COMISSÃO DAS COMUNIDADES EUROPEIAS

Bruxelas, 1.9.2006
COM(2006) 474 final

LIVRO VERDE

relativo a tecnologias de detecção no âmbito do trabalho das autoridades de aplicação da lei, das autoridades aduaneiras e de outras autoridades de segurança

(apresentada pela Comissão)

ÍNDICE

LIVRO VERDE

relativo a tecnologias de detecção no âmbito do trabalho das autoridades de aplicação da lei, das autoridades aduaneiras e de outras autoridades de segurança

(Texto relevante para efeitos do EEE)

INTRODUÇÃO

A segurança constitui uma das pedras angulares da política da Comissão. A luta contra a criminalidade e o terrorismo é uma vertente essencial da política de segurança. A Comissão expôs a sua política de luta contra oterrorismo na sua "*Comunicação sobre a prevenção, estado de preparação e capacidade de resposta aos atentados terroristas*", de Outubro de 2004. Essa comunicação sublinha que o *diálogo entre os sectores público e privado no domínio da segurança* constitui um meio para que estes sectores iniciem um diálogo frutuoso sobre as necessidades de segurança da Europa. O *Programa da Haia para o reforço da liberdade, da segurança e da justiça na União Europeia,* adoptado pelo Conselho Europeu em Novembro de 2004, que consubstancia o actual programa político da União em matéria de Justiça e Assuntos Internos, destaca igualmente a importância da interacção entre os sectores público e privado na luta contra a criminalidade organizada e o terrorismo. O presente Livro Verde destina-se a proporcionar os elementos necessários para encetar esse diálogo no domínio das tecnologias de detecção.

As tecnologias de detecção são cada vez mais utilizadas no trabalho quotidiano das autoridades de segurança na luta contra o terrorismo e outras formas de criminalidade. As tecnologias de detecção são largamente utilizadas para proteger os passageiros que embarcam em aviões e os adeptos que assistem aos seus eventos desportivos favoritos, bem como para detectar substâncias perigosas no ar, na água ou nos alimentos. As autoridades de segurança recorrem igualmente a estas tecnologias para proteger as nossas fronteiras e para controlar produtos que entram no território da União Europeia. Além disso, as tecnologias de detecção são essenciais para defender a propriedade privada e as infra-estruturas críticas. O presente Livro Verde destina-se a apurar qual o papel que a União pode desempenhar na promoção de tecnologias de detecção ao serviço da segurança dos seus cidadãos. Por outro lado, as tecnologias de detecção implicam forçosamente uma ingerência na vida privada das pessoas e podem constituir desafios em relação aos direitos e liberdades. Por conseguinte, sempre que se pondere a melhoria e a utilização de tecnologias de detecção, este aspecto e a questão fulcral das limitações à sua ingerência devem obrigatoriamente ser atentamente analisados. Através da presente iniciativa, a Comissão pretende contribuir para estas duas vertentes.

A Comissão organizou uma conferência[1] - *Diálogo entre os sectores público e privado no domínio da segurança: Tecnologias de detecção e tecnologias conexas na luta contra o terrorismo* - em Bruxelas, em 28-29 de Novembro de 2005. A participação de mais de cem representantes de importantes associações empresariais e industriais europeias e do sector público comprovou o interesse das partes interessadas na prossecução da política nesta área.

[1] Para mais informações de base, consultar a parte I do Anexo.

O sector público esteve representado por membros das autoridades de aplicação da lei, das autoridades aduaneiras e de outras autoridades de segurança.

O papel da Europa em áreas como a investigação ou a normalização em matéria de segurança encontra-se claramente estabelecido. Embora tenha sido desenvolvido um trabalho considerável em certas áreas em estreita cooperação com os Estados-Membros, a indústria e outras partes interessadas, é ainda possível melhorar a política europeia no domínio das tecnologias de detecção propriamente ditas. No que respeita à segurança da aviação, os Regulamentos (CE) n° 2320/2002 e n.° 622/2003[2] estabelecem ambos requisitos pormenorizados em relação ao desempenho do equipamento de rastreio a utilizar e à respectiva metodologia. Nesta matéria, foram estabelecidos normas e protocolos de ensaio em estreita cooperação com a Conferência Europeia da Aviação Civil, que congrega peritos das autoridades competentes dos Estados-Membros e de outros Estados europeus. Além disso, a Comissão mantém contactos estreitos e regulares com a indústria, bem como com outros intervenientes (*Stakeholders Advisory Group on Aviation Security* - Grupo Consultivo de Partes Interessadas na Segurança da Aviação - Grupo SAGAS).

Com vista ao reforço da abordagem comum em relação às tecnologias de detecção, a Comissão tomou esta iniciativa para fomentar a interacção entre os sectores público e privado numa tentativa de centrar o investimento na normalização, na investigação, na certificação e na interoperabilidade dos sistemas de detecção e de transformar os resultados da investigação em instrumentos úteis e viáveis. Tem de ser criado um círculo virtuoso em que o sector privado é orientado nas suas iniciativas de investigação e nas suas despesas por um sector público que sabe o que quer e o que o sector privado pode oferecer. Assim se contribuirá para o desenvolvimento de um mercado avançado de produtos de detecção e de soluções em matéria de segurança que, por seu turno, conduzirá a uma maior disponibilidade de produtos e a serviços mais económicos.

Uma acção comum e uma melhor coordenação e intercâmbio de informações entre todas as partes envolvidas na Europa são essenciais para que este objectivo seja alcançado. As necessidades têm de ser melhor definidas e há que fazer emergir soluções tecnológica e economicamente viáveis. O presente Livro Verde certamente **não pretende substituir-se a outras actividades a nível nacional ou europeu**. A Comissão não pretende reinventar a roda mas sim ficar a conhecer melhor as boas abordagens e práticas existentes, apoiando-as e divulgando-as por toda a União.

A Comissão gostaria que o presente Livro Verde gerasse o máximo número possível de respostas estimulantes e de sugestões concretas sobre os passos que se devem seguir. **É, por conseguinte, indispensável a participação alargada dos Estados-Membros, do sector privado e de outros interessados relevantes**. A Comissão está, porém, consciente dos requisitos de confidencialidade dos sectores quer público quer privado, por razões de segurança e de natureza comercial. Por conseguinte, solicita-se aos inquiridos que indiquem as respostas que consideram demasiado sensíveis para serem partilhadas e que sugiram uma abordagem alternativa para atender a tais preocupações.

---

[2] Regulamento (CE) n.º 2320/2002 do Parlamento Europeu e do Conselho, de 16 de Dezembro de 2002, relativo ao estabelecimento de regras comuns no domínio da segurança da aviação civil (JO L 355 de 30.12.2002, p. 1) e Regulamento (CE) n.º 622/2003 da Comissão, de 4 de Abril de 2003, relativo ao estabelecimento de medidas de aplicação das normas de base comuns sobre a segurança da aviação (JO L 89 de 5.4.2003, p. 9).

As políticas relativas às tecnologias de detecção e às tecnologias conexas têm de respeitar integralmente o quadro normativo existente, incluindo a Carta dos Direitos Fundamentais da União Europeia, a Convenção Europeia dos Direitos do Homem e os princípios e regras de protecção dos dados estabelecidos na Directiva 95/46/CE. Neste contexto, a Comissão sublinha que a concepção, o fabrico e a utilização de tecnologias de detecção e das tecnologias conexas, bem como a legislação ou outras medidas destinadas a regulamentá-los ou a promovê-los, **devem respeitar plenamente os Direitos Fundamentais**, tal como previstos na Carta dos Direitos Fundamentais da União Europeia e na Convenção Europeia dos Direitos do Homem. Há que prestar especial atenção à observância da protecção dos dados pessoais e ao respeito da vida privada. De facto, como a utilização de tecnologias de detecção implica geralmente uma ingerência nos direitos fundamentais à privacidade e à protecção dos dados pessoais, qualquer intrusão deste tipo deve estar em conformidade com a Convenção Europeia sobre os Direitos Fundamentais; deve designadamente respeitar a lei e ser necessária numa sociedade democrática para proteger um interesse público importante, devendo ser proporcional ao interesse público em causa.

I. NORMALIZAÇÃO E INVESTIGAÇÃO EM MATÉRIA DE SEGURANÇA

1. NORMALIZAÇÃO

É muito vasto o leque das possibilidades tecnológicas nas áreas relativas às tecnologias de detecção e tecnologias conexas e às actividades das autoridades de segurança. Por conseguinte, são necessárias normas mínimas. No entanto, em virtude desta multiplicidade, há que fixar prioridades no processo de normalização, o que apenas será possível se houver uma articulação adequada entre o sector público (necessidades) e o sector privado (soluções). A nível europeu, esta interacção é considerada insuficiente quer pelo sector público quer pelo sector privado. Por outro lado, estão a ser desenvolvidas muitas actividades positivas a nível nacional e europeu. Não existe, porém, uma panorâmica geral, necessária para evitar duplicações e para melhorar a definição de prioridades. É evidente que, por razões de segurança, o desenvolvimento de normas não pode ser objecto de discussão pública. O debate centrar-se-á, portanto, sobretudo na questão de saber até que ponto são desejáveis normas comuns.

A utilização e tratamento de dados e informações recolhidos por instrumentos de detecção, por exemplo como provas em processos judiciais, estão também estreitamente relacionados com a normalização. As autoridades relevantes podem beneficiar da identificação e intercâmbio das melhores práticas nesta matéria. Deve ser igualmente ponderada a elaboração de normas técnicas para assegurar que os dados obtidos respeitam os requisitos legais para poderem ser utilizados em processos judiciais[3].

Perguntas

São necessárias normas comuns em matéria de tecnologias de detecção e tecnologias conexas utilizadas no âmbito das actividades das autoridades de segurança? Que normas consideram prioritárias?

Que normas carecem de apoio financeiro na fase de pré-normalização?

Para evitar duplicações e aumentar a transparência, seria útil poder dispor-se de uma lista/manual/base de dados pesquisável e regularmente actualizada das iniciativas de normalização passadas, presentes e futuras em matéria de detecção e em domínios tecnologicamente muito relacionados a nível nacional e europeu ?

Haverá interesse na identificação e intercâmbio das melhores práticas no que respeita à utilização e tratamento de dados e informações recolhidos por instrumentos de detecção com a preocupação de observar plenamente a legislação e regras relevantes em matéria de utilização de provas em processos judiciais?

Qual seria a melhor forma de identificar e proceder ao intercâmbio destas práticas?

[3] No que respeita às disposições jurídicas que regem o intercâmbio dos dados pessoais, ver parte II do Anexo.

2. INVESTIGAÇÃO EM MATÉRIA DE SEGURANÇA

A investigação em matéria de segurança é outro domínio essencial para o desenvolvimento de novos produtos e soluções de segurança destinados às autoridades de segurança dos Estados-Membros. Neste contexto, há que realçar o papel do Comité Consultivo Europeu de Investigação em Matéria de Segurança (ESRAB). O ESRAB adopta uma perspectiva global e alargada desta área e aconselha a Comissão em relação ao conteúdo e aplicação da investigação a efectuar, bem como aos mecanismos de acompanhamento de progressos significativos registados noutros programas.

Encontram-se em curso a nível europeu e dos Estados-Membros algumas actividades de investigação em matéria de segurança. No entanto, não existe um mecanismo que permita agregar e divulgar a informação sobre a investigação em matéria de segurança passada, presente e proposta a nível europeu, nacional e, em última análise, do sector privado. Esse mecanismo pode assegurar que recursos escassos não sejam desperdiçados em duplicações e em projectos sobrepostos. Além disso, se necessário, poderá ser concebido um mecanismo distinto para divulgar actividades de investigação em matéria de segurança classificadas secretas, assegurando que a informação apenas seja acessível a pessoas autorizadas.

Ao fim de mais de um ano de trabalho, o ESRAB está a finalizar o seu relatório, que será publicado em Setembro de 2006. O relatório identifica cerca de 120 capacidades de segurança e 100 tecnologias-chave que carecem de investigação e de desenvolvimento adicional a nível da UE, ao passo que diversas outras tecnologias devem ser tratadas a nível nacional.

Perguntas

Como deveria ser divulgada a informação sobre a investigação em matéria de segurança na Europa a fim de promover a competitividade e evitar simultaneamente o desperdício de recursos escassos?

II. NECESSIDADES E SOLUÇÕES

1. NECESSIDADES E SOLUÇÕES TECNOLÓGICAS

O desenvolvimento de produtos e soluções de qualidade, eficazes e viáveis exige que os respectivos produtores disponham de informações suficientes sobre as necessidades reais dos utilizadores finais. Contudo, a nível europeu parece haver uma necessidade de melhor articulação entre os utilizadores das soluções tecnológicas (ou seja, as autoridades de segurança relevantes) e os fornecedores das mesmas. Neste contexto, é igualmente necessário procurar identificar as necessidades a curto, médio e a longo prazo. Por outro lado, os fornecedores de soluções devem também indicar o calendário de disponibilização destas soluções.

Além disso, no diálogo entre produtores e utilizadores devem ser levantadas e abordadas questões mais fundamentais que se prendem com a natureza das nossas sociedades e o papel das tecnologias de detecção. Este debate é igualmente importante na perspectiva da preservação dos valores e características das nossas sociedades.

Perguntas

Haverá interesse em proceder a um debate mais alargado sobre o papel das tecnologias de detecção e sobre a influência que a sua utilização pode ter nas sociedades europeias?

Em que áreas específicas necessitam as autoridades de segurança relevantes de progressos tecnológicos? Queiram especificar o grau de prioridade em relação a necessidades específicas.

Existe um fosso entre as necessidades em termos de capacidades de detecção e a tecnologia actualmente existente no mercado? Quais as possíveis soluções para colmatar estas lacunas?

Em que áreas específicas o sector privado oferece já, ou planeia oferecer, soluções tecnológicas? Queiram indicar o calendário de oferta de tais soluções e a sua relação custo-eficácia.

Seria positivo e útil criar uma lista/base de dados pesquisável à escala europeia que abrangesse áreas específicas das necessidades das autoridades de segurança relevantes, bem como as soluções propostas pelo sector privado?

Em caso negativo, que outras soluções proporiam para melhorar o fluxo de informações entre os utilizadores de soluções tecnológicas e os seus fornecedores?

1.1 Soluções versáteis

As ameaças actuais, desde a criminalidade até ao terrorismo, são múltiplas, encontram-se em constante mutação e apresentam-se sob formas diferentes, a níveis diferentes e em situações diferentes. Por conseguinte, requerem níveis de protecção diferentes e respostas em alturas diferentes, ou seja, soluções versáteis.

Pergunta

Quais os instrumentos e equipamentos existentes cuja aplicabilidade e eficácia podem ser melhoradas através de uma maior versatilidade?

Que novos instrumentos e equipamentos versáteis são necessários?

1.2 Soluções portáteis e móveis

O carácter da ameaça resultante do terrorismo e da criminalidade não só se está a alterar no tempo como se está a tornar cada vez mais móvel. Por conseguinte, as autoridades de segurança necessitam de soluções portáteis. Tais soluções podem melhorar a relação custo/eficácia e ser prontamente transferidas para locais diferentes onde sejam mais necessárias, dado ser impraticável dotar do mesmo nível de segurança todos os pontos de entrada ou locais sensíveis. Além disso, as soluções portáteis e móveis podem permitir novas abordagens operacionais.

Pergunta

Que instrumentos e equipamentos existentes poderiam ser melhor e mais eficazmente utilizados pelas autoridades de segurança relevantes se fossem móveis e portáteis?

Que novos instrumentos e equipamentos portáteis e móveis são necessários?

2. INTEROPERABILIDADE DOS SISTEMAS[4]

Os Estados-Membros da UE e as respectivas autoridades relevantes dispõem já de alguns sistemas de apoio na luta contra a criminalidade e o terrorismo. No entanto, estes sistemas são frequentemente incapazes de comunicar entre si, uma situação que pode comprometer as iniciativas comuns de luta contra a criminalidade e o terrorismo a nível nacional e europeu. Por outro lado, os sistemas devem respeitar os quadros normativos e outras directrizes existentes (por exemplo, em matéria de protecção de dados e de ingerência dos sistemas de detecção).

Pergunta

Que sistemas necessitam de melhor interoperabilidade?

Um estudo sobre os condicionalismos legais e outros em relação à interoperabilidade de sistemas na UE seria útil para identificar limitações?

3. INTEGRAÇÃO DE INFORMAÇÕES PROVENIENTES DE VÁRIAS TECNOLOGIAS DE DETECÇÃO E MELHORIA DA ANÁLISE DE DADOS

A integração de dados provenientes de várias tecnologias de detecção num sistema único de análise de dados pode aumentar a eficácia dos sistemas de detecção. Todas as medidas adoptadas neste domínio devem observar as regras de protecção dos dados.

---

[4] Devem igualmente ser considerados outros sistemas para além dos de informação.

Pergunta

Em que áreas consideram que a integração de informações provenientes de várias tecnologias de detecção melhoraria o desempenho global?

Em que domínios são necessários aperfeiçoamentos das técnicas de análise de dados?

III. UTILIZAÇÃO E CERTIFICAÇÃO DE EQUIPAMENTOS E INSTRUMENTOS

1. MELHORES PRÁTICAS E UTILIZAÇÃO DOS INSTRUMENTOS E EQUIPAMENTOS EXISTENTES

Nem sempre são necessárias soluções tecnológicas totalmente novas para enfrentar de forma eficaz ameaças existentes ou novas. Frequentemente, os orçamentos públicos não estão em condições de as financiar. Por conseguinte, deve prestar-se igualmente atenção à forma como instrumentos já existentes e adquiridos anteriormente podem ser modernizados ou utilizados mais eficazmente. Pode tratar-se de uma forma económica de melhorar a eficácia, aumentar a fiabilidade e diminuir o número de falsos alarmes.

Não existe um mecanismo de intercâmbio de experiências sobre estas questões entre as autoridades dos vários Estados-Membros. Poderiam, por exemplo, ser partilhadas informações sobre melhorias obtidas através de alterações do processo de funcionamento ou sobre iniciativas de modernização economicamente eficazes.

Perguntas

Qual seria a melhor forma de identificar e partilhar as boas práticas nesta matéria?

Identificação de boas práticas

Através da avaliação entre pares ou de questionários enviados aos Estados-Membros?

Divulgação de boas práticas

Através de uma base de dados segura e pesquisável ou em reuniões e seminários?

Solicitam-se sugestões sobre quaisquer outras opções para identificar e divulgar as boas práticas nesta matéria

Se for considerado necessário modernizar um instrumento ou equipamento e nenhuma autoridade de outros Estados-Membros tiver dado passos nesse sentido, considerar-se-ia aceitável a consulta do sector privado sobre esta matéria?

2. IDENTIFICAÇÃO E DIVULGAÇÃO DAS BOAS PRÁTICAS E UTILIZAÇÃO DOS NOVOS INSTRUMENTOS E EQUIPAMENTOS

No seu trabalho, as autoridades nacionais podem igualmente beneficiar de um sistema que facilite o intercâmbio de informações sobre a utilização dos novos instrumentos e equipamentos e lhes permita evoluir com base nas experiências das suas congéneres e aproveitar a experiência destas. Um tal intercâmbio de informações, experiências e boas práticas em matéria de instrumentos e equipamentos poderia ajudar as autoridades a identificar equipamentos que correspondessem às suas necessidades específicas.

Além disso, poderiam ser promovidos os ensaios de equipamentos novos ou experimentais através do co-financiamento por parte do orçamento comunitário e/ou do sector privado. Ensaios mais amplos de equipamentos novos e experimentais poderiam contribuir para que a indústria europeia convertesse a investigação em matéria de segurança em produtos eficazes e competitivos.

Perguntas

Qual seria a melhor forma de identificar e partilhar as informações e as boas práticas nesta matéria?

Identificação das boas práticas

Através da avaliação entre pares ou de questionários enviados aos Estados-Membros?

Divulgação da informação e das boas práticas

Através de uma base de dados segura e pesquisável ou em reuniões e seminários restritos?

Têm quaisquer outras sugestões sobre como identificar as melhores práticas nesta matéria e sobre a sua divulgação eficaz?

Instrumentos experimentais e novos

Estão interessados no ensaio de instrumentos e equipamentos novos ou experimentais?

Se sim/não, queiram especificar

Teria interesse o financiamento parcial de ensaios de instrumentos e equipamentos novos e experimentais pela Comunidade e/ou o sector privado?

3. UTILIZAÇÃO DE INSTRUMENTOS DE MINERAÇÃO DE DADOS E TEXTO

As autoridades de segurança nacionais e europeias têm de fazer face a um aumento constante do volume da documentação e informações que têm de processar. Para abordar este desafio de forma mais eficaz, existem instrumentos modernos de software para a mineração de dados e texto. Esta tecnologia pode ajudar a extrair informações relevantes de um elevadíssimo número de documentos. A título de exemplo, é possível filtrar inteligentemente texto e documentos para ajudar a navegação (agregação de documentos), para a autocategorização (canalizando e prioritizando o fluxo de documentos no âmbito de equipas de investigação) e para a verificação da validade da utilização de códigos. Os objectivos são os seguintes:

- panorâmica rápida das entidades-chave nas colecções de documentos;
- pré-processamento com vista à investigação documental orientada;
- classificação de documentos com base no conteúdo para ajudar a orientar análises subsequentes;
- análise automatizada das informações provenientes de várias fontes.

As potencialidades destes instrumentos modernos não estão a ser suficientemente exploradas pelos Estados-Membros. No entanto, ao promover a utilização destas tecnologias, há que analisar cuidadosamente se a sua utilização em determinadas aplicações, como o controlo de mensagens de correio electrónico, constitui ou não uma ingerência no direito fundamental dos cidadãos ao respeito da vida privada. As mensagens de correio electrónico são correspondência e, como tal, abrangidas pelo direito à confidencialidade da comunicação consagrado na Convenção Europeia dos Direitos do Homem. O recurso a quaisquer técnicas de mineração de dados e texto deve, por conseguinte, estar em conformidade com a lei, ser necessário numa sociedade democrática para proteger um interesse público importante e ser proporcional ao interesse público em causa. Tais instrumentos, bem como a sua aplicação, devem respeitar intrinsecamente os direitos fundamentais e os princípios de protecção de dados. Por último, estas actividades serão levadas a cabo sob o controlo e supervisão das autoridades públicas competentes.

Perguntas

Exercício de sensibilização

Os Estados-Membros e os organismos europeus relevantes estariam interessados no intercâmbio das boas práticas e nos benefícios potenciais decorrentes da utilização de instrumentos de mineração de dados e texto?

As autoridades dos Estados-Membros que utilizam esta tecnologia estariam dispostas a partilhar a experiência com as suas congéneres?

Seriam úteis seminários restritos sobre esta matéria organizados pelos Estados-Membros, pela Europol ou pelo OLAF ?

Melhoria da capacidade da UE em matéria de mineração de dados e texto

Um centro de excelência a nível europeu acessível a todos os Estados-Membros e às respectivas autoridades competentes contribuiria para aproveitar na prática as potencialidades destes instrumentos?

Em caso negativo, que outras opções sugerem para maximizar as potencialidades destes instrumentos?

Identificação e divulgação das boas práticas

Uma avaliação por pares ou um questionário enviado aos Estados-Membros seriam úteis para a identificação das boas práticas de utilização destes instrumentos?

Em caso negativo, que outras abordagens sugerem para identificar as boas práticas nesta matéria?

Melhoria das capacidades regionais da UE em matéria de mineração de dados e texto

Haveria uma capacidade de reserva disponível nos Estados-Membros e em organismos europeus para ajudar os Estados-Membros que não possuem esta tecnologia a processar os respectivos documentos?

Na ausência dessa capacidade de reserva ou caso exista apenas uma capacidade limitada, seria útil e prático um aumento financiado pela UE da capacidade dos Estados-Membros ou a nível europeu ?

Os Estados-Membros que não dispõem de uma capacidade suficiente de mineração de dados e texto .ponderariam utilizar instrumentos de outros organismos caso estes fossem tornados disponíveis?

Seria possível criar centros europeus ou regionais de mineração de dados e texto que vários Estados-Membros e as respectivas autoridades pudessem utilizar ?

Os instrumentos existentes de mineração de dados e texto cobrem adequadamente as várias línguas da Europa?

Há instrumentos adequados para apoiar as autoridades que processam textos e documentos em línguas estrangeiras?

Outros

Se discordam de algumas das opções acima sugeridas, como abordariam as preocupações evocadas neste ponto?

4. ENSAIOS E CERTIFICAÇÃO DA QUALIDADE DO EQUIPAMENTO E DOS INSTRUMENTOS

O mercado já oferece vários produtos de detecção. No entanto, é frequentemente muito difícil identificar os melhores instrumentos e produtos ou, pelo menos, os que satisfazem determinados requisitos mínimos. Um sistema a nível de toda a UE para a certificação de instrumentos de boa qualidade e para a sua comparação, concebido para simplificar o processo de determinação dos instrumentos ou equipamentos que podem satisfazer as necessidades específicas de uma dada autoridade, poderia colmatar esta lacuna. Tal sistema poderia facilitar as decisões de aquisição de equipamentos e instrumentos por parte das autoridades nacionais. Poderia igualmente ajudar as autoridades a utilizar de forma optimizada recursos necessariamente escassos.

Poderia ser estabelecida uma rede de autoridades de certificação *nacionais* que partilhasse experiência e conhecimentos para colmatar a ausência de um sistema de determinação da qualidade dos instrumentos. Estas autoridades poderiam igualmente aprovar normas para a comparação e certificação de soluções tecnológicas de boa qualidade. Este tipo de certificação poderia não só ser utilizado para ajudar as autoridades nacionais a determinar se um instrumento é ou não adequado como também para divulgar soluções europeias noutros mercados. É evidente que, por razões de segurança, o desenvolvimento de protocolos de ensaio não pode ser objecto de debate público.

Pergunta

Seria útil a criação de uma rede de autoridades de certificação nacionais para o intercâmbio de experiências e conhecimentos, bem como de um sistema certificação e avaliação comparativa da qualidade?

Em caso negativo, que outra solução sugerem para abordar este problema ?

Seriam úteis normas comuns de certificação e avaliação comparativa da qualidade ? Caso contrário, como assegurariam a transparência deste processo e a utilização dos resultados a nível da UE?

IV. ESTUDOS[5]

Os participantes na conferência identificaram diversos tópicos que requerem novos estudos. Por conseguinte, a Comissão propõe a realização de estudos sobre:

(1) tecnologias e protecção de eventos de massas;

(2) obstáculos à cooperação e à partilha de informações entre laboratórios forenses e institutos de investigação em matéria de segurança;

(3) disposições jurídicas que regulamentam a utilização de tecnologias de detecção específicas;

(4) utilização prática de tecnologias de detecção específicas;

(5) quadro normativo que rege o recurso à detecção de pessoas (incluindo a vigilância) a nível da UE;

(6) níveis de aceitação da detecção de pessoas (incluindo a vigilância e a utilização da biometria) na UE.

Em termos gerais, o objectivo dos estudos é utilizá-los como instrumento para aumentar o conhecimento dos intervenientes relevantes e assegurar o respeito dos quadros normativos existentes aquando da elaboração ou utilização de tecnologias de detecção. Noutros casos, os estudos poderiam ser utilizados para analisar opções de política e opções respeitantes a novas medidas práticas.

Pergunta

Estariam interessados em receber estudos relativos a estes temas baseados na informação de base constante do Anexo?

Em caso negativo, queiram especificar os motivos e sugerir abordagens alternativas dos problemas levantados.

[5] Para uma descrição mais aprofundada das ideias subjacentes à necessidade destes estudos, ver parte III do Anexo.

V. APLICAÇÃO DOS RESULTADOS DA CONSULTA

1. MELHORIA DO DIÁLOGO ESPECÍFICO ENTRE OS SECTORES PÚBLICO E PRIVADO SOBRE AS TECNOLOGIAS DE DETECÇÃO E TECNOLOGIAS CONEXAS

O presente Livro Verde expõe várias actividades que podem contribuir para melhorar a interacção entre os sectores público e privado no domínio das tecnologias de detecção, contribuindo assim para que as autoridades de segurança dos Estados-Membros tenham acesso aos melhores instrumentos, soluções e práticas disponíveis. Por outro lado, estas actividades podem ajudar a recentrar o investimento do sector privado e a adequá-lo às necessidades do sector público. É, no entanto, óbvio que para tal é necessária uma cooperação estreita entre os sectores público e privado. Por conseguinte é necessário melhorar o diálogo específico sobre esta matéria entre os sectores público e privado, que pode envolver várias modalidades, nomeadamente o estabelecimento de um organismo específico ou a criação de um grupo específico no quadro de exercícios horizontais de parceria entre o sector público e o sector privado ligados à segurança que devem ser lançados proximamente.

O objectivo desta actividade não será concorrer com os organismos existentes (como o ESRAB), mas sim colmatar lacunas na articulação entre os sectores público e privado que envolvam as autoridades de segurança competentes a nível europeu. Também não deve tratar-se de um organismo permanente; deve ter objectivos claramente definidos e ser extinto logo que estes objectivos sejam alcançados. Serviria como fórum para os peritos dos sectores público e privado, ajudando a abordar as questões levantadas no presente documento ou novos desafios que possam surgir durante a aplicação dos resultados da consulta pública sobre o presente documento.

Por outro lado, é claro que algumas das acções possíveis propostas no presente documento requerem iniciativas dos Estados-Membros sem a participação do sector privado. Além disso, a definição das tarefas de uma tal cooperação estará sujeita a um acordo entre os sectores público e privado e, graças à sua participação, os Estados-Membros poderiam influenciar o seu papel e objectivos. Terá igualmente de abordar a questão do intercâmbio de informações confidenciais entre os sectores público e privado, embora importe sublinhar que o sector público não é o único repositório de informações sensíveis.

Pergunta

Um instrumento como a melhoria do diálogo específico entre os sectores público e privado em matéria de tecnologias de detecção e tecnologias conexas será útil para a aplicação dos resultados da consulta pública sobre o presente documento?

Em caso afirmativo, aceitam as sugestões acima apresentadas ou têm ideias diferentes?

Em caso negativo, que outros mecanismos sugerem para acompanhar os resultados da consulta pública relativa ao presente documento?

Estariam interessados em contribuir para o seu trabalho ou em participar nele directamente?

2. PLANO DE ACÇÃO

A nível nacional e europeu, os planos de acção revelaram-se um bom instrumento para supervisar a acção em domínios complexos, como a luta contra o terrorismo ou a criminalidade. A conferência e o presente documento suscitaram numerosas questões em relação às tecnologias de detecção e tecnologias conexas no trabalho das autoridades de segurança competentes. Para acompanhar os progressos neste domínio e para estabelecer objectivos, poderia ser elaborado um plano de acção baseado nas respostas a estas questões e, se necessário, noutras consultas.

Pergunta
Um plano de acção seria um instrumento útil para aplicar as medidas apontadas nas respostas ao presente documento?

Observação final

As respostas ao presente documento devem ser enviadas por correio electrónico até 10 de Janeiro de 2007 para o seguinte endereço: **JLS-D1-Detection@ec.europa.eu**. Todas as respostas, quer do sector público quer do sector privado, serão publicadas no sítio Internet da Comissão, a menos que os inquiridos indiquem expressamente que pretendem preservar a confidencialidade de determinadas informações.

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 categories [6] 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) of 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.