

PT

PT

PT



COMISSÃO EUROPEIA

Bruxelas, 30.9.2010
SEC(2010) 1123 final

DOCUMENTO DE TRABALHO DOS SERVIÇOS DA COMISSÃO

RESUMO DA AVALIAÇÃO DE IMPACTO

documento que acompanha a

Proposta de

DIRECTIVA DO PARLAMENTO EUROPEU E DO CONSELHO

**relativa a ataques contra os sistemas de informação e que revoga a Decisão-Quadro
2005/222/JAI do Conselho**

{COM(2010) 517 final}
{SEC(2010) 1122 final}

RESUMO DA AVALIAÇÃO DE IMPACTO

1. DEFINIÇÃO DO PROBLEMA

O número de ataques contra os sistemas de informação aumentou significativamente desde a adopção da Decisão-Quadro relativa a ataques contra os sistemas de informação, («Decisão-Quadro relativa a ataques»). Uma das empresas líderes em matéria de segurança da Internet declarou que as ameaças às informações confidenciais (em oposição às informações disponíveis ao público) aumentaram consideravelmente em 2008, tendo sido identificadas 1 656 227 novas ameaças nesse ano contra 624 267 anteriormente¹. Além disso, foram observados vários ataques perigosos em larga escala anteriormente desconhecidos, como os cometidos na Estónia e na Lituânia em 2007 e 2008, respectivamente. Em Março de 2009, os sistemas informáticos de organismos governamentais e do sector privado de 103 países foram atacados por uma rede de computadores «sequestrados», que extraíram documentos sensíveis e confidenciais² através do recurso a «botnets»³, ou seja, redes de computadores infectados que podem ser controlados à distância. Por último, assiste-se actualmente à disseminação de um «botnet» chamado «Conficker» (também conhecido por «Downup», «Downadup» e «Kido»), que se tem propagado e actuado numa escala sem precedentes desde Novembro de 2008, afectando milhões de computadores no mundo inteiro⁴.

Em segundo lugar, a falta de cooperação suficiente entre os Estados-Membros, nomeadamente dos serviços responsáveis pela aplicação da lei e das autoridades judiciais da UE, torna difícil dar uma resposta coordenada e eficaz a estes ataques. Embora segundo o relatório sobre a aplicação da Decisão-Quadro relativa a ataques uma maioria de Estados-Membros tenha instituído pontos de contacto permanentes, em conformidade com o exigido no artigo 11.º da Decisão-Quadro, subsistem problemas ligados à sua capacidade de resposta e de reacção a pedidos de cooperação urgentes⁵.

A existência de um ponto de contacto não constitui uma garantia do seu bom funcionamento. Nas suas notificações à Comissão, vários Estados-Membros indicaram que, embora os seus pontos de contacto estivessem operacionais, não funcionavam 24 horas por dia, como exigido pela Decisão-Quadro relativa a ataques. Isto significa que não podem responder a pedidos

¹ http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf, p.10.

² www.theglobeandmail.com/servlet/story/RTGAM.20090328.wspy0328/BNStory/International/home?cid=al_gam_mostemail

³ O termo «botnet» designa uma rede de computadores que foram infectados por *software* maligno (vírus informáticos). Essa rede de computadores «sequestrados» («zombies») pode ser activada para executar acções específicas, como atacar sistemas de informação (ciberataques). Estes «zombies» podem ser controlados – frequentemente sem o conhecimento dos utilizadores dos computadores «sequestrados» – por outro computador, igualmente conhecido como «centro de comando e de controlo». As pessoas que controlam este centro fazem parte dos infractores, já que utilizam os computadores «sequestrados» para lançar ataques contra os sistemas de informação. É muito difícil localizar os autores da infracção, dado que os computadores que formam o «botnet» e realizam o ataque podem encontrar-se num local diferente daquele em que se encontra o infractor.

⁴ http://www.lemonde.fr/technologies/article/2009/03/31/virus-conficker-catastrophe-ou-poisson-d-avril_1174916_651865.html

⁵ Relatório da Comissão ao Conselho apresentado nos termos do artigo 12.º da Decisão-Quadro do Conselho de 24 de Fevereiro de 2005, relativa a ataques contra os sistemas de informação, COM (2008) 0448 final.

urgentes fora das horas de expediente. A falta de eficácia dos pontos de contacto e a sua incapacidade para satisfazer pedidos de cooperação do sector privado constituem um obstáculo à cooperação entre os sectores público e privado.

Em terceiro lugar, ainda existem poucos dados disponíveis sobre os ciberataques, bem como sobre o acompanhamento policial e judicial dos mesmos. Nem todos os Estados-Membros recolhem dados relativos a ciberataques. Aqueles que o fazem aplicam um procedimento que não permite a comparação dos dados devido à divergência das metodologias estatísticas existente entre os Estados-Membros.

As vítimas de ataques em larga escala contra os sistemas de informação são o grande público, utilizador de sistemas de informação, assim como a administração central e local, as organizações internacionais e as entidades do sector privado.

Os ataques podem ser lançados em países terceiros contra alvos situados na UE e vice-versa.

2. SUBSIDIARIEDADE

A cibercriminalidade é um problema verdadeiramente internacional, contra o qual só raramente se pode lutar num contexto puramente nacional. A necessidade de realizar acções a nível da UE e internacional para prevenir e combater este problema é geralmente reconhecida. A maioria dos ataques ignora as fronteiras da UE. Os ataques afectam todos os Estados-Membros e está provado que uma percentagem significativa envolve actividades de vários Estados-Membros. Os sistemas de informação são muitas vezes tecnicamente interconectados e interdependentes para além das fronteiras. Por conseguinte, é consensual entre os peritos a necessidade de realizar acções tanto a nível internacional como da UE e que o objectivo de combater eficazmente este tipo de criminalidade não pode ser alcançado de forma satisfatória pelos Estados-Membros isoladamente.

Uma abordagem puramente nacional da cibercriminalidade corre o risco de produzir resultados fragmentados e ineficazes na Europa. As diferenças entre as abordagens nacionais e a falta de cooperação transfronteiriça sistemática reduzem sensivelmente a eficácia das medidas de combate tomadas a nível nacional. Tal deve-se em parte à interconexão dos sistemas de informação: um baixo nível de segurança num país pode aumentar a vulnerabilidade de outros países.

3. QUAIS SÃO OS OBJECTIVOS?

3.1 Objectivos gerais, específicos e operacionais

O objectivo global da acção da UE consiste em combater e reprimir a criminalidade, organizada ou não, em conformidade com o artigo 67.º do Tratado sobre o Funcionamento da União Europeia, lutando contra os ataques em larga escala contra os sistemas de informação.

A Objectivo específico: Reprimir e condenar os criminosos responsáveis pelos ataques em larga escala, através da aproximação do direito penal no domínio dos ataques contra os sistemas de informação

B Objectivo específico: Melhorar a cooperação transfronteiriça entre os serviços responsáveis pela aplicação da lei

C Objectivo específico: Estabelecer sistemas de acompanhamento e de recolha de dados eficazes

4. QUAIS SÃO AS OPÇÕES ESTRATÉGICAS?

4.1 Opção (1) *Statu quo*/Nenhuma nova acção da UE

Esta opção significa que a UE não tomará quaisquer outras medidas para combater este tipo específico de cibercriminalidade. Seriam prosseguidas as acções em curso, em especial os programas destinados a reforçar a protecção das infra-estruturas críticas da informação e a melhorar a cooperação entre os sectores público e privado face à cibercriminalidade.

4.2 Opção (2) Desenvolvimento de um programa com vista a intensificar os esforços para combater os ataques contra os sistemas de informação através de medidas não legislativas

Paralelamente ao programa destinado a reforçar a protecção das infra-estruturas críticas da informação, as medidas não legislativas centrar-se-iam na repressão transfronteiriça e na cooperação entre os sectores público e privado e deveriam facilitar uma acção mais coordenada a nível da UE. Uma proposta não legislativa poderia incluir acções como o reforço da rede de pontos de contacto disponíveis 24 horas por dia e 7 dias por semana dos organismos responsáveis pela aplicação da lei, a criação de uma rede da UE de pontos de contacto dos sectores público e privado que reúnam peritos em cibercriminalidade e organismos responsáveis pela aplicação da lei e a elaboração de um modelo de acordo da UE sobre os níveis de serviço, com vista à cooperação policial com os operadores do sector privado.

4.3 Opção (3) Actualização orientada das disposições da Decisão-Quadro relativa aos ataques para responder à ameaça de ataques em larga escala contra os sistemas de informação

Esta opção prevê a introdução de legislação específica orientada (ou seja, limitada) para impedir os ataques em larga escala particularmente perigosos contra os sistemas de informação. Esta legislação orientada seria acompanhada de medidas destinadas a reforçar a cooperação operacional transfronteiriça face aos ataques contra os sistemas de informação e reforçaria as sanções mínimas já previstas. Esta opção assumiria a forma de uma actualização da Decisão-Quadro relativa aos ataques, que seria completada por várias medidas não legislativas, como o reforço da preparação, segurança e resiliência das infra-estruturas críticas da informação, a sua protecção, o reforço dos instrumentos e procedimentos para a cooperação transfronteiriça entre os serviços responsáveis pela aplicação da lei, bem como o intercâmbio de boas práticas.

4.4 Opção (4) Introdução de legislação global da UE contra a cibercriminalidade

A constatação da necessidade de tomar medidas rápidas face ao desenvolvimento de ataques sofisticados contra os sistemas de informação suscita a questão da oportunidade de introduzir legislação da UE mais abrangente contra a cibercriminalidade em geral. Tal legislação cobriria não só os ataques contra os sistemas de informação, mas também aspectos como a cibercriminalidade financeira, a difusão de conteúdos ilegais na Internet, a recolha/armazenagem/transfêrencia de provas electrónicas e a elaboração de regras de competência mais precisas. Esta legislação da UE seria aplicável paralelamente à Convenção

do Conselho da Europa sobre Criminalidade Informática, que seria completada por novas disposições consideradas necessárias na UE.

4.5 Opção (5) Actualização da Convenção do Conselho da Europa sobre Criminalidade Informática

Esta opção exigiria a renegociação de uma parte substancial da actual Convenção, um processo moroso e, portanto, incompatível com o calendário de acção proposto na avaliação de impacto. A nível internacional não parece haver vontade de renegociar a Convenção. Por conseguinte, a sua actualização não pode ser considerada uma opção viável, já que ultrapassaria o prazo previsto para a acção.

5. AVALIAÇÃO DE IMPACTOS

Opções	Impacto económico	Impacto social	Impacto a nível dos direitos fundamentais	Impacto sobre os países terceiros	Pertinência para os objectivos A, B e C	Coerência com o direito internacional
Opção 1 : <i>Statu quo</i> / Nenhuma nova acção da UE	0	0	0	-	0	0
Opção 2 : Desenvolvimento de um programa com vista a intensificar os esforços para combater os ataques contra os sistemas de informação através de medidas não legislativas	-/+	++	-/+	++	A + B ++ C +	-/+
Opção 3 : Actualização orientada das disposições da Decisão-Quadro relativa aos ataques para responder à ameaça de ataques em larga escala contra os sistemas de informação	--/++	-/+++	-/++	+++	A +++ B +++ C +++	++
Opção 4 : Introdução de legislação global da UE contra a cibercriminalidade	---/+++	+++	--/++	++	A ++ B ++ C ++	-/++
Opção preferida (Opções 2 e 3): Combinação de medidas não legislativas com uma actualização orientada da Decisão-Quadro relativa aos ataques	--/+++	+++	-/++	+++	A +++ B +++ C +++	++

6. COMPARAÇÃO DAS OPÇÕES

6.1 Opção (1) *Statu Quo*

Esta opção tornará inevitavelmente mais vulnerável a posição dos intervenientes privados, dos Estados-Membros e da União no seu conjunto na sua luta contra a cibercriminalidade, dada a natureza deste fenómeno e o crescimento que tem registado. Mesmo se o nível das acções em curso se mantivesse, seria necessário velar pela coordenação a nível europeu.

6.2 Opção (2) Desenvolvimento de um programa com vista a intensificar os esforços para combater os ataques contra os sistemas de informação através de medidas não legislativas

Esta opção tem todas as vantagens e desvantagens inerentes a um instrumento não vinculativo. O aspecto positivo é a possibilidade de descrever cada opção de forma coerente com as melhores práticas nacionais, facilitando assim a identificação das medidas mais eficazes.

Contudo, esta opção é menos eficaz em termos de realização dos objectivos.

6.3 Opção (3) Actualização orientada das disposições da Decisão-Quadro relativa aos ataques para responder à ameaça de ataques em larga escala contra os sistemas de informação

Esta opção permite responder de forma atempada e orientada aos problemas detectados. Aborda as questões de direito penal a ter em conta para reprimir eficazmente os autores destas infracções. Também melhora a cooperação internacional mediante a introdução de um mecanismo de assistência internacional imediata nos casos de pedidos urgentes de cooperação e promove a cooperação com o sector privado através de medidas de acompanhamento, como a realização de reuniões de peritos. No âmbito desta opção são também introduzidas várias circunstâncias agravantes, como a grande escala dos ataques e o facto de os ataques serem cometidos mediante a dissimulação da verdadeira identidade do seu autor e causando prejuízo ao titular legítimo da identidade.

Por último, para possibilitar a avaliação da extensão do problema, são introduzidas obrigações de acompanhamento.

6.4 Opção (4) Introdução de legislação global da UE contra a cibercriminalidade

Esta opção, tal como a opção 3, tem a mais-valia de estabelecer disposições vinculativas e, por conseguinte, prevê-se um maior grau de eficácia, se for aplicada na sua globalidade. Espera-se igualmente maximizar o impacto positivo dos instrumentos legislativos e não legislativos num leque mais vasto de questões ligadas à cibercriminalidade, e não só nos ataques em grande escala. Além disso, esta opção abordaria o quadro penal e melhoraria ao mesmo tempo a cooperação transfronteiriça entre os serviços responsáveis pela aplicação da lei. Todavia, nesta fase, esta abordagem global não reflecte um consenso das partes interessadas, embora a sua aplicação trouxesse maiores progressos para a luta contra a cibercriminalidade do que todas as outras opções.

7. OPÇÃO PRIVILEGIADA

Na sequência da análise do impacto económico e social e do impacto sobre os direitos fundamentais, as opções n.ºs 2 e 3, tendo em conta as soluções que propõem para os problemas, parecem mais susceptíveis de alcançar os objectivos estabelecidos.

Globalmente, a opção preferida seria uma combinação das opções 2 e 3, já que são complementares e, portanto, respondem melhor aos objectivos estabelecidos, quer no que diz respeito ao fundo quer em termos de calendário.

8. ACOMPANHAMENTO E AVALIAÇÃO

Deve ser publicado um relatório de aplicação no prazo de 2 anos a contar da data de entrada em vigor da directiva. Este relatório deve centrar-se na transposição exacta da directiva pelos Estados-Membros.

Além disso, devem ser feitas avaliações regulares para determinar de que modo e até que ponto a directiva terá contribuído para a realização dos seus objectivos. A primeira avaliação deve ser realizada no prazo de 5 anos após a entrada em vigor da directiva; posteriormente, a Comissão publicará relatórios de avaliação de 5 em 5 anos, que incluirão informações sobre a aplicação. Com base nas conclusões e recomendações das avaliações, a Comissão deve ponderar eventuais alterações ulteriores da directiva ou qualquer outra possível evolução da mesma.