COMISSÃO DAS COMUNIDADES EUROPEIAS

Bruxelas, 22.5.2007
COM(2007) 267 final

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO E AO COMITÉ DAS REGIÕES

Rumo a uma política geral de luta contra o cibercrime

{SEC(2007) 641}
{SEC(2007) 642}

COMUNICAÇÃO DA COMISSÃO
AO PARLAMENTO EUROPEU, AO CONSELHO
E AO COMITÉ DAS REGIÕES

Rumo a uma política geral de luta contra o cibercrime

1. INTRODUÇÃO

1.1. Em que consiste o cibercrime?

A segurança dos sistemas de informação, cada vez mais importantes nas nossas sociedades, abrange muitos aspectos, entre os quais a luta contra o cibercrime é um elemento crucial. Na ausência de uma definição consensual de cibercrime, as expressões "cibercrime", "crime informático", "crime relacionado com a informática" ou "crime de alta tecnologia" são utilizados com frequência de forma aleatória. Para efeitos da presente comunicação, entende-se por cibercrime "os actos criminosos praticados com recurso a redes de comunicações electrónicas e sistemas de informação ou contra este tipo de redes e sistemas".

Na prática, o termo cibercrime aplica-se a três categorias de actividades criminosas. A primeira abrange **formas tradicionais da criminalidade**, como a fraude ou a falsificação, apesar de no contexto do cibercrime se ligar especificamente a crimes cometidos em redes de comunicações electrónicas e sistemas de informação (a seguir designados "redes electrónicas"). A segunda refere-se à publicação de **conteúdos ilícitos** em meios de comunicação electrónicos (entre outros, pornografia infantil ou incitamento ao ódio racial). A terceira inclui **crimes exclusivos das redes electrónicas**, isto é, ataques contra sistemas de informação, bloqueio de serviços e pirataria. Estes tipos de ataques podem igualmente dirigir-se contra infra-estruturas críticas essenciais da Europa e afectar os sistemas de alerta rápido existentes em diversos domínios, com consequências potencialmente desastrosas para a sociedade no seu conjunto. É comum a todas as referidas categorias de crimes o facto de poderem ser cometidos em grande escala e de ser muito grande a distância geográfica entre o acto criminoso e os seus efeitos. Deste modo, os aspectos técnicos dos métodos de investigação aplicada são frequentemente os mesmos. A presente comunicação trata dos aspectos comuns atrás referidos.

1.2. Últimos desenvolvimentos em matéria de cibercrime

1.2.1. Gerais

A combinação de actividades criminosas em constante evolução com a falta de informação fiável torna difícil obter uma imagem exacta da situação actual. No entanto, podem ser identificadas algumas tendências gerais:

- O número de cibercrimes está a aumentar e as actividades criminosas estão a tornar-se cada vez mais sofisticadas e internacionalizadas[1]

- Há indicações claras no sentido de um envolvimento crescente de organizações criminosas no cibercrime

- Porém, o número de processos penais europeus com origem na cooperação policial transfronteiriça não aumenta

1.2.2. Crime tradicional nas redes electrónicas

A maior parte dos crimes pode ser cometida através da utilização de redes electrónicas, sendo especialmente comuns diversos tipos de fraude e de tentativas de fraude, constituindo formas crescentes de crime em redes electrónicas. Os instrumentos como a usurpação de identidade, o *phishing*[2] (ciber-iscagem), os *spams* (mensagens comerciais não solicitadas) e os códigos malévolos podem ser utilizados para cometer fraudes em larga escala. O comércio ilícito nacional e internacional realizado através da Internet também constitui um problema crescente. Este comércio inclui drogas, espécies ameaçadas e armas.

1.2.3. Conteúdos ilícitos

É cada vez maior o número de *sites* com conteúdos ilícitos acessíveis na Europa, incluindo pornografia infantil, incitamentos a actos terroristas, glorificação ilícita da violência, do terrorismo, do racismo e da xenofobia. As acções repressivas contra esses *sites* são extremamente difíceis, dados que os seus proprietários e administradores se encontram muitas vezes em países diferentes do país-alvo e muitas vezes mesmo fora da UE. Os *sites* podem ser transferidos muito rapidamente, mesmo para o exterior do território da UE, e a definição de ilicitude varia consideravelmente de país para país.

1.2.4. Crimes exclusivos das redes electrónicas

Ao que tudo indica, os ataques de larga escala contra sistemas de informação ou organizações e particulares (com frequências, através das chamadas *botnets*[3]) tornaram-se cada vez mais predominantes. Ocorreram também há pouco incidentes com ataques directos sistemáticos, bem coordenados e de larga escala contra infra-estruturas de informação cruciais de um país. Isto foi possível devido à fusão de tecnologias e à interligação acelerada de sistemas de informação, tornando-os mais vulneráveis. Os ataques são muitas vezes bem organizados e utilizados para efeitos de extorsão. Pode partir-se do princípio de que as ocorrências participadas são poucas, em parte devido aos prejuízos comerciais que podem resultar para as empresas caso o público fique a conhecer os problemas de segurança verificados.

---

1 A maioria das referências da presente comunicação às tendências actuais foram retiradas do estudo de avaliação do impacto de uma comunicação sobre o cibercrime, encomendado pela Comissão em 2006 (contrato n.º JLS/2006/A1/003).

2 Por phishing entende-se as tentativas fraudulentas de obtenção de informações sensíveis, como senhas e dados do cartão de crédito, através de uma comunicação electrónica, utilizando uma identidade falsa que se faz passar por verdadeira.

3 A *botnet* refere-se a um conjunto de máquinas que executam programas sob um comando comum.

1.3. Objectivos

Neste contexto de mudança, é urgente tomar medidas – a nível nacional mas também a nível europeu – contra todas as formas de cibercrime, que representam ameaças cada vez mais pesadas para as infra-estruturas cruciais, a sociedade, as empresas e os cidadãos. A protecção dos particulares contra o cibercrime é, muitas vezes, comprometida por questões relacionadas com a determinação do tribunal competente, da lei aplicável, da aplicação transfronteiriça ou do reconhecimento ou utilização de provas electrónicas. A dimensão essencialmente transfronteiriça do cibercrime realça estas dificuldades. Para contrariar estas ameaças, a Comissão está a lançar uma iniciativa política geral para melhorar a cooperação a nível europeu e internacional no domínio da luta contra o cibercrime.

O objectivo é reforçar a luta contra o cibercrime a nível nacional, europeu e internacional. Há muito que os Estados-Membros e a Comissão reconhecem que o desenvolvimento de uma política comunitária específica nesta matéria constitui uma prioridade. A iniciativa centrar-se-á nas dimensões de cumprimento da lei e de direito penal e a política virá complementar outras acções da UE para o reforço da segurança no ciberespaço em geral. Esta política englobará: melhor cooperação operacional para as acções policiais; melhor coordenação política e coordenação entre os Estados-Membros; cooperação política e jurídica com países terceiros; maior sensibilização; formação profissional; investigação; um diálogo reforçado com a indústria e eventuais medidas legislativas.

A política de luta e repressão do cibercrime será definida e executada no pleno respeito pelos direitos fundamentais, em especial a liberdade de expressão, o respeito pela vida privada e familiar e a protecção dos dados pessoais. Qualquer medida legislativa a tomar no contexto desta política será previamente analisada relativamente à compatibilidade com os referidos direitos, nomeadamente com a Carta dos Direitos Fundamentais da UE. Note-se igualmente que todas as iniciativas políticas deste tipo serão levadas a cabo em conformidade com os artigos 12.º a 15.º da chamada directiva do comércio electrónico[4], sempre que esta for aplicável.

O objectivo da presente comunicação pode ser dividido em três vertentes operacionais principais, que se podem resumir da seguinte forma:

- Melhorar e facilitar a coordenação e a cooperação entre as unidades de cibercrime, outras autoridades competentes e outros peritos na União Europeia

- Desenvolver – em coordenação com os Estados-Membros, organizações comunitárias e internacionais relevantes e outros interessados – um quadro político comunitário coerente no domínio da luta contra o cibercrime

- Aumentar a sensibilização para os custos e os perigos do cibercrime

---

[4] Directiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno (JO L 178, 17.7.2000, p. 1).

2. INSTRUMENTOS LEGAIS VIGENTES EM MATÉRIA DE LUTA CONTRA O CIBERCRIME

2.1. Instrumentos e medidas vigentes a nível comunitário

A presente comunicação sobre o cibercrime consolida e desenvolve a comunicação de 2001 com o título *Criar uma Sociedade da Informação mais segura reforçando a segurança das infra-estruturas de informação e lutando contra a cibercriminalidade*[5] (a seguir designada Comunicação de 2001). A Comunicação de 2001 propunha disposições materiais e processuais adequadas para combater as actividades criminosas nacionais e transnacionais. A esta comunicação seguiram-se várias propostas importantes, incluindo nomeadamente a proposta que conduziu à Decisão-Quadro 2005/222/JAI relativa a ataques contra os sistemas de informação[6]. Neste contexto, note-se igualmente que foi adoptada outra legislação, mais geral, que abrange igualmente aspectos da luta contra o cibercrime, como a Decisão-Quadro 2001/413/JAI relativa ao combate à fraude e à contrafacção de meios de pagamento que não em numerário[7].

A Decisão-Quadro 2004/68/JAI relativa à exploração sexual de crianças[8] é um bom exemplo da atenção especial que a Comissão dedica à **protecção de crianças**, especialmente no que se refere à luta contra todas as formas de publicação ilícita de pornografia infantil através de sistemas de informação, uma prioridade horizontal que será mantida no futuro.

Para enfrentar os desafios que se colocam à sociedade da informação no domínio da segurança, a Comissão Europeia desenvolveu uma abordagem tripartida relativamente à segurança das redes e da informação: medidas específicas em matéria de segurança das redes e da informação, quadro normativo para as comunicações electrónicas e luta contra o cibercrime. Embora estes três aspectos possam, até certo ponto, ser desenvolvidos separadamente, as numerosas interdependências exigem uma estratégia coordenada. No domínio conexo da segurança das redes e da informação, foi adoptada em 2001, paralelamente à comunicação sobre o cibercrime, uma comunicação com o título *Segurança das redes e da informação: proposta de abordagem de uma política europeia*[9]. A Directiva 2002/58/CE, relativa à privacidade das comunicações electrónicas, estabelece que os prestadores de serviços de comunicações electrónicas publicamente disponíveis devem tomar medidas adequadas para garantir a segurança dos seus serviços. Esta directiva inclui também disposições contra o *spam* e o *software*-espião. A política de segurança das redes e da informação tem vindo a ser desenvolvida desde então através de diversas medidas, entre as quais, mais recentemente, as comunicações *Estratégia para uma sociedade da informação segura*[10], que determina a estratégia revitalizada e prevê o quadro para prosseguir e aperfeiçoar uma abordagem coerente para a segurança das redes e da informação, e *Combater o* spam*, o* spyware *e o* malware[11] e, em 2004, a criação da Agência Europeia para a Segurança das Redes e da Informação[12]. O objectivo principal desta agência é desenvolver competências para estimular a cooperação entre os sectores público e privado e prestar assistência à

---

5 COM(2000) 890, 26.1.2001.
6 JO L 69 de 16.3.2005, p. 67.
7 JO L 149 de 2.6.2001, p. 1.
8 JO L 13 de 20.1.2004, p. 44.
9 COM(2001) 298.
10 COM(2006) 251.
11 COM(2006) 688.
12 Regulamento (CE) n.º 460/2004 que cria a Agência Europeia para a Segurança das Redes e da Informação, (JO L 77 de 13.3.2004, p. 1).

Comissão e aos Estados-Membros. Os **resultados da investigação** dedicada às tecnologias no domínio da segurança dos sistemas de informação terá também um papel importante na luta contra o cibercrime. Por conseguinte, as tecnologias da informação e da comunicação, assim como a segurança, são referidas como objectivos no sétimo programa-quadro de investigação da UE (PQ 7), aplicável durante o período de 2007-2013[13]. A revisão do quadro normativo das comunicações electrónicas pode dar origem a alterações no intuito de reforçar a eficácia das disposições em matéria de segurança da directiva relativa à privacidade das comunicações electrónicas e da directiva do serviço universal (2002/22/CE)[14].

2.2. Instrumentos internacionais vigentes

Dada a natureza global das redes de informação, nenhuma política de combate ao cibercrime pode ser eficaz se os esforços se limitarem à UE. Os criminosos podem atacar sistemas de informação ou cometer crimes de um Estado-Membro para outro, mas também a partir de territórios exteriores à UE. Por conseguinte, a Comissão participou activamente em debates internacionais e estruturas de cooperação, entre outros no Grupo do G8 Lião-Roma para o crime ligado às tecnologias de ponta e em projectos geridos pela Interpol. A Comissão acompanha especialmente o trabalho da rede permanente (24 horas) de contactos para o crime internacional ligado às tecnologias de ponta, a rede 24/7[15], da qual são membros bastantes países do mundo, incluindo a maioria dos Estados-Membros da UE. A rede do G8 constitui um mecanismo para favorecer os contactos entre os países participantes, com pontos de contacto que funcionam 24 horas por dia para os casos que envolvem provas electrónicas e os que carecem de assistência urgente de autoridades policiais estrangeiras.

Efectivamente, o instrumento europeu e internacional predominante neste domínio é a Convenção do Conselho da Europa sobre o cibercrime de 2001[16]. Esta convenção – que foi adoptada e entrou em vigor em 2004 – inclui definições comuns de diferentes tipos de cibercrimes e estabelece as bases para uma cooperação judicial eficaz entre os Estados contratantes. Foi assinada por muitos Estados, incluindo os EUA, outros países não europeus e todos os Estados-Membros. Alguns Estados-Membros, porém, ainda não ratificaram a convenção ou o protocolo adicional referente a actos de natureza racista ou xenófoba praticados através de sistemas informáticos. Atendendo à importância consensual atribuída à convenção, a Comissão instará os Estados-Membros e países terceiros relevantes a ratificá-la e irá ponderar a possibilidade de a Comunidade Europeia se tornar parte da mesma.

---

13 A União Europeia apoiou já, no âmbito do 6.º programa-quadro de investigação e desenvolvimento tecnológico, uma série de projectos de investigação relevantes e bem-sucedidos.

14 COM(2006) 334, SEC(2006) 816 e SEC(2006) 817.

15 Ver artigo 35.º da Convenção do Conselho da Europa sobre o cibercrime.

16 http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

3. DESENVOLVIMENTO DE INSTRUMENTOS ESPECÍFICOS DE LUTA CONTRA O CIBERCRIME

3.1. Reforço da cooperação operacional dos serviços de polícia e dos esforços de formação profissional a nível da UE

A ausência, ou subutilização, de estruturas imediatas para a **cooperação operacional transfronteiriça** constitui ainda uma das maiores fraquezas no contexto da Justiça, Liberdade e Segurança. A assistência mútua tradicional tem-se revelado lenta e ineficaz em casos urgentes de cibercrime e ainda não foram desenvolvidas de forma satisfatória novas estruturas de cooperação. Apesar de na Europa as autoridades judiciais e policiais, a nível nacional, cooperarem estreitamente através da Europol, Eurojust e outras estruturas, é ainda necessário reforçar e clarificar as responsabilidades. As consultas efectuadas pela Comissão indicam que estes canais essenciais não são utilizados de forma optimizada. A abordagem europeia mais coordenada deve ser operacional e estratégica e abranger também a troca de informações e as melhores práticas.

A Comissão irá, daqui para a frente, dedicar especial atenção às necessidades de **formação profissional**. É um facto que os desenvolvimentos tecnológicos criam uma necessidade de formação contínua em matéria de cibercrime para as autoridades policiais e judiciais. Prevê-se, assim, um apoio financeiro reforçado e mais bem coordenado da UE a programas de formação multinacionais. A Comissão irá igualmente trabalhar, em estreita cooperação com os Estados-Membros e outros organismos competentes como a Europol, a Eurojust, a Academia Europeia de Polícia (CEPOL) e a Rede Europeia de Formação Judiciária (REFJ), para alcançar uma cooperação a nível comunitário e interligar todos os programas de formação úteis.

A Comissão irá organizar uma **reunião** de peritos no domínio das acções policiais, não só dos Estados-Membros mas também da Europol, CEPOL e REFJ, para debater os modos de melhorar a cooperação estratégica e operacional e a formação em matéria de cibercrime na Europa em 2007. Entre outros aspectos, será ponderada a criação de um ponto de contacto permanente da UE para a troca de informações e de uma plataforma de formação profissional em matéria de cibercrime. A reunião de 2007 será a primeira de uma série de reuniões previstas para um futuro próximo.

3.2. Reforçar o diálogo com a indústria

Tanto o sector privado como o sector público têm interesse em desenvolver, em conjunto, métodos de identificação e prevenção dos danos resultantes de actividades criminosas. A participação partilhada dos sectores público e privado, baseada na confiança mútua e num objectivo comum de redução dos danos, afigura-se uma forma eficaz de reforçar a segurança, também na luta contra o cibercrime. Os aspectos público–privado da política da Comissão no domínio do cibercrime farão parte, em devido tempo, de uma política comunitária global prevista para o diálogo entre o sector público e o sector privado, abarcando toda a questão da segurança europeia. Esta última política será conduzida especialmente pelo Fórum Europeu da Investigação sobre Segurança e Inovação, que a Comissão tenciona criar em breve e que agrupará elementos representativos dos sectores público e privado.

O desenvolvimento das tecnologias da informação e dos sistemas de comunicações electrónicos modernos é controlado, em grande medida, por operadores privados. As empresas privadas avaliam as ameaças, estabelecem programas de luta contra o crime e desenvolvem soluções técnicas para o impedir. A indústria teve uma atitude muito positiva no que se refere à assistência prestada às autoridades públicas na luta contra o cibercrime, especialmente nos esforços para conter a pornografia infantil[17] e outros tipos de conteúdos ilícitos na Internet.

Outra questão consiste na aparente ausência de trocas de informação, de conhecimentos especializados e de melhores práticas entre os sectores público e privado. Frequentemente, no intuito de proteger modelos e segredos das empresas, os operadores do sector privado resistem – ou não têm a obrigação legal de o fazer – a comunicar ou partilhar informação útil sobre ocorrências criminosas com as autoridades policiais. No entanto, estas informações podem ser necessárias para que as autoridades públicas possam formular uma política eficaz e adequada de combate ao crime. As possibilidades de melhorar as trocas de informações transversais serão também analisadas à luz das regras vigentes em matéria de dados pessoais.

A Comissão participa já activamente em várias estruturas de luta contra o cibercrime, como o Grupo de Peritos da UE no domínio da Prevenção da Fraude[18]. Para a Comissão, uma política geral eficaz de luta contra o cibercrime deve incluir também uma estratégia de cooperação entre os operadores dos sectores público e privado, incluindo organizações da sociedade civil.

Para conseguir uma cooperação mais ampla entre os sectores público e privado neste domínio, a Comissão organizará em 2007 uma conferência para os especialistas dos serviços de polícia e representantes do sector privado, especialmente prestadores de serviços na Internet, para debater as formas de melhorar a cooperação operacional entre os sectores público e privado na Europa[19]. A conferência irá abordar todas as questões que tragam valor acrescentado a ambos os sectores, mas especialmente as seguintes:

- Melhoria da cooperação institucional na luta contra as actividades e os conteúdos ilícitos na Internet, especificamente nos domínios do terrorismo, pornografia infantil e outras actividades ilícitas particularmente sensíveis do ponto de vista da protecção das crianças

- Esboço de acordos entre os sectores público e privado para bloquear a nível comunitário os *sites* com conteúdos ilícitos, especialmente pornografia infantil

- Concepção de um modelo europeu para a troca das informações necessárias e relevantes nos sectores público e privado, pensando na importância de cultivar um clima de confiança mútua e ter em conta os interesses de todos os implicados

- Criar uma rede de pontos de contacto de serviços de repressão do crime tanto no sector público como no sector privado

---

17 Um exemplo recente neste domínio é a cooperação entre serviços de polícia e empresas de cartões de crédito, que permitiu que a polícia conseguisse seguir, através destas empresas, o rasto dos compradores de pornografia infantil em linha.

18 Ver http://ec.europa.eu/internal_market/payments/fraud/index_en.htm

19 A conferência pode ser vista como a continuação do Fórum da UE apresentado no ponto 6.4 da comunicação sobre a cibercriminalidade.

3.3. Legislação

A harmonização geral das definições de crime e das legislações penais nacionais no domínio do cibercrime ainda não se afigura adequada, devido à variedade dos tipos de infracções abrangidos por este conceito. Visto que a cooperação eficaz entre os serviços policiais depende muitas vezes da existência de definições de crimes pelo menos parcialmente harmonizadas, continuar a harmonização da legislação dos Estados-Membros mantém-se como um dos objectivos a longo prazo[20]. Relativamente a determinadas definições-chave de crimes, a decisão-quadro sobre os ataques aos sistemas de informação constitui um passo importante. Como se descreveu atrás, novas ameaças surgiram entretanto e a Comissão acompanha de perto esta evolução, visto que é muito importante avaliar continuamente a necessidade de legislação adicional. O acompanhamento da evolução das ameaças é coordenado de perto com o Programa Europeu de Protecção das Infra-Estruturas Críticas.

Porém, deve igualmente ser prevista neste momento legislação específica de combate ao cibercrime. Um aspecto concreto que pode carecer de legislação consiste na situação em que o cibercrime é cometido juntamente com a **usurpação de identidade**. Em geral, entende-se por "usurpação de identidade" a utilização de dados de identificação pessoal, por exemplo o número do cartão de crédito, como instrumento para cometer outros crimes. Na maior parte dos Estados-Membros, o criminoso seria muito provavelmente julgado pela fraude, ou outro crime potencial, e não pela usurpação de identidade, visto que o primeiro é considerado um crime mais grave. A usurpação de identidade não é, em si, considerada crime em todos os Estados-Membros. É com frequência mais fácil provar o crime de usurpação de identidade do que o de fraude, pelo que a cooperação policial a nível comunitário ficaria mais bem servida se a usurpação de identidade fosse tipificada como crime em todos os Estados-Membros. Em 2007, a Comissão iniciará consultas para avaliar se é necessário aprovar legislação nesta matéria.

3.4. Desenvolvimento de dados estatísticos

É relativamente consensual que o actual estado da informação relativa à prevalência do crime é muito inadequado e, nomeadamente, que são necessários muitos esforços para melhorar a comparabilidade dos dados entre Estados-Membros. Numa comunicação de 7.8.2006, a Comissão apresentou um plano de acção ambicioso para abordar esta questão: *Elaboração de uma estratégia europeia global e coerente para a avaliação estatística da criminalidade e da justiça penal: Plano de Acção da UE para 2006-2010*[21]. O grupo de peritos criado no âmbito deste plano de acção constituirá um fórum adequado para o desenvolvimento de indicadores relevantes para medir a extensão do cibercrime.

4. CAMINHO A SEGUIR

A Comissão levará agora avante a política geral de luta contra o cibercrime. Visto que os seus poderes no domínio do direito penal são limitados, esta política pode apenas constituir um complemento às medidas tomadas pelos Estados-Membros e outros organismos. As medidas mais importantes – cada uma das quais implicará o recurso a um, a vários ou a todos os instrumentos descritos no ponto 3 – serão também custeadas através do programa financeiro "Prevenção e Luta contra a Criminalidade":

---

[20] Este objectivo de longo prazo já foi referido na página 3 da Comunicação de 2001.

[21] COM(2006) 437, 7.8.2006.

4.1. Luta contra o cibercrime em geral

- Estabelecer uma cooperação reforçada entre as autoridades policiais e judiciais dos Estados-Membros, uma medida que terá início com a organização de uma reunião de peritos em 2007 e que poderá incluir a criação de um ponto de contacto comunitário central para o cibercrime

- Aumentar o apoio financeiro a iniciativas no domínio da formação profissional das autoridades policiais e judiciais no que se refere ao tratamento dos casos de cibercrime e tomar medias para coordenar todos os esforços multinacionais de formação neste domínio através da criação de uma plataforma comunitária de formação profissional

- Promover um empenhamento mais forte dos Estados-Membros e todas as autoridades públicas no sentido de tomarem medidas eficazes contra o cibercrime e de afectarem recursos suficientes ao combate a este tipo de crime

- Apoiar a investigação que possa ajudar a luta contra o cibercrime

- Organizar pelo menos uma grande conferência (em 2007) com autoridades policiais e operadores privados, que visa especialmente iniciar a cooperação na luta contra as actividades ilícitas na Internet nas e contra as redes electrónicas e promover uma troca de informações mais eficaz sem ser a nível pessoal, e ainda acompanhar os resultados desta conferência de 2007 com projectos concretos de cooperação entre os sectores público e privado

- Tomar a iniciativa de organizar e participar em acções que impliquem os sectores público e privado destinadas a aumentar a sensibilização, especialmente entre os consumidores, para os custos e os perigos do cibercrime, evitando ao mesmo tempo afectar a confiança dos consumidores e utilizadores referindo apenas os aspectos negativos da segurança

- Participar activamente e promover a cooperação global internacional na luta contra o cibercrime

- Iniciar, contribuir e custear projectos internacionais que seguem a política da Comissão neste domínio, por exemplo projectos geridos pelo G8 e que respeitem os documentos de estratégia nacionais e regionais (no que se refere à cooperação com países terceiros)

- Tomar medidas concretas para incentivar todos os Estados-Membros e países terceiros relevantes a ratificar a Convenção sobre o Cibercrime do Conselho da Europa e respectivo protocolo e ponderar a hipótese de a Comunidade se tornar parte desta convenção

- Analisar, juntamente com os Estados-Membros, o fenómeno dos ataques coordenados e de larga escala contra infra-estruturas de informação de Estados-Membros, a fim de os prevenir e combater, incluindo respostas coordenadas e partilha de informações e de melhores práticas

4.2. Luta contra a criminalidade tradicional nas redes electrónicas

- Iniciar uma análise aprofundada no intuito de redigir uma proposta de legislação comunitária especificamente contra a usurpação de identidade

- Promover o desenvolvimento de métodos e procedimento técnicos para combater a fraude e o comércio ilícito na Internet, incluindo projectos de cooperação entre os sectores público e privado

- Continuar e desenvolver o trabalho em domínios específicos, como o trabalho desenvolvido pelo grupo de peritos para a prevenção da fraude relativamente ao combate à fraude com meios de pagamento não monetários nas redes electrónicas

4.3. Conteúdos ilícitos

- Continuar a desenvolver acções contra conteúdos ilícitos específicos, especialmente no que se refere à pornografia infantil e ao incitamento ao terrorismo, nomeadamente através do acompanhamento da aplicação da decisão-quadro relativo à exploração sexual de crianças

- Instar os Estados-Membros a afectar recursos financeiros suficientes para reforçar o trabalho dos serviços policiais, dando especial atenção à identificação das vítimas da pornografia distribuída em linha

- Iniciar e apoiar acções contra conteúdos ilícitos que possam incitar menores a comportamentos violentos e outros gravemente punidos por lei, isto é, determinados tipos de jogos de vídeo em linha extremamente violentos

- Iniciar e promover o diálogo entre Estados-Membros e com países terceiros acerca dos métodos técnicos para combater os conteúdos ilícitos, bem como dos procedimentos para encerrar *sites* ilegais, também com vista à eventual celebração de acordos formais com países vizinhos e outros nesta matéria

- Elaborar acordos voluntários e convenções entre autoridades públicas e operadores privados, especialmente prestadores de serviços na Internet, relativos ao bloqueio e encerramento de *sites* ilegais da Internet

4.4. Acompanhamento

Na presente comunicação é indicada, como passo seguinte, uma série de medidas destinadas a melhorar as estruturas de cooperação da UE. A Comissão aplicará estas medidas, avaliará os progressos obtidos com a realização das acções e comunicará os resultados ao Conselho e ao Parlamento.