CONSELHO DA UNIÃO EUROPEIA

Bruxelas, 2 de Abril de 2009 (03.04)
(OR. en)

8375/09

TELECOM 69
DATAPROTECT 24
JAI 192
PROCIV 46

NOTA DE ENVIO

de:	Secretário-Geral da Comissão Europeia, assinado por Jordi AYET PUIGARNAU, Director
data de recepção:	31 de Março de 2009
para:	Javier SOLANA, Secretário-Geral/Alto Representante
Assunto:	Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões relativa à protecção das infra-estruturas críticas da informação "Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência"

Envia-se em anexo, à atenção das delegações, o documento da Comissão – COM(2009) 149 final.

Anexo: COM(2009) 149 final

COMISSÃO DAS COMUNIDADES EUROPEIAS

Bruxelas, 30.3.2009
COM(2009) 149 final

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

relativa à protecção das infra-estruturas críticas da informação

"Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência"

{SEC(2009) 399}
{SEC(2009) 400}

(apresentada pela Comissão)

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

relativa à protecção das infra-estruturas críticas da informação

"Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência"

1. INTRODUÇÃO

As tecnologias da informação e das comunicações (TIC) estão cada vez mais integradas nas nossas actividades diárias. Alguns destes sistemas, serviços, redes e infra-estruturas TIC (em suma, infra-estruturas TIC) são uma parte vital da economia e da sociedade europeias, fornecendo produtos e serviços essenciais ou constituindo a plataforma subjacente a outras infra-estruturas críticas. São, em geral, considerados infra-estruturas críticas da informação (ICI)[1], já que a sua perturbação ou a sua destruição teria um forte impacto nas funções vitais da sociedade. Exemplos recentes são os ciberataques em grande escala contra a Estónia em 2007 e os cortes de cabos transcontinentais em 2008.

Em 2008, o Fórum Económico Mundial calculou que a probabilidade de ocorrer uma ruptura importante nas ICI nos próximos 10 anos era de 10 a 20%, com um potencial custo económico global de cerca de 250 000 000 000 USD[2].

A presente comunicação centra-se na prevenção, preparação e sensibilização e define um plano de acções imediatas para reforçar a segurança e a resiliência das ICI. Esta centragem é coerente com o debate lançado a pedido do Conselho e do Parlamento Europeu sobre os desafios e as prioridades da política de segurança das redes e da informação (SRI) e sobre os instrumentos mais adequados necessários a nível comunitário nesta matéria. As acções propostas são igualmente complementares das que visam prevenir, combater e reprimir as actividades criminosas e terroristas contra as ICI e procuram criar sinergias com as actividades comunitárias de investigação em curso ou previstas no domínio da segurança das redes e da informação, assim como com iniciativas internacionais neste domínio.

2. CONTEXTO POLÍTICO

A presente comunicação visa desenvolver a política europeia no sentido de reforçar a segurança e a confiança na sociedade da informação. Em 2005, a Comissão[3] tinha já sublinhado a necessidade urgente de coordenar esforços para aumentar a confiança das partes interessadas nas comunicações e serviços electrónicos. Nesse sentido, foi adoptada em 2006 uma estratégia para uma sociedade da informação segura[4]. Os seus elementos principais, nomeadamente os respeitantes à segurança e à resiliência das infra-estruturas TIC, foram

---

1 No documento COM(2005) 576 final foi proposta uma definição de ICI.
2 Global Risks 2008
3 COM(2005) 229
4 COM(2006) 251

aprovados na Resolução 2007/068/01 do Conselho. No entanto, o nível de adesão e de execução pelas partes interessadas afigura-se insuficiente. Esta estratégia reforça igualmente o papel, a nível táctico e operacional, da Agência Europeia para a Segurança das Redes e da Informação (ENISA), instituída em 2004 com a missão de contribuir para os objectivos de assegurar um nível elevado e efectivo de segurança das redes e da informação (SRI) na Comunidade e desenvolver uma cultura de SRI em favor dos cidadãos, consumidores, empresas e administrações públicas da União Europeia.

Em 2008, o mandato da ENISA foi prorrogado sem modificações até Março de 2012[5]. Ao mesmo tempo, o Conselho e o Parlamento Europeu apelaram a uma maior discussão sobre o futuro da ENISA e sobre a orientação geral do esforço europeu com vista a uma maior segurança das redes e da informação. Como contributo para este debate, a Comissão lançou em Novembro último uma consulta pública em linha[6], cuja análise será disponibilizada em breve.

As actividades previstas na presente comunicação são realizadas no âmbito do programa europeu de protecção das infra-estruturas críticas (PEPIC)[7] e em paralelo com as suas actividades. Um elemento essencial do PEPIC é a directiva[8] relativa à identificação e designação das infra-estruturas críticas europeias[9], que identifica o sector das TIC como um futuro sector prioritário. Outro elemento importante do PEPIC é a rede de alerta para as infra-estruturas críticas (RAIC)[10].

No que respeita à regulamentação, a proposta da Comissão relativa à reforma do quadro regulamentar das redes e serviços de comunicações electrónicas[11] inclui novas disposições sobre segurança e integridade que visam, nomeadamente, reforçar as obrigações dos operadores de assegurarem a adopção de medidas adequadas para fazer face a riscos identificados, garantirem a continuidade do fornecimento dos serviços e notificarem os casos de violação da segurança[12]. Esta estratégia contribui para a realização do objectivo geral de melhorar a segurança e a resiliência das ICI. O Parlamento Europeu e o Conselho apoiam amplamente estas disposições.

As acções propostas na presente comunicação complementam as medidas em vigor e em estudo na área da cooperação policial e judicial para prevenir, combater e reprimir actividades criminosas e terroristas contra as infra-estruturas TIC, tal como previsto, nomeadamente, na decisão-quadro do Conselho relativa a ataques contra os sistemas de informação[13] e na sua próxima actualização[14].

Esta iniciativa tem em conta as actividades da NATO no âmbito da política comum de ciberdefesa, ou seja, a entidade de gestão da ciberdefesa e o centro de excelência cooperativo para a ciberdefesa.

---

5 Regulamento (CE) n.º 1007/2008
6 http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464
7 COM(2006) 786 final
8 2008/114/CE
9 http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/gena/104617.pdf
10 COM(2008) 676 final
11 COM(2007) 697, COM(2007) 698, COM(2007) 699
12 Artigo 13.º da Directiva-Quadro
13 2005/222/JAI
14 COM(2008) 712

Por último, são devidamente tomadas em conta a evolução política internacional, em especial os princípios do G8 para a protecção das ICI[15], a Resolução 58/199 da Assembleia Geral da ONU sobre a criação de uma cultura mundial de cibersegurança e a protecção das infra-estruturas críticas da informação e a recente recomendação da OCDE sobre a protecção das infra-estruturas críticas da informação.

3. O QUE ESTÁ EM JOGO

3.1. As infra-estruturas críticas da informação são vitais para o desenvolvimento económico e social da UE

O papel económico e social do sector das TIC e das infra-estruturas TIC é sublinhado em relatórios recentes sobre a inovação e o crescimento económico, como a comunicação sobre a avaliação intercalar da iniciativa i2010[16], o relatório do grupo Aho[17] e os relatórios económicos anuais da União Europeia[18]. A OCDE sublinha a importância das TIC e da Internet para estimular o desempenho económico e o bem-estar social e reforçar a capacidade das sociedades para melhorarem a qualidade de vida dos cidadãos no mundo inteiro[19]. Recomenda ainda políticas que reforcem a confiança na infra-estrutura da Internet.

O sector das TIC é vital para todos os segmentos da sociedade. As empresas confiam no sector das TIC tanto para as vendas directas como para a eficiência dos processos internos. As TIC são um factor de inovação essencial e estão na origem de quase 40% do aumento da produtividade[20]. As TIC penetraram igualmente em todas as actividades dos governos e das administrações públicas: a adopção dos serviços de administração pública em linha a todos os níveis, bem como de novas aplicações, nomeadamente soluções inovadoras relacionadas com a saúde, a energia e a participação política, torna o sector público fortemente dependente das TIC. Por último, mas igualmente importante, os cidadãos confiam nas TIC e utilizam-nas cada vez mais nas suas actividades diárias: o reforço da segurança das ICI fará aumentar a confiança dos cidadãos nas TIC, nomeadamente graças a uma melhor protecção dos dados pessoais e da privacidade.

3.2. Os riscos para as infra-estruturas críticas da informação

Os riscos devidos a ataques de origem humana, catástrofes naturais ou falhas técnicas não são, muitas vezes, inteiramente compreendidos e/ou suficientemente analisados. Consequentemente, o nível de sensibilização entre as partes interessadas é insuficiente para conceber salvaguardas e contramedidas eficazes.

Os ciberataques atingiram um nível de sofisticação sem precedentes. O que era simples diletantismo está a transformar-se numa actividade sofisticada lucrativa ou ditada por motivos políticos. Os recentes ciberataques em grande escala contra a Estónia, a Lituânia e a Geórgia são os exemplos mais amplamente conhecidos de uma tendência geral. A enorme quantidade

---

15 http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf

16 COM(2008) 199 final

17 http://ec.europa.eu/invest-in-research/action/2006_ahogroup_en.htm

18 "The EU Economy: 2007 Review", http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf

19

20 http://epp.eurostat.ec.europa.eu/ - Ciência e tecnologia/Sociedade da informação

de vírus, vermes e outras formas de *malware*, a expansão das *botnets* (redes de computadores *zombies*) e o aumento contínuo do *spam* confirmam a gravidade do problema[21].

A imprescindibilidade das ICI, a sua interconexão e interdependência transfronteiras com outras infra-estruturas, as suas vulnerabilidades e as ameaças com que se defrontam fazem aumentar a necessidade de medidas que reforcem a sua segurança e resiliência numa perspectiva sistémica, como primeira linha de defesa contra falhas e ataques.

3.3. A segurança e a resiliência das infra-estruturas críticas da informação como factores de reforço da confiança na sociedade da informação

Para que as infra-estruturas TIC sejam utilizadas ao máximo, concretizando assim plenamente as oportunidades económicas e sociais da sociedade da informação, é necessário que todas as partes interessadas confiem nelas em elevado grau, o que depende de vários elementos, dos quais o mais importante é a garantia de um nível elevado de segurança e resiliência. Diversidade, abertura, interoperabilidade, facilidade de utilização, transparência, responsabilidade, auditabilidade dos diferentes componentes e concorrência são elementos essenciais para o desenvolvimento da segurança e estimulam a implantação de produtos, processos e serviços que melhoram a segurança. Como foi já sublinhado pela Comissão[22], nesta matéria, a responsabilidade é partilhada: nenhum interessado dispõe, por si só, de meios que lhe permitam garantir a segurança e a resiliência de todas as infra-estruturas TIC e assumir todas as responsabilidades neste domínio.

Tais responsabilidades exigem uma abordagem e uma cultura de gestão de riscos capazes de dar resposta às ameaças conhecidas e prevenir futuras ameaças desconhecidas, sem reacções excessivas e sem impedir o surgimento de serviços e aplicações inovadores.

3.4. Os desafios para a Europa

Além disso e como complemento de todas as actividades relacionadas com a aplicação da directiva relativa à identificação e designação das infra-estruturas críticas europeias, nomeadamente a identificação de critérios específicos para o sector das TIC, é necessário dar resposta a um conjunto de desafios mais amplos, a fim de reforçar a segurança e a resiliência das ICI.

3.4.1. Estratégias nacionais heterogéneas e descoordenadas

Embora haja pontos comuns nos desafios e nas questões a resolver, as medidas e os regimes destinados a garantir a segurança e a resiliência das ICI, bem como o nível de competência e de preparação, diferem de Estado-Membro para Estado-Membro.

A adopção de estratégias puramente nacionais pode produzir uma situação de fragmentação e ineficiência na Europa. As diferenças nas estratégias nacionais e a falta de cooperação transfronteiras sistemática reduzem substancialmente a eficácia das contramedidas domésticas, nomeadamente porque, devido à interconexão das ICI, o baixo nível de segurança e resiliência das ICI num país pode aumentar as vulnerabilidades e os riscos noutros.

---

21 COM(2006)688 final

22 COM(2006)251 final

Para superar esta situação, é necessário um esforço europeu que acrescente valor às políticas e programas nacionais promovendo uma maior sensibilização e um melhor entendimento comum dos desafios, estimulando a adopção de objectivos e prioridades políticos comuns, reforçando a cooperação entre os Estados-Membros e integrando as políticas nacionais numa dimensão mais europeia e mundial.

3.4.2. Necessidade de um novo modelo de governação europeia para as ICI

A melhoria da segurança e da resiliência das ICI levanta desafios específicos de governação. Embora os Estados-Membros continuem a ser, em última análise, responsáveis pela definição das políticas respeitantes às ICI, a aplicação destas depende da participação do sector privado, que possui ou controla um grande número de ICI. Por outro lado, os mercados nem sempre oferecem incentivos suficientes para que o sector privado invista na protecção das ICI ao nível normalmente requerido pelos governos.

Para resolver este problema de governação, surgiram, como modelo de referência, parcerias público-privadas (PPP) a nível nacional. No entanto, apesar de ser consensual que as PPP seriam igualmente desejáveis ao nível europeu, não foram criadas até agora PPP europeias. O estabelecimento de um quadro de governação multilateral à escala europeia, onde a ENISA poderá ter um papel de relevo, pode promover a participação do sector privado na definição de objectivos políticos estratégicos e de prioridades e medidas operacionais. Este quadro iria colmatar o fosso entre a definição das políticas nacionais e a realidade operacional no terreno.

3.4.3. Reduzida capacidade europeia de alerta rápido e de resposta a incidentes

Os mecanismos de governação só serão verdadeiramente eficazes se todos os participantes puderem trabalhar com informações fiáveis, condição esta que é especialmente importante para os governos, primeiros responsáveis pela segurança e o bem-estar dos cidadãos.

No entanto, os processos e as práticas de monitorização e comunicação de incidentes de segurança das redes variam significativamente de Estado-Membro para Estado-Membro. Em alguns deles não existe uma organização de referência que funcione como ponto de monitorização. Mais significativa ainda é a aparente insuficiência da cooperação e da partilha, entre os Estados-Membros, de dados fiáveis e operáveis sobre incidentes de segurança, partilha essa que é informal ou se limita a um intercâmbio bilateral ou escassamente multilateral. Além disso, a simulação de incidentes e a realização de exercícios para testar a capacidade de resposta assumem uma importância estratégica na melhoria da segurança e da resiliência das ICI, privilegiando, em especial, estratégias e processos flexíveis para lidar com a imprevisibilidade das potenciais crises. Na UE, os exercícios de cibersegurança estão ainda numa fase embrionária. Os exercícios de dimensão transnacional são muito limitados. Como ficou demonstrado em eventos recentes[23], o auxílio mútuo é um elemento essencial de uma resposta adequada a ameaças e ataques em grande escala contra as ICI.

Para se dispor de uma elevada capacidade europeia de alerta rápido e de resposta a incidentes, são necessárias equipas nacionais/governamentais eficientes de resposta a emergências informáticas (CERT), ou seja, uma base comum em termos de capacidades. Estes organismos devem funcionar como catalisadores nacionais dos interesses das partes envolvidas e da capacidade de realização de actividades a nível político (incluindo as relacionadas com os

[23] http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/

sistemas de partilha de informações e de alertas destinados aos cidadãos e às PME) e empreender uma cooperação e um intercâmbio de informações transfronteiras efectivos, eventualmente potenciando o papel de organizações existentes, como o grupo das CERT governamentais europeias (CGE)[24].

3.4.4. Cooperação internacional

O facto de a Internet se ter tornado uma ICI essencial exige que se preste uma atenção especial à sua resiliência e estabilidade. A Internet, graças à sua arquitectura distribuída e redundante, revelou-se uma infra-estrutura muito robusta. No entanto, o seu crescimento fenomenal deu origem a uma complexidade física e lógica crescente e ao surgimento de novos serviços e utilizações: justifica-se questionar a capacidade da Internet para suportar o número crescente de perturbações e ciberataques.

A divergência de opiniões sobre o carácter crítico dos elementos que constituem a Internet explica em parte a diversidade das posições governamentais expressas em fóruns internacionais e as percepções frequentemente contraditórias da importância desta questão. Esta situação pode dificultar a adequada prevenção, preparação e capacidade de recuperação relativamente às ameaças que pesam sobre a Internet. Por exemplo, devem igualmente ser avaliadas as consequências da transição do IPv4 para o IPv6, em termos de segurança das ICI.

A Internet é uma rede de redes mundial e altamente distribuída, cujos centros de controlo não estão necessariamente limitados pelas fronteiras nacionais. Exige-se, pois, uma abordagem específica e com alvos bem definidos, para assegurar a sua resiliência e estabilidade, baseada em duas medidas convergentes. A primeira consiste em alcançar um consenso sobre as prioridades europeias para a resiliência e a estabilidade da Internet, em termos de política e de implantação operacional. A segunda, em levar a comunidade mundial a estabelecer um conjunto de princípios, consonantes com os valores fundamentais europeus, para a resiliência e a estabilidade da Internet, no âmbito do diálogo e da cooperação estratégicos que mantemos com países terceiros e com organizações internacionais. Estas actividades basear-se-ão no reconhecimento, pela cimeira mundial sobre a sociedade da informação[25], da importância fundamental da estabilidade da Internet.

4. O CAMINHO A SEGUIR: MAIOR COORDENAÇÃO E COOPERAÇÃO A NÍVEL DA UE

Devido à dimensão comunitária e internacional do problema, uma estratégia integrada a nível da UE para melhorar a segurança e a resiliência das ICI iria complementar e acrescentar valor aos programas nacionais, bem como aos actuais regimes de cooperação bilateral e multilateral entre os Estados-Membros.

As discussões políticas subsequentes aos eventos na Estónia sugerem que os efeitos de ataques similares podem ser mitigados mediante medidas preventivas e uma acção coordenada durante a própria crise. Um intercâmbio mais estruturado de informações e de boas práticas em toda a UE poderá facilitar consideravelmente o combate às ameaças transfronteiras.

---

[24] http://www.egc-group.org/

[25] Agenda de Túnis para a sociedade da informação, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

É necessário reforçar os instrumentos existentes de cooperação, nomeadamente a ENISA, e, se necessário, criar novos instrumentos. É essencial uma abordagem multilateral e multiníveis de dimensão europeia, mas que respeite e complemente inteiramente as competências nacionais.

É necessária uma compreensão profunda do contexto e dos condicionalismos. Por exemplo, o facto de a Internet ter uma arquitectura distribuída em que os nós periféricos podem ser utilizados como vectores de ataque (p. ex., *botnets*) constitui motivo de preocupação. Contudo, esta característica é um factor essencial de estabilidade e resiliência, podendo contribuir para uma recuperação mais rápida do que a que se conseguiria normalmente com procedimentos descendentes (*top-down*), excessivamente formalizados. Neste contexto, é necessária uma análise casuística cautelosa das políticas e procedimentos operacionais a estabelecer.

O horizonte temporal é igualmente importante. É claramente necessário agir de imediato e criar rapidamente os elementos necessários para construir um quadro que nos permita responder aos actuais desafios e que contribua para a futura estratégia de segurança das redes e da informação.

São propostos cinco pilares para fazer face a estes desafios:

(1) Preparação e prevenção: assegurar a preparação a todos os níveis;

(2) Detecção e resposta: criar mecanismos adequados de alerta rápido;

(3) Mitigação e recuperação: reforçar os mecanismos de defesa das ICI na UE;

(4) Cooperação internacional: promover internacionalmente as prioridades da UE;

(5) Critérios para o sector das TIC: apoiar a aplicação da directiva relativa à identificação e designação das infra-estruturas críticas europeias[26].

5. PLANO DE ACÇÃO

5.1. Preparação e prevenção:

Capacidades e serviços de base para uma cooperação pan-europeia. A Comissão convida os Estados-Membros e as partes interessadas a:

- definirem, com o apoio da ENISA, um nível mínimo de capacidades e serviços para as CERT nacionais/governamentais e de operações de resposta a incidentes, como suporte da cooperação pan-europeia.
- certificarem-se de que as CERT nacionais/governamentais funcionam como o elemento-chave da capacidade nacional em termos de preparação, partilha de informações, coordenação e resposta.

[26] Directiva 2008/114/CE do Conselho

Objectivo: final de 2010 para a definição comum das normas mínimas; final de 2011 para a criação em todos os Estados-Membros de CERT nacionais/governamentais que funcionem adequadamente.

Parceria público-privada europeia para a resiliência (PPPER). A Comissão irá:

- promover a cooperação entre os sectores público e privado no que respeita aos objectivos de segurança e resiliência, aos requisitos de base e às boas práticas e medidas políticas. A PPPER centrar-se-á essencialmente na dimensão europeia vista numa perspectiva estratégica (p. ex., boas práticas políticas) e táctica/operacional (p. ex., implantação industrial). A PPPER deve basear-se nas - e complementar as - iniciativas nacionais existentes e as actividades operacionais da ENISA.

Objectivo: final de 2009 para o roteiro e o plano da PPPER; meados de 2010 para a criação da PPPER; final de 2010 para os primeiros resultados da PPPER.

Fórum europeu de partilha de informações entre os Estados-Membros. A Comissão irá:

- criar um fórum europeu onde os Estados-Membros partilhem informações e boas práticas políticas no domínio da segurança e da resiliência das ICI. Este fórum beneficiará dos resultados das actividades de outras organizações, nomeadamente a ENISA.

Objectivo: final de 2009 para o lançamento do fórum; final de 2010 para a produção dos primeiros resultados.

5.2. Detecção e resposta

Sistema europeu de partilha de informações e de alerta (SEPIA). A Comissão apoia:

o desenvolvimento e a implantação do SEPIA, destinado aos cidadãos e às PME e que se baseia em sistemas nacionais e privados de partilha de informações e de alertas. A Comissão apoia financeiramente dois projectos de prototipagem complementares[27]. A ENISA deve proceder ao inventário dos resultados destes projectos e de outras iniciativas nacionais e elaborar um roteiro para impulsionar o desenvolvimento e a implantação do SEPIA.

Objectivo: final de 2010 para a conclusão dos projectos de prototipagem; final de 2010 para o roteiro destinado a criar um sistema europeu.

5.3. Mitigação e recuperação:

Planos e exercícios nacionais de emergência. A Comissão convida os Estados-Membros a:

- elaborarem planos nacionais de emergência e organizarem exercícios periódicos em grande escala de resposta a incidentes de segurança das redes e de recuperação em caso de catástrofe, como etapa para uma coordenação pan-europeia mais estreita. As CERT/CSIRT nacionais/governamentais podem ser encarregadas de realizar exercícios e testes no âmbito

[27] No âmbito do programa comunitário "Prevenção, preparação e gestão das consequências em matéria de terrorismo e outros riscos relacionados com a segurança", http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm

dos planos nacionais de emergência, com a participação das partes interessadas dos sectores privado e público. A ENISA é convidada a apoiar o intercâmbio das boas práticas entre os Estados-Membros.

Objectivo: final de 2010 para a realização de, no mínimo, um exercício nacional em cada Estado-Membro.

Exercícios pan-europeus de incidentes em grande escala que afectam a segurança das redes. A Comissão irá:

- apoiar financeiramente o desenvolvimento de exercícios pan-europeus de incidentes que afectam a segurança da Internet[28], que podem igualmente constituir a plataforma operacional para uma participação pan-europeia em exercícios internacionais de incidentes que afectam a segurança das redes, como o "Cyber Storm" dos EUA.

Objectivo: final de 2010 para a concepção e realização do primeiro exercício pan-europeu; final de 2010 para uma participação pan-europeia em exercícios internacionais.

Cooperação reforçada entre CERT nacionais/governamentais. A Comissão convida os Estados-Membros a:

- reforçarem a cooperação entre as CERT nacionais/governamentais, designadamente potenciando e alargando os mecanismos de cooperação existentes, como o grupo CGE[29]. A ENISA deve ter um papel activo de estímulo e apoio à cooperação pan-europeia entre as CERT nacionais/governamentais, que deverá conduzir a uma maior preparação, a um reforço da capacidade da Europa para reagir e responder a incidentes e à realização de exercícios pan-europeus (e/ou regionais).

Objectivo: final de 2010 para a duplicação do número de organismos nacionais participantes no CGE; final de 2010 para a elaboração, pela ENISA, de material de referência que sirva de suporte à cooperação pan-europeia.

5.4. Cooperação internacional

Resiliência e estabilidade da Internet. Estão previstas três actividades complementares:

- Prioridades europeias no que respeita à resiliência e à estabilidade a longo prazo da Internet. A Comissão conduzirá um debate à escala europeia, envolvendo todas as partes interessadas públicas e privadas, com vista à definição de prioridades comunitárias respeitantes à resiliência e à estabilidade a longo prazo da Internet.

Objectivo: final de 2010 para prioridades comunitárias respeitantes a componentes e questões críticas da Internet.

- Princípios e orientações para a resiliência e a estabilidade da Internet (a nível europeu). A Comissão trabalhará com os Estados-Membros na definição de orientações para a resiliência e a estabilidade da Internet, centrando-se, nomeadamente, em medidas

[28] Ver nota 27
[29] Ver nota 24

correctivas regionais, acordos de assistência mútua, estratégias coordenadas de recuperação e continuidade, distribuição geográfica dos recursos críticos da Internet, salvaguardas tecnológicas na arquitectura e nos protocolos da Internet, reprodução e diversidade dos serviços e dos dados. A Comissão está já a financiar um grupo de trabalho para a resiliência do DNS, que, a par de outros projectos neste domínio, contribuirá para a criação de um consenso[30].

Objectivo: final de 2009 para o roteiro europeu destinado a estabelecer princípios e orientações para a resiliência e a estabilidade da Internet; final de 2010 para a aprovação de uma primeira formulação dos referidos princípios e orientações.

- Princípios e orientações para a resiliência e a estabilidade da Internet (a nível mundial). A Comissão trabalhará com os Estados-Membros num roteiro para a promoção dos princípios e orientações a nível mundial. Será desenvolvida uma cooperação estratégica com países terceiros, nomeadamente no âmbito dos diálogos sobre a sociedade da informação, que contribuirá para um consenso mundial[31].

Objectivo: início de 2010 para um roteiro da cooperação internacional respeitante aos princípios e orientações para a segurança e a resiliência; final de 2010 para a formulação inicial de princípios e orientações reconhecidos a nível internacional a discutir com países terceiros e em fóruns relevantes, nomeadamente o fórum sobre a governação da Internet.

Exercícios a nível mundial de recuperação e mitigação dos efeitos de incidentes em grande escala na Internet. A Comissão convida as partes interessadas europeias a:

- reflectirem sobre uma forma prática de alargar à escala mundial os exercícios realizados no âmbito do pilar "mitigação e recuperação", tomando como base os planos de emergência e as capacidades regionais.

Objectivo: final de 2010 para uma proposta da Comissão relativa a um quadro e um roteiro de apoio à participação da Europa em exercícios a nível mundial de recuperação e mitigação dos efeitos de incidentes em grande escala na Internet.

5.5. Critérios aplicáveis às infra-estruturas críticas europeias no sector das TIC

Critérios específicos para o sector das TIC. Baseando-se na actividade inicial realizada em 2008, a Comissão irá:

- continuar a elaborar, em colaboração com os Estados-Membros e todas as partes interessadas, os critérios de identificação das infra-estruturas críticas europeias no sector das TIC. Para tal, serão utilizadas as informações pertinentes de um estudo específico que está em vias de lançamento[32].

Objectivo: primeiro semestre de 2010 para a definição, pela Comissão, dos critérios aplicáveis às infra-estruturas críticas europeias no sector das TIC.

---

30 Ver nota 27
31 COM(2008)588 final
32 Ver nota 27

6. CONCLUSÕES

A segurança e a resiliência das ICI são a primeira linha de defesa contra falhas e ataques. A sua melhoria em toda a UE é essencial para que se possam colher plenamente os benefícios da sociedade da informação. Para alcançar este ambicioso objectivo, propõe-se um plano de acção que reforce a cooperação táctica e operacional a nível europeu. O êxito destas acções depende da sua capacidade para tirar partido das actividades dos sectores público e privado, beneficiando-as simultaneamente, bem como do empenho e da plena participação dos Estados-Membros, das instituições europeias e das partes interessadas.

Nesse sentido, terá lugar em 27-28 de Abril de 2009 uma conferência ministerial que irá discutir as iniciativas propostas com os Estados-Membros e oficializar o seu empenho no debate sobre a modernização e o reforço da política de segurança das redes e da informação na Europa.

Por último, a melhoria da segurança e da resiliência das ICI é um objectivo de longo prazo, pelo que é necessário reavaliar periodicamente a estratégia e as medidas neste domínio. Consequentemente, dado que este objectivo está em consonância com o debate geral sobre o futuro da política de segurança das redes e da informação na UE após 2012, a Comissão irá lançar, no final de 2010, um exercício de levantamento da situação, a fim de avaliar a primeira fase de acções e identificar e propor novas medidas, se necessário.