) 474 endgültig

KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 1.9.2006
KOM(2006) 474 endgültig

GRÜNBUCH

über Detektionstechnologien und ihre Anwendung durch Strafverfolgungs-, Zoll- und andere Sicherheitsbehörden

(von der Kommission vorgelegt)

INHALTSVERZEICHNIS

GRÜNBUCH

über Detektionstechnologien und ihre Anwendung durch Strafverfolgungs-, Zoll- und andere Sicherheitsbehörden

(Text von Bedeutung für den EWR)

EINLEITUNG

Sicherheit ist ein wesentlicher Aspekt der Kommissionspolitik, und ein entscheidender Bestandteil der Sicherheitspolitik ist die Bekämpfung von Terrorismus und Kriminalität. In ihrer Mitteilung vom Oktober 2004 „*Terroranschläge – Prävention, Vorsorge und Reaktion*" hat die Kommission ihre Strategie zur Bekämpfung des Terrorismus vorgestellt. Darin wird ein *öffentlich-privater Sicherheitsdialog* angeregt, in dessen Rahmen sich der öffentliche und der private Sektor konstruktiv mit der Frage auseinander setzen sollen, was für die Sicherheit in Europa getan werden muss. Der Interaktion von Staat und Gesellschaft im Kampf gegen den Terrorismus und die organisierte Kriminalität wird auch im *Haager Programm* des Europäischen Rates vom November 2004 *zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union*, große Bedeutung beigemessen. Das Haager Programm enthält die aktuellen politischen Vorgaben der Union für den Bereich Justiz und Inneres. Auf der Grundlage des vorliegenden Grünbuchs soll ein solcher Dialog im Bereich der Detektionstechnologien in Gang gebracht werden.

Detektionstechnologien finden zunehmend Eingang in die tägliche Arbeit der Sicherheitsbehörden in ihrem Kampf gegen Terrorismus und andere Formen der Kriminalität. Sie werden umfassend eingesetzt im Luftverkehr zum Schutz der Fluggäste oder bei Sportveranstaltungen zum Schutz der Zuschauer. Auch gefährliche Substanzen in der Luft, im Wasser oder in Nahrungsmitteln können mit diesen Techniken aufgespürt werden. Weitere Einsatzmöglichkeiten sind der Grenzschutz und die Kontrolle von Waren, bevor sie in das Gebiet der Europäischen Union gelangen. Unerlässlich sind Detektionstechnologien auch für den Schutz von Privateigentum und kritischen Infrastrukturen. In diesem Grünbuch wird der Frage nachgegangen, in welcher Weise die Europäische Union den Einsatz von Detektionstechnologien zum Schutz ihrer Bürger fördern kann. Diese Technologien sind jedoch so beschaffen, dass sie in die Privatsphäre eindringen und in Grundrechte und Grundfreiheiten eingreifen können. Wenn es deshalb um den Einsatz und die Verbesserung dieser Technologien geht, sollte und muss dieser Aspekt sowie die grundlegende Frage, wo die Grenzen ihrer Einsatzmöglichkeiten sind, jedes Mal sorgfältig geprüft werden. Mit ihrem Grünbuch will die Kommission einen Beitrag zu beiden Problemstellungen leisten.

Am 28./29. November 2005 veranstaltete die Kommission in Brüssel eine Konferenz zum Thema „Öffentlich-privater Sicherheitsdialog: Detektionstechnologien und ihre Anwendung im Kampf gegen den Terrorismus"[1]. Das Interesse an einer politischen Strategie in diesem Bereich zeigte sich an der großen Teilnehmerzahl: über hundert Vertreter aus der europäischen Wirtschaft, Industrieverbänden und dem öffentlichen Sektor waren zugegen.

[1] Näheres hierzu in Teil I des Anhangs.

Der öffentliche Sektor war durch Angehörige der Strafverfolgungs-, Zoll- und anderer Sicherheitsbehörden vertreten.

Dass Europa bei der Sicherheitsforschung und Normung eine wichtige Aufgabe zukommt, ist unbestritten. Zwar wurde in enger Zusammenarbeit mit den Mitgliedstaaten, der Industrie und anderen Beteiligten in diversen Bereichen schon einiges erreicht, aber bei den Detektionstechnologien besteht auf europäischer Ebene durchaus noch Handlungsbedarf. Im Bereich der Luftsicherheit enthalten die Verordnungen (EG) Nr. 2320/2002 und (EG) Nr. 622/2003[2] detaillierte Vorgaben für die zu verwendenden Sicherheitsausrüstungen und Verfahrensweisen. In enger Abstimmung mit der Europäischen Zivilluftfahrtkonferenz, der Sachverständige aus den Fachbehörden der EU-Mitgliedstaaten und anderer europäischer Staaten angehören, wurden Normen und Testprotokolle erstellt. Darüber hinaus steht die Kommission in engem Kontakt mit Vertretern aus Wirtschaft und Industrie und anderen Interessengruppen („Stakeholders Advisory Group on Aviation Security“ (SAGAS) - Beratungsgruppe der beteiligten Kreise zur Luftsicherheit).

Die Kommission hat jetzt die Initiative ergriffen, um mit vereinten Kräften bei den Detektionstechnologien voranzukommen und den öffentlichen und den privaten Sektor zu einer engeren Zusammenarbeit zu bewegen. Schwerpunkt sind die Bereiche Normung und Standardisierung, Forschung, Zertifizierung und Interoperabilität von Detektionssystemen, wobei es darauf ankommt, die Forschungsergebnisse einer zweckmäßigen, praktikablen Anwendung zuzuführen. Hier muss eine positive Interaktion einsetzen, bei der die Privatwirtschaft in Forschung und Finanzierung von einem öffentlichen Sektor unterstützt wird, der nicht nur weiß, was er will, sondern der auch weiß, was der private Sektor leisten kann. Damit ließe sich zur Entwicklung eines breiteren und damit letztlich auch kostengünstigeren Angebots an Detektionsprodukten und Sicherheitslösungen beitragen.

Ohne ein gemeinsames Vorgehen, eine bessere Koordination und ein besserer Informationsaustausch zwischen allen Beteiligten in Europa ist dieses Ziel aber nicht zu erreichen. Der Bedarf muss besser definiert werden, und es müssen Lösungen erarbeitet werden, die sowohl technisch als auch ökonomisch tragfähig sind. Mit diesem Grünbuch **soll keinesfalls in andere Unternehmungen auf nationaler oder europäischer Ebene eingegriffen werden**. Die Kommission will nicht das Rad neu erfinden, sondern mehr über bewährte Konzepte und Praktiken in Erfahrung bringen, sie fördern und in der EU verbreiten.

Die Kommission wünscht sich zu diesem Grünbuch möglichst viele konstruktive Beiträge und konkrete Vorschläge zum weiteren Vorgehen. **Eine breite Beteiligung der Mitgliedstaaten, der Privatwirtschaft sowie anderer Interessengruppen ist daher unerlässlich**. Sowohl aus sicherheitspolitischen als auch aus kommerziellen Erwägungen sind im öffentlichen wie im privaten Sektor bestimmte Aspekte vertraulich zu behandeln. In den Beiträgen zum Grünbuch sollten daher die Antworten kenntlich gemacht werden, die zu sensibel sind, als dass sie allen zugänglich gemacht werden könnten. Gleichzeitig sollten Alternativen vorgeschlagen werden, wie diesem Anliegen Rechnung getragen werden kann.

Politische Strategien, die sich mit Detektionstechnologien und ihrer Anwendung befassen, müssen mit den bestehenden Rechtsvorschriften einschließlich der Grundrechtscharta der EU,

---

[2] Verordnung (EG) Nr. 2320/2002 des Europäischen Parlaments und des Rates vom 16. Dezember 2002 zur Festlegung gemeinsamer Vorschriften für die Sicherheit in der Zivilluftfahrt, ABl. L 355 vom 30.12.2002, S. 1, und Verordnung (EG) Nr. 622/2003 der Kommission vom 4. April 2003 zur Festlegung von Maßnahmen für die Durchführung der gemeinsamen grundlegenden Normen für die Luftsicherheit, ABl. L 89 vom 5.4.2003, S. 9.

der Europäischen Menschenrechtskonvention und den Datenschutzgrundsätzen und –bestimmungen der Richtlinie 95/46/EG in vollem Umfang vereinbar sein. In diesem Zusammenhang weist die Kommission darauf hin, dass bei der Konzeption, der Realisierung und dem Einsatz solcher Technologien sowie bei den Rechtsvorschriften und Maßnahmen, mit denen diese Technologien gefördert und geregelt werden sollen, **die Grundrechte**, wie sie in der EU-Grundrechtscharta und in der Menschenrechtskonvention niedergelegt sind, **uneingeschränkt zu beachten sind**. Der Schutz personenbezogener Daten und das Recht auf Achtung des Privatlebens verdienen besondere Beachtung, da Detektionstechnologien in der Regel einen Eingriff in das Grundrecht auf Achtung der Privatsphäre und auf Schutz personenbezogener Daten bedeuten und jeder Eingriff in die Grundrechte mit der Europäischen Menschenrechtskonvention vereinbar sein muss. Insbesondere müssen solche Eingriffe in einer demokratischen Gesellschaft gesetzmäßig sein, zum Schutz eines übergeordneten öffentlichen Interesses erforderlich sein und im Verhältnis zum angestrebten Ziel stehen.

I. NORMUNG, STANDARDISIERUNG UND SICHERHEITSFORSCHUNG

1. NORMUNG UND STANDARDISIERUNG

In sicherheitsrelevanten Bereichen besteht eine enorme Bandbreite an Einsatzmöglichkeiten für Detektionstechnologien und damit zusammenhängende Technologien. Mindeststandards sind daher erforderlich. Angesichts der breiten Einsatzmöglichkeiten müssen Normung und Standardisierung Vorrang erhalten. Dies ist aber nur möglich, wenn ein gewisser Austausch zwischen dem öffentlichen Sektor (Bedarf) und dem privaten Sektor (Anwendungslösungen) stattfindet. Dieser Austausch wird auf europäischer Ebene sowohl vonseiten des öffentlichen als auch des privaten Sektors als unzureichend angesehen. In diesem Bereich laufen zudem zahlreiche Arbeiten sowohl auf nationaler als auch auf europäischer Ebene. Um Doppelaufwand zu vermeiden und Prioritäten besser setzen zu können, bedarf es eines allgemeinen Überblicks über die laufenden Aktivitäten, an dem es jedoch noch fehlt. Die Ausarbeitung von Normen und Standards in diesem Bereich kann aus Sicherheitsgründen selbstverständlich nicht in aller Öffentlichkeit erörtert werden. Die Diskussion wird sich deshalb in erster Linie auf die Frage konzentrieren, inwieweit gemeinsame Normen und Standards von Vorteil sein können.

Eng mit Normung und Standardisierung verbunden ist auch der Einsatz und Umgang mit Daten und Informationen, die mit Hilfe von Detektionstechniken erhoben wurden (z. B. Verwendung als Beweismittel vor Gericht). Die Festlegung und Verbreitung bewährter Praktiken könnte sich für die zuständigen Behörden als nützlich erweisen. Zu erörtern wäre auch die Ausarbeitung von Normen und Standards, die gewährleisten, dass die erhobenen Daten den gesetzlichen Anforderungen an die Verwendung dieser Daten vor Gericht genügen[3].

Fragen

Sind für die von den Sicherheitsbehörden eingesetzten Detektionstechnologien einheitliche Normen und Standards erforderlich? Welche Standards und Normen halten Sie für vorrangig?

Bei welchen Standards und Normen fehlt es in der Entwicklungsphase an finanziellen Mitteln?

Wäre ein regelmäßig aktualisiertes Verzeichnis/Handbuch oder eine abfragbare Datenbank mit den auf nationaler und europäischer Ebene geplanten, laufenden und abgeschlossenen Normungs-/Standardisierungsarbeiten im Bereich der Detektionstechnologien und anderer damit eng verbundener Techniken im Interesse der Transparenz und um Doppelarbeit zu vermeiden nützlich?

Wären Sie daran interessiert, bewährte Praktiken für den Einsatz und den Umgang mit Daten und Informationen, die mit Hilfe von Detektionstechniken erhoben wurden, zu ermitteln und auszutauschen, um auf diese Weise den einschlägigen Rechtsvorschriften und Regeln für die Verwendung von Beweismitteln vor Gericht in vollem Umfang genügen zu können?

[3] Siehe Teil II des Anhangs zu den Rechtsvorschriften für den Austausch personenbezogener Daten.

Wie ließen sich solche Praktiken am besten erfassen und austauschen?

2. SICHERHEITSFORSCHUNG

Ein anderer Bereich, der für die Entwicklung neuer Sicherheitslösungen und –produkte für die mitgliedstaatlichen Behörden von grundlegender Bedeutung ist, ist die Sicherheitsforschung. Hier ist auf die Rolle des Europäischen Beirats für Sicherheitsforschung (ESRAB) hinzuweisen. ESRAB legt allgemeine Forschungsperspektiven in diesem Bereich fest und berät die Kommission zum Inhalt und zur Durchführung der Forschungsagenda. Gleichzeitig sorgt der Beirat dafür, dass sicherheitsrelevante Entwicklungen in anderen Programmen verfolgt werden.

In der Sicherheitsforschung sind auf europäischer Ebene und in den Mitgliedstaaten diverse Arbeiten im Gange. Es gibt jedoch kein Instrumentarium, um Informationen über geplante, laufende und abgeschlossene Forschungsarbeiten auf europäischer, nationaler und letztlich privatwirtschaftlicher Ebene zusammenzufassen und zu verbreiten. Mit einem entsprechenden Verfahren könnte sichergestellt werden, dass knappe Ressourcen nicht für Doppelarbeit und sich überschneidende Projekte verschwendet werden. Erforderlichenfalls könnte auch ein separates Verfahren für die Verbreitung vertraulicher Forschungsarbeiten eingerichtet werden, um zu gewährleisten, dass nur Zugangsberechtigte auf diese Arbeiten zugreifen können.

Nach über einjähriger Tätigkeit wird der Beirat jetzt im September 2006 seinen Tätigkeitsbericht herausgeben. In dem Bericht werden etwa 120 Sicherheitskompetenzen und 100 Schlüsseltechnologien genannt, bei denen auf EU-Ebene weitere Forschungs- und Entwicklungsarbeiten erforderlich sind. Andere Technologien sollen oder werden bereits auf nationaler Ebene entwickelt.

Frage

Wie sollen Informationen im Bereich der Sicherheitsforschung in Europa verbreitet werden, um die Wettbewerbsfähigkeit zu fördern, gleichzeitig aber auch der Verschwendung knapper Ressourcen zu begegnen?

II. BEDARF UND LÖSUNGEN

1. BEDARF UND LÖSUNGEN AUS TECHNOLOGISCHER SICHT

Die Entwicklung guter, effizienter und brauchbarer Lösungen und Produkte setzt voraus, dass die Hersteller über ausreichende Informationen darüber verfügen, welcher Bedarf bei den Endnutzern tatsächlich besteht. Auf europäischer Ebene sieht es so aus, als wäre ein besserer Austausch zwischen denjenigen, die technologische Lösungen brauchen (d. h. den Sicherheitsbehörden), und denjenigen, die solche Lösungen anbieten, erforderlich. Ein solcher Austausch sollte auch auf die Ermittlung des kurz-, mittel- und langfristigen Bedarfs gerichtet sein. Dabei sollten diejenigen, die Sicherheitslösungen anbieten, gleichzeitig angeben, wann ihre Produkte voraussichtlich verfügbar sein werden.

Im Dialog zwischen Herstellern und Nutzern sollten aber auch Fragen grundsätzlicherer Art über das Wesen unserer Gesellschaft und die Rolle der Detektionstechnologien zur Sprache kommen. Ein solcher Austausch ist nicht zuletzt für den Erhalt der Werte unserer Gesellschaft wichtig.

Fragen

Sind Sie an einer breiteren Debatte über die Rolle der Detektionstechnologien und ihren möglichen Einfluss auf die europäische Gesellschaft interessiert?

In welchen konkreten Bereichen sind für die Sicherheitsbehörden technologische Verbesserungen erforderlich? Geben Sie bitte die Prioritätsstufe des jeweiligen konkreten Bedarfs an.

Besteht eine Diskrepanz zwischen den erforderlichen Detektionskapazitäten und der derzeit auf dem Markt angebotenen Technologie? Welche Lösungsmöglichkeiten gibt es, um diese Diskrepanz zu beseitigen?

Für welche konkreten Bereiche plant die Privatwirtschaft, technologische Lösungen anzubieten, oder bietet sie bereits an? Geben Sie bitte an, wann kostengünstige Lösungen zur Verfügung stehen werden.

Wäre es nützlich und hilfreich, auf EU-Ebene eine abrufbare Liste/Datenbank einzurichten, die Aufschluss über den konkreten Bedarf der Sicherheitsbehörden und gleichzeitig über das Angebot des privaten Sektors gibt?

Falls nein, welche anderen Lösungen würden Sie vorschlagen, um den Informationsfluss zwischen denen, die technische Lösungen nachfragen, und denjenigen, die solche Lösungen anbieten, zu verbessern?

1.1 Vielseitige Lösungen

Wir sind heute vielfältigen, ständig wechselnden und in verschiedenen Formen, auf verschiedenen Ebenen und in verschiedenen Situationen präsenten Bedrohungen durch Kriminalität oder Terrorismus ausgesetzt. Diese Bedrohung erfordert deshalb zu

verschiedenen Zeiten ein unterschiedliches Schutzniveau und eine unterschiedliche Reaktion, d. h. vielseitige Lösungen.

Fragen

Bei welchen vorhandenen Ausrüstungen und Instrumenten könnten Verwendbarkeit und Effizienz durch Erweiterung ihrer Einsatzmöglichkeiten verbessert werden?

Welche neuen, vielseitig einsetzbaren Instrumente und Ausrüstungen sind erforderlich?

1.2 Tragbare, mobile Lösungen

Die Bedrohung durch Terrorismus und Kriminalität verändert sich nicht nur im Laufe der Zeit, sondern wird zunehmend mobiler. Die Sicherheitsbehörden verlangen entsprechend mobile Lösungen. Sicherheitsprodukte, die problemlos an einen anderen Ort gebracht werden können, wo sie am dringendsten gebraucht werden, können sich als kostengünstiger erweisen, da es ganz einfach nicht möglich ist, jeden sicherheitskritischen Ort mit der gleichen Sicherheitsstufe abzuschirmen. Tragbare, mobile Lösungen können ein neues operatives Vorgehen ermöglichen.

Fragen

Welche vorhandenen Instrumente und Ausrüstungen könnten besser und effizienter von den Sicherheitsbehörden eingesetzt werden, wenn sie mobil und tragbar wären?

Welche neuen tragbaren, mobilen Instrumente und Ausrüstungen sind erforderlich?

2. INTEROPERABILITÄT DER SYSTEME[4]

Die EU-Mitgliedstaaten und ihre Behörden verfügen bereits über eine Reihe von Systemen, die sie im Kampf gegen Terrorismus und Kriminalität unterstützen. Diese Systeme sind jedoch häufig nicht in der Lage, miteinander zu kommunizieren. Dies kann sich nachteilig auf die gemeinsamen Anstrengungen zur Bekämpfung von Terrorismus und Kriminalität auf nationaler und europäischer Ebene auswirken. Gleichzeitig müssen diese Systeme geltenden gesetzlichen oder sonstigen Anforderungen (z. B. Datenschutz, Achtung der Privatsphäre) genügen.

Fragen

Bei welchen Systemen muss die Interoperabilität verbessert werden?

Wäre eine Studie über die rechtlichen und sonstigen Grenzen für die Interoperabilität der Systeme in der EU nützlich?

[4] Berücksichtigt werden sollten nicht nur Informationssysteme.

3. INTEGRATION VON INFORMATIONEN AUS VERSCHIEDENEN DETEKTIONSSYSTEMEN UND VERBESSERUNG DER DATENANALYSE

Mit der Integration von Daten aus verschiedenen Detektionssystemen in ein einziges Analysesystem ließe sich die Leistungsfähigkeit dieser Systeme erhöhen. Jede diesbezügliche Maßnahme muss den Datenschutzbestimmungen genügen.

Fragen

In welchen Bereichen würde die Integration von Informationen aus verschiedenen Detektionssystemen Ihrer Ansicht nach die Leistungsfähigkeit dieser Systeme insgesamt erhöhen?

In welchen Bereichen ist eine Verbesserung der Auswertungstechniken erforderlich?

III. VERWENDUNG UND ZERTIFIZIERUNG VON INSTRUMENTEN UND AUSRÜSTUNGEN

1. ‚BEST PRACTICE' UND DIE VERWENDUNG VORHANDENER INSTRUMENTE UND AUSRÜSTUNGEN

Um bestehenden oder neuen Gefahren wirksam begegnen zu können, braucht es nicht immer vollständig neuer technologischer Lösungen. Die Öffentliche Hand kann sich diese häufig auch nicht leisten. Es ist somit darauf zu achten, wie das bereits vorhandene Instrumentarium effizienter eingesetzt oder aufgerüstet werden kann. Dies kann sich als eine kostengünstige Lösung erweisen, um die Leistungsfähigkeit der Ausrüstung zu verbessern, ihre Verlässlichkeit zu erhöhen und die Zahl der Falschalarme zu reduzieren.

Es fehlt an einem Verfahren, mit dem die mitgliedstaatlichen Behörden solche Erfahrungen untereinander austauschen können. Ausgetauscht werden könnten beispielsweise Informationen, wie sich durch Veränderungen in der Betriebsweise oder durch kostengünstige Aufrüstung Verbesserungen erzielen lassen.

Fragen

Wie lassen sich bewährte Praktiken in diesem Bereich am besten ermitteln und austauschen?

Ermittlung bewährter Praktiken

Sollte dies im Wege der Begutachtung oder durch Übersendung von Fragebögen an die Mitgliedstaaten geschehen?

Verbreitung bewährter Praktiken

Sollte dies im Wege einer sicheren, abrufbaren Datenbank geschehen oder durch Sitzungen und Seminare?

Haben Sie noch weitere Vorschläge, wie sich bewährte Praktiken in diesem Bereich am besten ermitteln und verbreiten lassen?

Wird die Aufrüstung eines Instruments oder einer Ausrüstung als erforderlich angesehen und hat noch keine andere mitgliedstaatliche Behörde eine solche Aufrüstung vorgenommen, wäre es akzeptabel, sich in dieser Frage an den privaten Sektor zu wenden?

2. ERMITTLUNG UND VERBREITUNG BEWÄHRTER PRAKTIKEN UND DIE VERWENDUNG NEUER INSTRUMENTE UND AUSRÜSTUNGEN

Von Vorteil wäre für die einzelstaatlichen Behörden auch ein System, das den Austausch von Informationen über neue Instrumente und Ausrüstungen erleichtern würde, so dass die Behörden voneinander lernen und auf den Erfahrungen der anderen aufbauen könnten. Mit Hilfe eines solchen Austauschs von Informationen, Erfahrungen und bewährten Praktiken könnten die Behörden die Instrumente und Ausrüstungen ausfindig machen, die ihren Bedürfnissen am besten entsprechen.

Auch könnten Tests mit neuen Ausrüstungen oder mit Versuchsgeräten aus dem Gemeinschaftshaushalt und/oder mit Mitteln des privaten Sektors gefördert werden. Breit angelegte Versuche mit neuen Ausrüstungen oder Testgeräten könnten dazu beitragen, dass die Sicherheitsforschung leistungs- und wettbewerbsfähige Produkte hervorbringt.

Fragen

Wie lassen sich Informationen und bewährte Praktiken in diesem Bereich am besten ermitteln und austauschen?

Ermittlung bewährter Praktiken

Sollte dies im Wege der Begutachtung oder durch Übersendung von Fragebögen an die Mitgliedstaaten geschehen?

Verbreitung von Informationen und bewährten Praktiken

Sollte dies im Wege einer sicheren, abrufbaren Datenbank geschehen oder durch Sitzungen und Seminare für einen beschränkten Teilnehmerkreis?

Haben Sie noch weitere Vorschläge, wie sich bewährte Praktiken in diesem Bereich am besten ermitteln und verbreiten lassen?

Neue Geräte und Versuchsgeräte

Sind Sie daran interessiert, neue Geräte oder Versuchsgeräte zu testen?

Falls ja/nein, bitte erläutern.

Wäre eine Teilfinanzierung von Versuchen mit neuen Geräten oder Testgeräten durch die Gemeinschaft und/oder den privaten Sektor von Interesse?

3. EINSATZ VON DATA- UND TEXTMININGSYSTEMEN

Das Volumen an Informationen und Dokumentation, das nationale und europäische Sicherheitsbehörden zu verarbeiten haben, nimmt ständig zu. Um der Datenflut effizienter begegnen zu können, gibt es moderne Softwaresysteme für Data- und Textmining. Mit dieser Technologie können relevante Informationen aus einer Vielzahl von Dokumenten gefiltert werden. Beispielsweise ist eine intelligente Filterung von Texten und Dokumenten als Suchhilfe (Gruppierung von Dokumenten) möglich, zur Autokategorisierung (Zuordnung von Dokumenten innerhalb von Ermittlungsteams und Einstufung ihrer Priorität) und Prüfung der Gültigkeit des Benutzercodes. Das Data- und Textmining soll Folgendes leisten:

- Schnellerkennung von Schlüsselbegriffen in Dokumentenbeständen
- Vorverarbeitung des Textmaterials für eine gezielte Dokumentensuche
- inhaltsgestützte Dokumentenklassifizierung für gezieltere Analysen
- automatisierte Analyse von Informationen aus mehreren Quellen.

Das Potenzial dieser neuen Software wird in den Mitgliedstaaten noch nicht voll ausgeschöpft. Der Einsatz dieser Technologien soll zwar gefördert werden, doch darf dabei nicht übersehen werden, dass sie bei bestimmten Anwendungen – z. B. bei der Überwachung von E-Mails – einen Eingriff in das Grundrecht des Einzelnen auf Achtung seiner Privatsphäre darstellen. E-Mails gehören zum Schriftverkehr und unterliegen somit dem Recht auf Schutz des Briefverkehrs im Sinne der Europäischen Menschenrechtskonvention. In einer demokratischen Gesellschaft muss die Verwendung von Data- und Textminingsoftware daher gesetzmäßig sein, zum Schutz eines übergeordneten öffentlichen Interesses erforderlich sein und im Verhältnis zum angestrebten Ziel stehen. Die Achtung der Grundrechte und der Datenschutzgrundsätze sollte daher bei dieser Software und ihrer Anwendung gewährleistet sein. Diese Tätigkeiten unterliegen staatlicher Kontrolle und Überwachung.

Fragen

Sensibilisierungskampagne

Wären die Mitgliedstaaten und die zuständigen europäischen Einrichtungen am Austausch bewährter Praktiken und an den potenziellen Vorteilen von Data- und Textminingsystemen interessiert?

Wären die mitgliedstaatlichen Behörden, die diese Technologie anwenden, bereit, anderen Behörden über ihre Erfahrungen zu berichten?

Wären von den Mitgliedstaaten, Europol oder OLAF für einen beschränkten Teilnehmerkreis veranstaltete Seminare zu diesem Thema nützlich?

Steigerung der EU-Kapazitäten im Bereich Data- und Textmining

Würde ein Exzellenzzentrum auf europäischer Ebene, das allen Mitgliedstaaten und ihren zuständigen Behörden offen steht, dazu beitragen, das Potenzial dieser Technologie in der Praxis nutzbar zu machen?

Falls nein, was würden Sie vorschlagen, um die potenziellen Einsatzmöglichkeiten dieser Technologie zu maximieren?

Ermittlung und Verbreitung bewährter Praktiken

Wäre zur Ermittlung der ‚Best Practice' bei der Verwendung dieser Technologie ein Gutachten oder ein Fragebogen an die Mitgliedstaaten hilfreich?

Falls nein, welche Vorgehensweise würden Sie vorschlagen, um bewährte Praktiken in diesem Bereich zu erfassen?

Ausbau der regionalen Kapazitäten im Bereich Data- und Textmining

Verfügen die Mitgliedstaaten oder europäische Einrichtungen über ungenutzte Kapazitäten, um den Mitgliedstaaten, die nicht über diese Technologie verfügen, bei der Bearbeitung ihrer Dokumente zu helfen?

Falls es keine ungenutzten oder nur sehr beschränkte Kapazitäten gibt, wäre es sinnvoll und praktisch, diese Kapazitäten in den Mitgliedstaaten oder auf EU-Ebene mit EU-Mitteln auszubauen?

Würden die Mitgliedstaaten, die nicht über ausreichende Data- und Textminingkapazitäten verfügen, in Erwägung ziehen, die Systeme anderer Einrichtungen zu nutzen, sofern diese sie zur Verfügung stellen?

Wäre es möglich, europäische oder regionale Zentren für Data- und Textmining einzurichten, die von mehreren Mitgliedstaaten und ihren Behörden genutzt werden könnten?

Reichen die vorhandenen Data- und Textminingsysteme für die Verarbeitung der verschiedenen Sprachen in Europa aus?

Gibt es geeignete Systeme, um die Behörden bei der Bearbeitung fremdsprachiger Texte und Dokumente zu unterstützen?

Sonstiges

Falls Sie keinem der vorstehenden Vorschläge zustimmen können, wie würden Sie die hier angesprochenen Probleme angehen?

5. PRÜFUNG UND ZERTIFIZIERUNG DER QUALITÄT VON INSTRUMENTEN UND AUSRÜSTUNGEN

Auf dem Markt werden bereits Detektionstechniken angeboten. Es ist sehr häufig jedoch nicht einfach festzustellen, welche Produkte und Systeme am besten sind oder zumindest gewissen Mindestanforderungen genügen. Dieser Mangel ließe sich mit einem EU-weiten System zur Zertifizierung und Bewertung hochwertiger Produkte beheben, mit dessen Hilfe die Behörden leichter feststellen können, welche der Instrumente oder Ausrüstungen für ihre besonderen Zwecke geeignet sind. Ein solches System kann den nationalen Behörden die Kaufentscheidung erleichtern und kann ihnen auch dabei helfen, knappe Ressourcen optimal zu nutzen.

Als Ausgleich für ein fehlendes System zur Bestimmung der Produktqualität könnte auch ein Netzwerk *nationaler* Zertifizierungsstellen eingerichtet werden, die ihre Erfahrungen und ihr Wissen untereinander austauschen. Diese Stellen würden sich auf entsprechende Bewertungs- und Zertifizierungsstandards für qualitativ hochwertige technische Lösungen verständigen. Diese Art der Zertifizierung könnte nicht nur dazu verwendet werden, um nationalen Behörden bei ihrer Entscheidung zu helfen, ob ein Instrument ihren Qualitätsanforderungen genügt, sondern auch dazu, auf anderen Märkten für europäische Sicherheitslösungen zu werben. Es liegt auf der Hand, dass die Entwicklung von Testprotokollen aus Sicherheitsgründen nicht in aller Öffentlichkeit erörtert werden kann.

Fragen

Wäre es nützlich, neben einem System zur Qualitätsbewertung und -zertifizierung ein Netzwerk nationaler Zertifizierungsstellen einzurichten, die ihre Erfahrungen und ihr Wissen untereinander austauschen?

Falls nein, welche andere Lösung würden Sie vorschlagen, um die angesprochenen Probleme anzugehen?

Wären gemeinsame Zertifizierungs- und Bewertungsstandards hilfreich?

Falls nein, wie würden Sie in diesem Bereich für Transparenz und für die Verwertbarkeit der Ergebnisse in der EU sorgen?

IV. STUDIEN[5]

Die Konferenzteilnehmer nannten mehrere Themen, die in weiteren Studien zu vertiefen wären. Die Kommission schlägt dementsprechend vor, Studien zu folgenden Themen in Auftrag zu geben:

(1) Technologie und Sicherheit von Großveranstaltungen

(2) Hindernisse bei der Kooperation und beim Informationsaustausch zwischen kriminaltechnischen Labors und Instituten für Sicherheitsforschung

(3) Rechtsvorschriften für die Verwendung bestimmter Detektionstechnologien

(4) Einsatz bestimmter Detektionstechnologien in der Praxis

(5) Rechtsvorschriften für den Einsatz von Personendetektionssystemen (einschließlich Personenüberwachung) in der EU

(6) Akzeptanz der Personendetektion (einschließlich Personenüberwachung und Einsatz von Biometrie) in der EU.

Die Studien sind generell als Hilfsmittel gedacht, um den Beteiligten genauere Informationen an die Hand zu geben und um dafür zu sorgen, dass die geltenden Rechtsvorschriften bei der Entwicklung und beim Einsatz von Detektionstechnologien beachtet werden. Darüber hinaus können die Studien herangezogen werden, um politische Strategien und Optionen für das weitere Vorgehen zu entwickeln.

Fragen

Wären Sie an Studien zu diesen Themen auf der Grundlage der im Anhang enthaltenen Hintergrundinformationen interessiert?

Falls nein, geben Sie bitte die Gründe hierfür an und schlagen Sie Alternativen vor, wie den angesprochenen Problemen abgeholfen werden kann.

[5] Auf die Begründung dieser Studien wird in Teil III des Anhangs näher eingegangen.

V. UMSETZUNG DER KONSULTATIONSERGEBNISSE

1. INTENSIVER, ZIELGERICHTETER ÖFFENTLICH-PRIVATER DIALOG ÜBER DETEKTIONSTECHNOLOGIEN UND IHRE ANWENDUNG

In diesem Grünbuch werden eine Reihe von Handlungsmöglichkeiten aufgezeigt, die dazu beitragen können, die Interaktion zwischen dem öffentlichen und dem privaten Sektor im Bereich der Detektionstechnologien zu verbessern, und die auf diese Weise den Sicherheitsbehörden der Mitgliedstaaten Zugang zu den bestmöglichen Instrumenten, Lösungen und Praktiken verschaffen können. Gleichzeitig erhält der private Sektor die Möglichkeit, seine Investitionen gezielter einzusetzen und auf den Bedarf des öffentlichen Sektors auszurichten. Hierzu ist allerdings eine enge Zusammenarbeit zwischen öffentlichem und privatem Sektor und damit ein intensiverer, zielgerichteter öffentlich-privater Dialog in diesem Bereich erforderlich. Dies könnte u. a. im Rahmen horizontaler öffentlich-privater Partnerschaften zu Sicherheitsfragen durch die Einrichtung eines besonderen Gremiums oder einer Gruppe erreicht werden. Damit sollte baldmöglichst begonnen werden.

Dieses Gremium oder diese Gruppe würde nicht in Konkurrenz zu den vorhandenen Stellen treten, sondern Lücken in der Interaktion zwischen dem öffentlichen und dem privaten Sektor schließen und die zuständigen Sicherheitsbehörden auf europäischer Ebene einbeziehen. Auch sollte es sich nicht um eine ständige Einrichtung handeln. Sind die Zielvorgaben erreicht, würde die Gruppe aufgelöst. Die Einrichtung würde als Expertenforum für den öffentlichen und den privaten Sektor dienen und mithelfen, die in diesem Grünbuch aufgezeigten Problemfelder anzugehen oder neue Herausforderungen aufzugreifen, die sich möglicherweise aus der Konsultation zu diesem Grünbuch ergeben.

Einige der in diesem Grünbuch vorgeschlagenen Maßnahmen erfordern allerdings ein Tätigwerden der Mitgliedstaaten ohne Beteiligung des privaten Sektors. Zudem müssten sich der öffentliche und der private Sektor über die Aufgabenstellung einigen. Die Mitgliedstaaten wären als Kooperationspartner in der Lage, Tragweite und Schwerpunkt dieser Kooperation zu beeinflussen. Zu regeln wäre auch, wie vertrauliche Informationen zwischen dem öffentlichen und dem privaten Sektor ausgetauscht werden. Dabei ist allerdings darauf hinzuweisen, dass sensitive Informationen nicht auf den öffentliche Sektor beschränkt sind.

Fragen

Wäre ein intensiverer, zielgerichteter öffentlich-privater Dialog zu Detektionstechnologien und ihre Anwendung bei der Umsetzung der Ergebnisse aus der öffentlichen Konsultation zu diesem Grünbuch hilfreich?

Wenn ja, sind Sie mit den vorstehenden Vorschlägen einverstanden oder haben Sie andere Vorstellungen?

Wenn nein, welche andere Vorgehensweise würden Sie im Nachgang zu der Grünbuchkonsultation vorschlagen?

Wären Sie daran interessiert, einen Beitrag zur Umsetzung der Konsultationsergebnisse zu leisten oder direkt daran mitzuwirken?

2. AKTIONSPLAN

Aktionspläne haben sich auf nationaler und europäischer Ebene zur Verfolgung von Maßnahmen in komplexen Bereichen wie der Terrorismus- oder Verbrechensbekämpfung als erfolgreich erwiesen. Sowohl auf der Konferenz als auch in diesem Grünbuch sind zahlreiche Fragen zu Detektionstechnologien in der Arbeit der Sicherheitsbehörden angesprochen worden. Um Zielvorgaben zu formulieren und die Fortschritte in diesem Bereich zu verfolgen, könnte anhand der Antworten auf die im Grünbuch gestellten Fragen und erforderlichenfalls auf der Grundlage weiterer Konsultationen ein Aktionsplan erstellt werden.

Frage

Wäre ein Aktionsplan zur Umsetzung der in den Beiträgen zu diesem Grünbuch genannten Maßnahmen hilfreich?

Beiträge zum Grünbuch

Beiträge zu diesem Grünbuch sind bis 10. Januar 2007 elektronisch an folgende E-Mail-Adresse zu richten: **JLS-D1-Detection@ec.europa.eu**. Sofern nicht ausdrücklich um vertrauliche Behandlung gebeten wird, werden alle Grünbuch-Beiträge des öffentlichen und des privaten Sektors auf der Website der Kommission veröffentlicht.

ANHANG

I. HINTERGRUNDINFORMATIONEN ZUM GRÜNBUCH

Dieses Grünbuch basiert auf den Ergebnissen der Konferenz vom 28./29. November 2005 und greift Themen und Fragen auf, die bei den Diskussionen im Vordergrund standen (z. B. Normung und Standardisierung, Sicherheitsforschung, Verbesserung technologischer Sicherheitslösungen, Schutz der Privatsphäre, Rechtsvorschriften und sonstige Vorgaben, nach denen sich Detektionstechnologien zu richten haben, usw.). Über hundert Teilnehmer aus Wirtschaft und Industrie sowie aus dem öffentlichen Sektor haben sich an der Debatte beteiligt. Der öffentliche Sektor war durch Angehörige der Strafverfolgungs-, Zoll- und anderer Sicherheitsbehörden, der Kommission und der Mitgliedstaaten vertreten. Die Bezeichnung der Konferenz deutet darauf hin, dass die Bekämpfung des Terrorismus im Mittelpunkt stand. Schon zu Anfang wurde jedoch deutlich, dass ein breiteres Sicherheitskonzept unerlässlich ist, wenn nicht wichtige Sicherheitsbelange unberücksichtigt bleiben sollen. Dies wurde vom Rat im Dezember 2005 bestätigt, als er ein umfassendes Schutzkonzept für europäische kritische Infrastrukturen beschloss. Die Konferenz verfolgte darüber hinaus einen ganzheitlichen Ansatz, indem sie Vertreter aus verschiedenen Wissensbereichen zusammenführte, um folgende Themen zu erörtern:

- Einsatz von Detektionstechnologien beim Schutz von Infrastruktureinrichtungen
- Personendetektion und Biometrie
- Detektion von Sprengstoffen sowie chemischen, biologischen, radiologischen und nuklearen Stoffen (CBRN).

Im Mittelpunkt aller Themen stand jeweils die Arbeit der Strafverfolgungs-, Sicherheits- und der Zollbehörden. Auf diese Weise gelang es der Konferenz, zahlreiche Bereiche auszumachen, die für den öffentlichen und den privaten Sektor gleichermaßen von Belang sind (z. B. Interaktion zwischen denjenigen, die Lösungen anbieten, und denjenigen, die im öffentlichen Sektor Lösungen nachfragen). Dies kommt durchgängig im ganzen Grünbuch zum Ausdruck.

Definition und Kategorisierung von Detektionstechnologien

Der Begriff ‚Detektionstechnologie' wird in dieser Konsultation im weitesten Sinne verwendet. Detektionstechnologien können vor Ort oder extern eingesetzt werden. Um Sicherheitsprobleme in verschiedenen Szenarien anzugehen, bietet sich jedoch die Integration dieser Technologien in ein komplexes System (z. B. Verkehrssystem) an. Detektionstechnologie kann fast alles sein, was in einem Sicherheitskontext vor allem von Strafverfolgungs-, Zoll- oder Sicherheitsbehörden zu Detektionszwecken eingesetzt wird. Es lassen sich mehrere Kategorien unterscheiden[6], die, wenn sie bei der Beantwortung der in diesem Grünbuch gestellten Fragen berücksichtigt werden, u. U. eine präzisere Aussage ermöglichen:

[6] Diese Aufzählung ist nicht erschöpfend.

- Handdetektoren
- Detektorschleusen
- Überwachungslösungen
- Biometrische Detektionstechniken
- Data- und Textminingsysteme
- Andere IT-gestützte Detektionssysteme.

In den Beiträgen sollten auch Anwendungstechnologien berücksichtigt werden, da für effiziente Sicherheitslösungen auch Technologien wichtig sind, die eine Auswertung und Interpretation der mit Hilfe von Detektoren erhobenen Daten ermöglichen. Technologie wird auch gebraucht, um Problemlösungen zu integrieren und Systeme zu vernetzen. Die vorstehende Aufzählung ist nicht erschöpfend. Die Konsultationsteilnehmer können durchaus auf weitere Kategorien eingehen.

II. STANDARDISIERUNG UND AUSTAUSCH PERSONENBEZOGENER DATEN

Zum Umgang mit personenbezogenen Daten weist die Kommission darauf hin, dass die Richtlinie 95/46/EG bei Tätigkeiten, die in die Zuständigkeit der Gemeinschaft fallen, bereits den Austausch von Informationen regelt, die personenbezogene Daten enthalten. Was den Austausch von Informationen im Rahmen der justiziellen Zusammenarbeit in Zivil- und Strafsachen sowie nach dem Verfügbarkeitsgrundsatz anbelangt, so hat die Kommission einen Legislativvorschlag vorgelegt, über den derzeit beraten wird.

III. STUDIEN

1. Sicherheit von Großveranstaltungen

In den EU-Mitgliedstaaten werden jedes Jahr Großveranstaltungen von nationaler, europäischer oder gar internationaler Bedeutung veranstaltet. Bei der heutigen Sicherheitslage können die Kosten für den Schutz solcher Veranstaltungen einen beträchtlichen Teil ihres Budgets ausmachen. Von einer gemeinsamen Sicherheitslösung würden alle Mitgliedstaaten profitieren.

Als Grundlage für etwaige weitere Schritte in diesem Bereich schlägt die Kommission eine Studie zur Sicherheitsproblematik von Großveranstaltungen vor. In der Studie würde untersucht, welche Sicherheitsausrüstungen und -systeme, die zum Schutz von Großveranstaltungen eingesetzt werden, von einem Veranstaltungsort zu einem anderen transferiert werden können. Dabei wäre auch zu prüfen, inwieweit sich für diese Zwecke gemeinschaftseigene oder von den Mitgliedstaaten gemeinsam genutzte Ausrüstungen eignen würden und welche Folgen damit verbunden wären, ob ein Geschäftsmodell für Dienstleistungen der Privatwirtschaft ausgearbeitet werden sollte oder eine Kombination aller drei Ansätze in Frage käme. Als Ergebnis wäre in der Studie festzuhalten,

- welche Vorgehensweise am kostengünstigsten und flexibel genug ist, um den unterschiedlichen Anforderungen der Mitgliedstaaten zu genügen, und

- sicherstellen kann, dass alle Mitgliedstaaten diese Lösung in Anspruch nehmen und sich in angemessener Weise in die Kosten teilen können.

Anhand der Ergebnisse der Studie würde die Kommission dann gemeinsam mit den Mitgliedstaaten und den anderen Beteiligten erörtern, wie in diesem Bereich weiter vorzugehen wäre.

2. Kooperation und Informationsaustausch zwischen kriminaltechnischen Labors und Instituten für Sicherheitsforschung

Die Konferenzteilnehmer wiesen auf Hindernisse rechtlicher und sonstiger Art auf nationaler Ebene hin, die einer effizienten Zusammenarbeit und einem effizienten Informationsaustausch zwischen nationalen kriminaltechnischen Labors in Europa entgegenstehen. Die Kommission schlägt vor, zu dieser Problematik eine Studie in Auftrag zu geben. In der Studie könnten auch Problemlösungen erörtert werden.

Ähnliche Bedenken wurden bei der Zusammenarbeit und beim Informationsaustausch zwischen den Instituten für Sicherheitsforschung laut. Diese Problematik könnte in einer separaten Studie untersucht werden.

3. Detektionstechnologie und Recht

Strafverfolgungs-, Zoll- und andere Sicherheitsbehörden werden häufig daraufhin überprüft, ob sie den rechtlichen Anforderungen genügen. Auch wenn die Technologie als solche nicht gegen geltendes Recht verstößt, kann die Art und Weise ihres Einsatzes problematisch sein. Die Feststellung der Rechtsvorschriften, die den Einsatz dieser Technologie und deren Grenzen regeln, könnte dazu beitragen, das Problembewusstsein sowohl im öffentlichen als auch im privaten Sektor zu erhöhen und die Einhaltung der rechtlichen Vorgaben zu erleichtern. Auch der private Sektor könnte von einer solchen Studie profitieren, wenn es darum geht, für den öffentlichen Sektor technologische Lösungen und Dienstleistungen zu entwerfen und zu realisieren.

4. Detektionstechnologie und ihr Einsatz in der Praxis

Empfehlungen und bewährte Praktiken für den Einsatz von Technologie, insbesondere Detektionstechnologie, müssen der Art und Weise, wie diese Technologie in der Praxis tatsächlich eingesetzt wird und wie mit den Personen umgegangen wird, bei denen diese Technologie angewandt wird, Rechnung tragen. Eine bestimmte Technologie verstößt vielleicht nicht gegen geltendes Recht, aber ihr Einsatz in der Praxis kann Anlass zu Bedenken geben. Außerdem können sich infolge der Entwicklung neuer Technologien oder einer anderen Verwendung bestehender Technologien Situationen ergeben, in denen der Einsatz solcher Technologien nicht geregelt ist. Denkbar ist auch, dass eine bestimmte Verwendungsweise durchaus rechtmäßig sein kann, aber u. U. bewährten Praktiken oder Verhaltenskodizes zuwiderläuft, die als Ergänzung rechtlicher Bestimmungen eingeführt wurden. Die Kenntnis einschlägiger Regelungen für die betreffenden Technologien kann Aufschluss darüber geben, ob diese Technologien mit dem geltenden Recht (insbesondere mit den Grundrechten und den Datenschutzbestimmungen) in Einklang stehen und was in einem gesetzlich nicht geregelten Fall akzeptabel ist oder nicht.

5. Personendetektion und Biometrie

Personendetektion (einschließlich Überwachung) und Biometrie sind Bereiche, die den Einzelnen direkt betreffen. Der Einsatz dieser Techniken zur Verbesserung der Sicherheit in Europa ist zurzeit Gegenstand einer kontroversen politischen Debatte. Die Kommission schlägt die Vergabe einer Studie vor, in der die rechtlichen Bestimmungen im Bereich der Personendetektion und Biometrie erfasst werden. In dieser Studie soll untersucht werden, welche Vorschriften es in den Rechtssystemen der Mitgliedstaaten und im EU-Recht für den Bereich Personendetektion und Biometrie gibt. Eine solche Untersuchung ist besonders hilfreich, um die vom privaten Sektor vorgeschlagenen technischen Lösungen mit den rechtlichen Vorgaben in Einklang zu bringen. Der private Sektor könnte auf diese Weise bereits bei der Konzeption den rechtlichen und sonstigen Anforderungen Rechnung tragen.

In weiteren Studien könnte auch der Frage nachgegangen werden, inwieweit Überwachungs- und Biometriesysteme von der Bevölkerung in den Mitgliedstaaten und in der EU insgesamt akzeptiert werden. Dabei wäre auf eine saubere methodische Trennung beider Bereiche – Überwachung und Biometrie - zu achten. Studien dieser Art könnten es der EU und den nationalen Regierungen erleichtern, geeignete Kommunikationsstrategien zu diesen Fragen zu entwickeln, und würden allgemein einen Beitrag zur politischen Debatte in Europa leisten.