COMISSÃO EUROPEIA

ALTA REPRESENTANTE DA UNIÃO EUROPEIA PARA OS NEGÓCIOS ESTRANGEIROS E A POLÍTICA DE SEGURANÇA

Bruxelas, 7.2.2013
JOIN(2013) 1 final

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

Estratégia da União Europeia para a cibersegurança:

Um ciberespaço aberto, seguro e protegido

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

Estratégia da União Europeia para a cibersegurança:

Um ciberespaço aberto, seguro e protegido

1. INTRODUÇÃO

1.1. Contexto

Nas últimas duas décadas, a Internet e, mais genericamente, o ciberespaço teve um impacto enorme em todos os setores da sociedade. A nossa vida diária, os direitos fundamentais, as interações sociais e as economias dependem do funcionamento fluido das tecnologias da informação e das comunicações. Um ciberespaço aberto e livre tem promovido a inclusão política e social em todo o mundo; derrubou as barreiras entre países, comunidades e cidadãos, permitindo a interação e a partilha de informações e ideias entre todos os pontos do globo; proporcionou um fórum para a liberdade de expressão e o exercício dos direitos fundamentais e deu às pessoas meios para lutarem por sociedades democráticas e mais justas – como a primavera árabe demonstrou de modo impressionante.

Para que o ciberespaço permaneça aberto e livre, devem aplicar-se no universo em linha as mesmas normas, princípios e valores que a UE defende para o mundo físico. Os direitos fundamentais, a democracia e o Estado de direito devem ser protegidos no ciberespaço. A nossa liberdade e prosperidade dependem cada vez mais de uma Internet robusta e inovadora, que continuará a prosperar se a inovação por parte do setor privado e da sociedade civil favorecer o seu crescimento. Mas a liberdade em linha exige também segurança e proteção. O ciberespaço deve ser protegido contra incidentes, atividades maliciosas e utilizações abusivas; e os governos têm um importante papel a desempenhar na garantia de um ciberespaço livre e seguro. São várias as funções que competem aos governos: salvaguardar o acesso e a abertura, respeitar e proteger os direitos fundamentais em linha e manter a fiabilidade e a interoperabilidade da Internet. No entanto, o setor privado detém e explora partes significativas do ciberespaço e, por conseguinte, qualquer iniciativa que pretenda ser bem sucedida nesta matéria deve reconhecer o seu papel crucial.

As tecnologias da informação e das comunicações tornaram-se a espinha dorsal do nosso crescimento económico e são um recurso crítico de que todos os setores económicos dependem. Estão atualmente na base dos complexos sistemas que fazem funcionar as nossas economias em setores fundamentais como as finanças, a saúde, a energia e os transportes; muitos modelos de negócio estão construídos com base na disponibilidade ininterrupta da Internet e no bom funcionamento dos sistemas informáticos.

Uma vez concretizado o mercado único digital, a Europa poderá aumentar o seu PIB em quase 500 000 milhões de euros por ano[1], uma média de 1000 euros por pessoa. Para que possamos assistir ao arranque das novas tecnologias ligadas à Internet, incluindo os pagamentos eletrónicos, a computação em nuvem ou a comunicação máquina-máquina[2], os

[1] http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

[2] Por exemplo, plantas equipadas com sensores que comunicam ao sistema de aspersão que está na hora de serem regadas.

cidadãos terão de se sentir confiantes. Infelizmente, um inquérito Eurobarómetro de 2012[3] revelou que quase um terço dos europeus não têm confiança na sua capacidade de utilizar a Internet para serviços bancários ou compras. Uma esmagadora maioria afirmou também que evita a divulgação de informações pessoais em linha por uma questão de segurança. Em toda a UE, mais de um em cada dez utilizadores da Internet já foi vítima de fraudes em linha.

Nos últimos anos verificou-se que, embora traga enormes benefícios, o mundo digital é também vulnerável. Os incidentes de cibersegurança[4], intencionais ou acidentais, estão a aumentar a um ritmo alarmante e poderão perturbar a prestação de serviços essenciais que consideramos garantidos, como a água, os cuidados de saúde, a eletricidade ou os serviços móveis. As ameaças podem ter origens diversas — nomeadamente ataques criminosos, politicamente motivados, terroristas ou patrocinados por Estados, assim como catástrofes naturais e erros involuntários.

A economia da UE já é afetada pela cibercriminalidade[5] contra o setor privado e os particulares. Os cibercriminosos utilizam métodos cada vez mais sofisticados para se introduzirem nos sistemas informáticos, roubarem dados críticos ou exigirem resgates às empresas. O aumento da espionagem económica e de atividades patrocinadas por Estados no ciberespaço coloca os governos e as empresas dos países da UE à mercê de uma nova categoria de ameaças.

Nos países não pertencentes à UE, os governos podem também utilizar de forma abusiva o ciberespaço para a vigilância e o controlo dos seus próprios cidadãos. A UE pode contrariar esta situação promovendo a liberdade em linha e garantindo o respeito dos direitos fundamentais em linha.

Todos estes fatores explicam por que razão os governos de todo o mundo começaram a elaborar estratégias em matéria de cibersegurança e a considerar o ciberespaço uma questão internacional cada vez mais importante. Chegou a altura de a UE intensificar as suas ações neste domínio. A presente proposta para uma estratégia da União Europeia em matéria de cibersegurança, apresentada pela Comissão e pela Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança (Alta Representante), define a visão da UE neste domínio, clarifica os papéis e as responsabilidades e descreve as ações necessárias, apostadas em proteger e promover eficazmente e por todos os meios os direitos dos cidadãos a fim de tornar o ambiente em linha na UE o mais seguro do mundo.

1.2. Princípios da cibersegurança

A Internet sem fronteiras e multicamadas tornou-se um dos mais poderosos instrumentos de progresso a nível mundial sem supervisão ou regulação governamental. Embora o setor

---

[3] Eurobarómetro especial 390 sobre cibersegurança, de 2012.

[4] O termo cibersegurança refere-se, geralmente, às precauções e ações que podem ser utilizadas para proteger o ciberespaço, tanto nos domínios civil como militar, contra as ameaças decorrentes da interdependência das suas redes e infraestruturas informáticas ou que as possam danificar. A cibersegurança procura manter a disponibilidade e a integridade das redes e infraestruturas e a confidencialidade das informações nelas contidas.

[5] A cibercriminalidade refere-se, geralmente, a um amplo leque de diferentes atividades criminosas que envolvem os computadores e os sistemas informáticos, quer como instrumentos quer como alvos principais. A cibercriminalidade inclui as infrações tradicionais (por exemplo, fraude, falsificação e roubo de identidade), infrações relativas aos conteúdos (por exemplo, distribuição de material pedopornográfico em linha ou incitamento ao ódio racial) e crimes respeitantes exclusivamente a computadores e sistemas informáticos (por exemplo, ataques contra os sistemas informáticos, recusa de serviço e *software* malicioso).

privado deva continuar a desempenhar um papel primordial na construção e na gestão quotidiana da Internet, a necessidade de requisitos de transparência, responsabilização e segurança está a tornar-se cada vez mais premente. A presente estratégia clarifica os princípios que devem orientar a política de cibersegurança na UE e a nível internacional.

Os valores fundamentais da UE aplicam-se tanto no mundo digital como no mundo físico

As leis e normas que se aplicam noutros domínios das nossas vidas quotidianas aplicam-se igualmente no domínio do ciberespaço.

Proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade

A cibersegurança apenas pode ser sólida e eficaz se se basear nos direitos e liberdades fundamentais consagrados na Carta dos Direitos Fundamentais da União Europeia e nos valores fundamentais da UE. Reciprocamente, os direitos individuais não podem ser assegurados sem redes e sistemas seguros. Toda a partilha de informações para efeitos da cibersegurança, quando estejam em causa dados pessoais, deve respeitar a legislação da UE sobre proteção de dados e ter plenamente em conta os direitos individuais neste domínio.

Acesso para todos

Um acesso limitado ou a falta de acesso à Internet e a iliteracia digital constituem uma desvantagem para os cidadãos, tendo em conta a importância e a quase omnipresença do mundo digital nas atividades da sociedade. Toda a gente deve poder aceder à Internet e a um fluxo de informações livre. A integridade e a segurança da Internet devem ser garantidas para permitir um acesso seguro para todos.

Governação multilateral, democrática e eficiente

O mundo digital não é controlado por uma só entidade. Existem atualmente várias partes envolvidas, muitas das quais entidades comerciais e não governamentais, implicadas na gestão diária dos recursos, protocolos e normas da Internet e no seu futuro desenvolvimento. A UE reafirma a importância de todos os intervenientes no atual modelo de governo da Internet e subscreve esta abordagem de governação multilateral[6].

Uma responsabilidade partilhada para garantir a segurança

A dependência crescente em relação às tecnologias da informação e das comunicações em todos os domínios da vida humana trouxe à tona de água vulnerabilidades que é necessário definir adequadamente e analisar em profundidade, corrigir ou reduzir. Todos os intervenientes relevantes, sejam as autoridades públicas, o setor privado ou os cidadãos individualmente, têm de reconhecer esta responsabilidade partilhada, tomar medidas para se protegerem e, se necessário, procurar uma resposta coordenada para reforçar a cibersegurança.

[6] Ver também COM(2009) 277, Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «Governo da Internet: as próximas etapas».

2. PRIORIDADES ESTRATÉGICAS E AÇÕES

A UE deve preservar um ambiente em linha que garanta o maior grau de liberdade e de segurança possível, em benefício de todos. Embora reconheça que cabe predominantemente aos Estados-Membros responder aos desafios da segurança no ciberespaço, a presente estratégia propõe ações específicas que podem melhorar o desempenho geral da UE. Tais ações, de curto e de longo prazos, incluem uma variedade de ferramentas políticas[7] e envolvem diferentes tipos de atores – desde as instituições da UE aos Estados-Membros ou à indústria.

A visão da UE apresentada na presente estratégia articula-se em cinco prioridades estratégicas, que abordam os desafios acima destacados:

- Garantir a resiliência do ciberespaço
- Reduzir drasticamente a cibercriminalidade
- Desenvolver a política e as capacidades no domínio da ciberdefesa no quadro da política comum de segurança e defesa (PCSD)
- Desenvolver os recursos industriais e tecnológicos para a cibersegurança
- Estabelecer uma política internacional coerente em matéria de ciberespaço para a União Europeia e promover os valores fundamentais da UE

2.1. Garantir a resiliência do ciberespaço

Para promover a resiliência do ciberespaço na UE, tanto as autoridades públicas como o setor privado devem desenvolver capacidades e cooperar de forma eficaz. Com base nos resultados positivos alcançados através das atividades realizadas até à data[8], a prossecução da ação da UE pode ajudar, nomeadamente, a combater os riscos e ameaças de dimensão transfronteiras de que é alvo o ciberespaço e contribuir para uma resposta coordenada em situações de emergência. Essas medidas darão um forte contributo para o bom funcionamento do mercado interno e promoverão a segurança interna da UE.

A Europa permanecerá vulnerável se não fizer um esforço substancial para melhorar as capacidades, os recursos e os processos públicos e privados para prevenir, detetar e dar resposta aos incidentes a nível da cibersegurança. É por esta razão que a Comissão tem vindo a desenvolver uma política de segurança das redes e da informação (SRI)[9]. A **Agência Europeia para a Segurança das Redes e da Informação, ENISA**, foi criada em 2004[10] e o seu mandato será reforçado e modernizado através de um novo regulamento que está a ser negociado pelo Conselho e pelo Parlamento[11]. Além disso, a diretiva-quadro das

---

7 As ações relacionadas com a partilha de informações, quando estejam em causa dados pessoais, devem ser conformes com a legislação da UE relativa à proteção de dados.

8 Ver as referências feitas na presente comunicação, bem como na avaliação de impacto que integra o documento de trabalho dos serviços da Comissão, anexo à proposta de diretiva relativa à segurança das redes e da informação, em particular as secções 4.1.4 e 5.2, os anexos 2, 6 e 8.

9 Em 2001, a Comissão adotou uma Comunicação intitulada «Segurança das redes e da informação: Proposta de uma abordagem política europeia», COM(2001) 298 final; em 2006, adotou uma estratégia para uma sociedade da informação segura (COM (2006) 251). Desde 2009, a Comissão adotou também um plano de ação e uma comunicação sobre a proteção das infraestruturas críticas da informação **(**COM(2009)149), aprovados pelo Conselho através da Resolução 2009/C 321/01; e COM(2011)163, aprovada pelo Conselho nas suas Conclusões 10299/11**.**

10 Regulamento (CE) n.º 460/2004.

11 COM(2010) 521. As ações propostas na presente estratégia não implicam a alteração do mandato existente ou futuro da ENISA.

comunicações eletrónicas[12] exige que os fornecedores de serviços de comunicações eletrónicas giram adequadamente os riscos para as suas redes e comuniquem as violações de segurança significativas. Além disso, a legislação da UE relativa à proteção de dados[13] exige que os responsáveis pelo tratamento dos dados adotem requisitos e salvaguardas para a proteção dos dados, incluindo medidas de segurança, e que, no domínio dos serviços de comunicações eletrónicas publicamente disponíveis, notifiquem os incidentes que envolvam uma violação de dados pessoais às autoridades nacionais competentes.

Apesar dos progressos realizados com base em compromissos voluntários, ainda existem lacunas em toda a UE, nomeadamente em termos de meios disponíveis a nível nacional, de coordenação em caso de incidentes que ultrapassem as fronteiras e de envolvimento e preparação do setor privado. A presente estratégia é acompanhada por uma proposta **legislativa** que visa, nomeadamente:

- Estabelecer requisitos mínimos comuns para a SRI (segurança das redes e da informação) a nível nacional, o que obrigará os Estados-Membros a designar as autoridades nacionais competentes em matéria de SRI; criar uma CERT que funcione corretamente; e adotar uma estratégia nacional para a SRI e um plano nacional de cooperação nessa matéria. A criação de capacidades e a coordenação dizem igualmente respeito às instituições da UE: em 2012, foi instituída de modo permanente uma equipa de resposta a emergências informáticas responsável pela segurança dos sistemas informáticos das instituições, agências e organismos da UE («CERT-UE»).
- Criar mecanismos coordenados de prevenção, deteção, atenuação e resposta, que permitam a partilha de informações e a assistência mútua entre as autoridades nacionais competentes em matéria de SRI. Estas autoridades serão convidadas a garantir uma cooperação adequada a nível da UE, nomeadamente com base num plano de cooperação da União nessa matéria, concebido para dar resposta aos incidentes informáticos com dimensão transfronteiras. Esta cooperação basear-se-á também nos progressos realizados no contexto do «Fórum Europeu dos Estados-Membros (EFMS)»[14], que tem mantido discussões e trocas de pontos de vista produtivos sobre a política pública para a SRI e pode ser integrado no mecanismo de cooperação, uma vez instaurado.
- Melhorar o grau de preparação e a participação do setor privado. Como a grande maioria das redes e dos sistemas informáticos são privados e explorados por privados, é crucial melhorar o envolvimento do setor privado para promover a cibersegurança. O setor privado deve desenvolver, a nível técnico, capacidades próprias de resiliência do ciberespaço e partilhar as melhores práticas entre os seus vários ramos de atividade. As ferramentas desenvolvidas pela indústria para responder aos incidentes, identificar as causas e conduzir as investigações forenses deverão igualmente beneficiar o setor público.

No entanto, os atores do setor privado continuam a não ter incentivos eficazes para fornecerem dados fiáveis sobre a ocorrência ou o impacto de incidentes SRI, adotarem uma cultura de gestão de riscos ou investirem em soluções de segurança. A legislação proposta visa, por conseguinte, garantir que os atores de uma série de domínios essenciais (a saber, a energia, os transportes, a banca, as bolsas de valores e os viabilizadores de serviços essenciais da Internet, bem como as administrações públicas) avaliem os riscos que enfrentam em matéria de cibersegurança, assegurem a fiabilidade e a resiliência das redes e dos sistemas

[12] Artigos 13.ºA e B da Diretiva 2002/21/CE.

[13] Artigo 17.º da Diretiva 95/46/CE; Artigo 4.º da Diretiva 2002/58/CE.

[14] O Fórum Europeu dos Estados-Membros, lançado por via da Comunicação COM(2009) 149, é uma plataforma para promover o debate entre as autoridades públicas dos Estados-Membros sobre as boas práticas políticas em matéria de segurança e resiliência das infraestruturas críticas da informação.

informáticos através de uma gestão adequada dos riscos e partilhem as informações identificadas com as autoridades nacionais competentes em matéria de SRI. A adoção de uma cultura de cibersegurança poderá aumentar as oportunidades de negócio e a competitividade do setor privado, o que poderá fazer da cibersegurança um trunfo.

Essas entidades terão de comunicar às autoridades nacionais competentes em matéria de SRI os incidentes com impacto significativo na continuidade de serviços fundamentais e no fornecimento de produtos que dependem das redes e dos sistemas informáticos.

As autoridades nacionais competentes em matéria de SRI devem colaborar e trocar informações com outras entidades reguladoras e, em particular, com as autoridades responsáveis pela proteção dos dados pessoais. As autoridades competentes em matéria de SRI devem, por seu turno, comunicar às autoridades policiais/judiciais os incidentes que suspeitem terem um caráter criminal grave. As autoridades nacionais competentes devem também publicar regularmente num sítio Web próprio informações não classificadas sobre alertas recentemente lançados de incidentes e riscos e sobre as respostas coordenadas. As obrigações legais não devem substituir nem impedir o desenvolvimento de uma cooperação informal e voluntária, nomeadamente entre os setores público e privado, a fim de reforçar os níveis de segurança e o intercâmbio de informações e melhores práticas. Em particular, a parceria público-privada europeia para a resiliência (PPPER ou, na sigla inglesa, EP3R[15]), uma plataforma válida e bem estruturada a nível da UE, deve ser mais desenvolvida.

O Mecanismo Interligar a Europa (CEF)[16] concederá apoio financeiro às infraestruturas fundamentais, ligando as capacidades dos Estados-Membros em matéria de SRI e tornando assim mais fácil a cooperação em toda a UE.

Por último, é essencial realizar exercícios de simulação de incidentes informáticos a nível da UE para treinar a cooperação entre os Estados-Membros e o setor privado. O primeiro exercício que envolveu os Estados-Membros realizou-se em 2010 («Cyber Europe 2010») e um segundo exercício, que envolveu também o setor privado, teve lugar em outubro de 2012 («Cyber Europe 2012»). Em novembro de 2011 efetuou-se um exercício de simulação UE-EUA («Cyber Atlantic 2011»). Estão planeados outros exercícios para os próximos anos, nomeadamente com parceiros internacionais.

A Comissão irá:

- Prosseguir as suas atividades de identificação das vulnerabilidades das infraestruturas críticas europeias no tocante à SRI e de estímulo ao desenvolvimento de sistemas com maior capacidade de resistência, executadas pelo Centro Comum de Investigação em estreita coordenação com as autoridades dos Estados-Membros e os proprietários e operadores de infraestruturas críticas.
- Lançar um projeto-piloto financiado pela UE[17], no início de 2013, para **combater os *botnets* e o *malware***, de modo a fornecer um enquadramento para a coordenação

[15] A Parceria Público-Privada Europeia para a Resiliência foi lançada através do documento COM (2009) 149. Esta plataforma começou a trabalhar e tem promovido a cooperação entre os setores público e privado sobre a identificação dos ativos, recursos, funções e requisitos de base essenciais para a resiliência, assim como das necessidades de cooperação e dos mecanismos destinados a dar resposta a perturbações em grande escala que afetem as comunicações eletrónicas.

[16] https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. Rubrica orçamental do CEF: 09.03.02 – Redes de telecomunicações (promover a interconexão e a interoperabilidade dos serviços públicos em linha nacionais, bem como o acesso a essas redes).

e a cooperação entre os Estados-Membros da UE, as organizações do setor privado, como os fornecedores de serviços de Internet, e os parceiros internacionais.

A Comissão pede à ENISA que:

- Preste assistência aos Estados-Membros no desenvolvimento de **capacidades nacionais** fortes **de resiliência para o ciberespaço**, nomeadamente através da formação de especialistas em segurança e resiliência dos sistemas de controlo industriais e das infraestruturas de transporte e de energia.
- Examine em 2013 a viabilidade da criação de equipas de resposta a incidentes no domínio da segurança informática para os sistemas de controlo industriais (ICS-CSIRTs) para a UE.
- Continue a apoiar os Estados-Membros e as instituições da UE na realização regular de **exercícios pan-europeus de resposta a incidentes informáticos**, que constituirão também a base operacional para a participação da UE em exercícios internacionais de resposta a incidentes informáticos.

A Comissão convida o Parlamento Europeu e o Conselho a:

- **Adotarem** rapidamente a proposta de diretiva relativa a um **nível comum elevado de segurança das redes e da informação (SRI)** em toda a União, que incide sobre as questões das capacidades nacionais e da preparação de cada Estado-Membro, da cooperação ao nível da UE, da adoção de práticas de gestão de riscos e da partilha de informações sobre segurança das redes e da informação.

A Comissão pede às empresas que:

- Tomem a iniciativa de **investir** num elevado nível de cibersegurança e desenvolvam as melhores práticas e a partilha de informações a nível setorial e com as autoridades públicas, com o objetivo de assegurar uma proteção sólida e eficaz dos bens e das pessoas, nomeadamente através de parcerias entre os setores público e privado como a EP3R e a *Trust in Digital Life* (TDL)[18].

Sensibilização

Assegurar a cibersegurança é uma responsabilidade comum. Os utilizadores finais desempenham um papel crucial na garantia da segurança das redes e dos sistemas informáticos: é preciso que conheçam os riscos que enfrentam em linha e que tenham capacidade para tomarem medidas simples para os prevenir.

Nos últimos anos, foram lançadas diversas iniciativas, que devem ser prosseguidas. A ENISA tem, nomeadamente, contribuído para a sensibilização através da publicação de relatórios, da organização de *workshops* de peritos e do desenvolvimento de parcerias entre os setores público e privado. A Europol, a Eurojust e as autoridades nacionais de proteção de dados estão também ativamente empenhadas na sensibilização. Em outubro de 2012, a ENISA, com alguns Estados-Membros, lançou o projeto-piloto «Mês europeu da cibersegurança». A sensibilização é um dos domínios sobre os quais o Grupo de Trabalho UE-EUA sobre

[17] Programa de apoio à política das TIC, que faz parte do Programa para a Competitividade e a Inovação (PCI) -2012-6, 325188. Dispõe de um orçamento total de 15 milhões de euros, com um financiamento da União no valor de 7,7 milhões de euros.

[18] http://www.trustindigitallife.eu/

cibersegurança e cibercriminalidade[19] se vai debruçar, e é igualmente essencial no contexto do programa «Para uma Internet mais segura»[20] (que visa a segurança das crianças em linha).

A Comissão pede à ENISA que:

- Proponha em 2013 um roteiro para a criação de uma «carta de condução» em matéria de segurança das redes e da informação como programa de certificação voluntário para promover a melhoria das qualificações e a competência dos profissionais das TI (por exemplo, administradores de sítios Web).

A Comissão irá:

- Organizar em 2014, com o apoio da ENISA, um **campeonato** de cibersegurança entre estudantes universitários, em que os vencedores serão os que apresentarem as melhores soluções de segurança para as redes e a informação.

A Comissão convida os Estados-Membros[21] a:

- Organizarem anualmente um **mês da cibersegurança**, com o apoio da ENISA e a participação do setor privado a partir de 2013, com o objetivo de sensibilizar os utilizadores finais. A partir de 2014, será organizado um mês da cibersegurança sincronizado com os Estados Unidos.
- **Intensificar os esforços nacionais na educação e na formação para a SRI**, através das seguintes medidas: a partir de 2014, formação em segurança das redes e da informação a ministrar nas escolas; formação sobre a SRI e para o desenvolvimento de *software* seguro e a proteção de dados pessoais para estudantes de informática; e formação básica em SRI para o pessoal que trabalha nas administrações públicas.

A Comissão convida as empresas a:

- Promoverem a **sensibilização para a cibersegurança a todos os níveis**, tanto nas práticas empresariais como na interface com os clientes. Em particular, a indústria deverá refletir sobre formas de tornar os CEO e os conselhos de administração mais responsáveis pela cibersegurança.

2.2. Reduzir drasticamente a cibercriminalidade

Quanto mais as nossas vidas assentam no mundo digital, mais são as oportunidades a explorar pelos cibercriminosos. A cibercriminalidade é uma das formas de criminalidade que mais têm aumentado, fazendo mais de um milhão de vítimas por dia em todo o mundo. Os cibercriminosos e as redes de cibercriminalidade estão a tornar-se cada vez mais sofisticados,

19 Este grupo de trabalho, criado na cimeira UE-EUA de novembro de 2010 (MEMO/10/597), está encarregado de desenvolver abordagens colaborativas para uma vasta gama de questões relacionadas com a cibersegurança e a cibercriminalidade.

20 O programa «Internet mais segura» financia uma rede de ONG ativas no domínio da proteção das crianças em linha, uma rede de organismos policiais/judiciais que trocam informações e boas práticas no que respeita à exploração criminosa da Internet na difusão de material pedopornográfico e uma rede de investigadores que recolhem informações sobre as utilizações, os riscos e as consequências das tecnologias em linha para a vida das crianças.

21 Também com o envolvimento das autoridades nacionais competentes, incluindo as autoridades competentes em matéria de SRI e as autoridades responsáveis pela proteção de dados.

pelo que precisamos de dispor das ferramentas operacionais corretas e de capacidades para os combater. Os cibercrimes são altamente lucrativos e de baixo risco e muitas vezes os criminosos exploram o anonimato dos domínios dos sítios Web. A cibercriminalidade não conhece fronteiras – graças ao alcance planetário da Internet, as autoridades policiais devem adotar uma abordagem transfronteiras coordenada e de colaboração para responder a esta ameaça crescente.

Uma legislação rigorosa e eficaz

A UE e os Estados-Membros devem dotar-se de uma legislação rigorosa e eficaz para combater a cibercriminalidade. A Convenção do Conselho da Europa sobre Cibercriminalidade, também conhecida por Convenção de Budapeste, é um tratado internacional vinculativo que fornece um quadro apropriado para a adoção de legislação nacional.

A UE já adotou legislação relativa à cibercriminalidade, nomeadamente uma diretiva relativa à luta contra a exploração sexual das crianças em linha e a pornografia infantil[22]. A UE está também prestes a chegar a acordo sobre uma diretiva relativa a ataques contra os sistemas de informação, especialmente através da utilização de «botnets».

A Comissão irá:

- Assegurar a transposição e a implementação rápidas das diretivas relativas à cibercriminalidade;
- Instar os Estados-Membros que ainda não ratificaram a **Convenção do Conselho da Europa sobre Cibercriminalidade** a ratificarem e aplicarem as suas disposições o mais depressa possível.

Meios operacionais acrescidos para combater a cibercriminalidade

A evolução das técnicas de cibercriminalidade conheceu uma rápida aceleração: as agências responsáveis não podem combater a cibercriminalidade com ferramentas operacionais ultrapassadas. Atualmente, nem todos os Estados-Membros da UE dispõem da capacidade operacional necessária para reagirem eficazmente à cibercriminalidade. Todos os Estados-Membros necessitam de unidades nacionais eficazes de combate à cibercriminalidade.

A Comissão irá:

- Através dos seus programas de financiamento[23], apoiar os Estados-Membros na **identificação das lacunas e no reforço da sua capacidade** para investigar e combater a cibercriminalidade. Além disso, a Comissão irá apoiar os organismos que fazem a ligação entre a investigação/as universidades, os agentes policiais/judiciais e o setor privado, cujo trabalho tem afinidades com o atualmente realizado pelos centros de excelência para a cibercriminalidade já criados em alguns Estados-Membros e que são financiados pela Comissão.
- Juntamente com os Estados-Membros, coordenar os esforços para identificar as

[22] Diretiva 2011/93/UE, que substitui a Decisão-Quadro 2004/68/JAI do Conselho.

[23] Em 2013, no âmbito do programa «Prevenir e combater a criminalidade» (ISEC). Após 2013, no âmbito do Fundo para a Segurança Interna (novo instrumento do QFP).

melhores práticas e as melhores técnicas disponíveis, inclusivamente com o apoio do JRC, para combater a cibercriminalidade (por exemplo, no que diz respeito ao desenvolvimento e à utilização de ferramentas forenses ou à análise das ameaças).

- Trabalhar em estreita cooperação com o recém-criado **Centro Europeu da Cibercriminalidade (EC3), no quadro da Europol e com a Eurojust** para harmonizar tais abordagens políticas com as melhores práticas na esfera operacional.

Uma melhor coordenação a nível da UE

A UE pode complementar o trabalho dos Estados-Membros facilitando a adoção de uma abordagem coordenada e colaborativa, que reúna as autoridades policiais e judiciais e as partes interessadas dos setores público e privado da UE e internacionais.

A Comissão irá:

- Apoiar o recém-criado **Centro Europeu da Cibercriminalidade** (EC3), enquanto ponto focal europeu no combate à cibercriminalidade. O EC3 fornecerá análises e informações (Intelligence), apoiará as investigações, garantirá investigação forense de elevado nível, facilitará a cooperação, criará canais para a partilha de informações entre as autoridades competentes dos Estados-Membros, o setor privado e outras partes interessadas e assumirá progressivamente o papel de porta-voz das forças policiais[24].
- Apoiar os esforços para melhorar a prestação de contas dos agentes de registo de nomes de domínio e garantir a exatidão das informações sobre a propriedade dos sítios Web, nomeadamente com base nas recomendações *Law Enforcement Recommendations* à ICANN (Internet Corporation for Assigned Names and Numbers), em conformidade com o direito da União, incluindo as regras da proteção de dados.
- Tirar partido da legislação recente para intensificar os esforços da UE no combate aos abusos sexuais de crianças em linha. A Comissão adotou uma estratégia europeia destinada a melhorar a Internet para as crianças[25] e, juntamente com os países da União Europeia e outros, lançou uma **aliança mundial contra os abusos sexuais de crianças em linha**[26]. A Aliança é um veículo para outras ações dos Estados-Membros apoiadas pela Comissão e pelo Centro Europeu da Cibercriminalidade.

A Comissão pede à Europol (EC3) que:

- Inicialmente focalize a sua análise e o seu apoio operacional às investigações da cibercriminalidade efetuadas pelos Estados-Membros de modo a ajudar a desmantelar e a desorganizar as redes de cibercriminalidade principalmente nas

[24] Em 28 de março de 2012, a Comissão Europeia adotou uma Comunicação intitulada «Luta contra a criminalidade na era digital: criação de um Centro Europeu da Cibercriminalidade».

[25] COM(2012) 196 final.

[26] Conclusões do Conselho sobre uma aliança mundial contra os abusos sexuais de crianças em linha (Declaração Conjunta UE-EUA) de 7 e 8 de junho de 2012 e Declaração sobre o lançamento da aliança mundial contra os abusos sexuais de crianças em linha (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm).

áreas do abuso sexual de crianças, das fraudes nos pagamentos, dos «*botnets*» e da intrusão.

- Elabore regularmente relatórios estratégicos e operacionais sobre as tendências e as novas ameaças, para identificar as prioridades e definir alvos para a atividade de investigação das equipas dos Estados-Membros especializadas em cibercriminalidade.

A Comissão pede à Academia Europeia de Polícia (CEPOL) que, em cooperação com a Europol:

- Coordene a conceção e o planeamento de cursos de formação para dotar os órgãos policiais/judiciais dos conhecimentos e competências especializadas necessários para combater eficazmente a cibercriminalidade.

A Comissão pede à Eurojust que:

- Identifique os principais obstáculos à cooperação judiciária em matéria de investigações da cibercriminalidade e à coordenação entre os Estados-Membros e com os países terceiros e apoie a investigação e a repressão da cibercriminalidade, tanto ao nível estratégico como operacional, assim como as atividades de formação neste domínio.

A Comissão pede à Eurojust e à Europol (EC3) que:

- Cooperem estreitamente, nomeadamente através do intercâmbio de informações, para aumentar a sua eficácia no combate à cibercriminalidade, de acordo com os respetivos mandatos e competência.
-

2.3. Desenvolver a política e as capacidades de ciberdefesa no quadro da Política Comum de Segurança e Defesa (PCSD)

Os esforços da UE no domínio da cibersegurança também envolvem a dimensão da ciberdefesa. Para aumentar a resiliência dos sistemas de comunicação e informação que apoiam a política de defesa dos Estados-Membros e os interesses da segurança nacional, o desenvolvimento de capacidades de ciberdefesa deve centrar-se na deteção de ameaças informáticas sofisticadas, na resposta a dar e na recuperação posterior.

Perante ameaças multifacetadas, há que melhorar as sinergias entre as abordagens civil e militar na proteção dos ativos informáticos críticos. Estes esforços devem ser apoiados pela investigação e desenvolvimento e por uma cooperação mais estreita entre os governos, o setor privado e as universidades da UE. Para evitar duplicações, a UE irá explorar as possibilidades de a UE e a NATO complementarem os seus esforços para aumentar a resiliência das infraestruturas críticas das Administrações, da defesa e outras infraestruturas informáticas das quais dependem os membros de ambas as organizações.

A Alta Representante, pedindo a colaboração dos Estados-Membros e da Agência Europeia de Defesa, centrar-se-á nas seguintes atividades cruciais:

- Avaliar as exigências operacionais da UE em matéria de ciberdefesa e promover o desenvolvimento das capacidades e das tecnologias da UE nessa matéria para abordar todos os aspetos do desenvolvimento de capacidades - incluindo a doutrina, a liderança, a organização, o pessoal, a formação, as tecnologias, as infraestruturas, a logística e a interoperabilidade;

- Desenvolver o quadro político da UE em matéria de ciberdefesa para proteger as redes no quadro das missões e operações da PCSD, incluindo a gestão dinâmica dos riscos, a melhoria da análise das ameaças e a partilha de informações. Melhorar as oportunidades de formação e exercícios de ciberdefesa para os militares no contexto europeu e multinacional, incluindo a integração de elementos de ciberdefesa nos atuais catálogos de exercícios;

- Promover o diálogo e a coordenação entre os atores civis e militares na UE – com especial realce para o intercâmbio de boas práticas, o intercâmbio de informações, o alerta precoce, a resposta a incidentes, a avaliação dos riscos, a sensibilização e a atribuição de prioridade à cibersegurança.

- Assegurar o diálogo com os parceiros internacionais, incluindo a NATO, outras organizações internacionais e centros de excelência multinacionais, a fim de garantir capacidades de defesa efetivas, identificar os domínios de cooperação e evitar a duplicação de esforços.

2.4. Desenvolver os recursos industriais e tecnológicos para a cibersegurança

A Europa dispõe de excelentes capacidades de investigação e desenvolvimento, mas muitos dos líderes mundiais em matéria de produtos e serviços TIC inovadores estão sediados fora da UE. Existe o risco de a Europa se tornar excessivamente dependente não só de TIC produzidas noutros países, mas também de soluções de segurança desenvolvidas fora das suas fronteiras. É fundamental garantir que os componentes de *hardware* e *software* produzidos na UE e em países terceiros que são utilizados em serviços e infraestruturas críticos, e cada vez mais em dispositivos móveis, sejam de confiança, seguros e garantam a proteção dos dados pessoais.

Promover um mercado único dos produtos de cibersegurança

Apenas é possível assegurar um elevado nível de segurança se todos os elementos da cadeia de valor (por exemplo, fabricantes de equipamentos, criadores de *software*, fornecedores de serviços da sociedade da informação) fizerem da segurança uma prioridade. Tudo indica[27], no entanto, que muitos intervenientes ainda veem na segurança pouco mais do que um encargo adicional e é escassa a procura de soluções nesse domínio. É necessário que sejam implementados ao longo de toda a cadeia de valor dos produtos TIC utilizados na Europa requisitos de desempenho em matéria de cibersegurança. O setor privado precisa de incentivos para garantir um elevado nível de cibersegurança; por exemplo, rótulos que indiquem um desempenho adequado a nível da cibersegurança permitirão às empresas com um bom desempenho e um bom historial a esse nível transformá-lo num trunfo e obter

[27] Ver a avaliação de impacto constante do documento de trabalho dos serviços da Comissão, que acompanha a proposta de diretiva relativa à segurança das redes e da informação, ponto 4.1.5.2.

vantagem competitiva. Também as obrigações estabelecidas na proposta de diretiva relativa à segurança das redes e da informação contribuirão significativamente para incrementar a competitividade das empresas nos setores abrangidos.

Deve igualmente ser estimulada a procura de produtos altamente seguros no mercado europeu. Em primeiro lugar, a presente estratégia visa aumentar a cooperação e a transparência sobre a segurança dos produtos TIC. Apela ao estabelecimento de uma plataforma que reúna as partes interessadas europeias relevantes, públicas e privadas, para identificar as boas práticas em matéria de cibersegurança em toda a cadeia de valor e criar condições de mercado propícias ao desenvolvimento e à adoção de soluções TIC seguras. Uma das primeiras prioridades deverá ser a criação de incentivos à realização de uma gestão adequada dos riscos e a adoção de normas e soluções de segurança, bem como, eventualmente, o estabelecimento de sistemas voluntários de certificação a nível da UE com base nos sistemas existentes na UE e a nível internacional. A Comissão promoverá a adoção de abordagens coerentes entre os Estados-Membros, a fim de evitar disparidades que causam desvantagens para as empresas em função da localização.

Em segundo lugar, a Comissão apoiará a elaboração de normas de segurança e colaborará no estabelecimento de sistemas de certificação voluntários no domínio da computação em nuvem em toda a UE, não deixando de ter na devida conta a necessidade de assegurar a proteção dos dados. Os trabalhos devem incidir na segurança da cadeia de abastecimento, em particular nos setores económicos críticos (sistemas de controlo industrial, infraestruturas energéticas e de transportes). Esses trabalhos devem basear-se no trabalho de normalização em curso nos organismos europeus de normalização (CEN, CENELEC e ETSI)[28], no trabalho do Grupo de Coordenação da Cibersegurança (CSCG), assim como nos conhecimentos especializados da ENISA, da Comissão e de outros intervenientes relevantes.

A Comissão irá:

- Lançar em 2013 uma **plataforma** público-privada **sobre soluções SRI** para criar incentivos à adoção de soluções TIC seguras e à adesão ao conceito de bom desempenho em matéria de cibersegurança, a aplicar aos produtos TIC utilizados na Europa.
- Propor, em 2014, recomendações para garantir a cibersegurança em toda a cadeia de valor das TIC, inspirando-se nos trabalhos desta plataforma.
- Estudar de que modo os principais fornecedores de hardware e software TIC poderão informar as autoridades nacionais competentes das vulnerabilidades detetadas suscetíveis de terem importantes implicações na segurança.

A Comissão pede à ENISA que:

- Elabore, em cooperação com as autoridades nacionais competentes, com os intervenientes relevantes, com os organismos de normalização internacionais e europeus e com o Centro Comum de Investigação da Comissão Europeia, **orientações técnicas e recomendações para a adoção de normas e de boas práticas no domínio da segurança das redes e da informaçã**o nos setores público e privado.

[28] Em particular no âmbito do mandato M/490 relativo a normas para as redes inteligentes, no que respeita ao primeiro conjunto de normas para uma rede inteligente e uma arquitetura de referência.

A Comissão convida as partes interessadas dos setores público e privado a:

- Estimularem o desenvolvimento e a adoção de **normas de segurança** e de normas técnicas da iniciativa da indústria e a observância dos princípios da segurança e da proteção da privacidade asseguradas de raiz pelos fabricantes de produtos TIC e pelos prestadores de serviços TIC, incluindo os prestadores de serviços de computação em nuvem; as novas gerações de *software* e *hardware* devem estar equipadas com **características de segurança mais robustas, incorporadas e conviviais para o utilizador**.
- Elaborarem normas de desempenho das empresas, por iniciativa destas, em matéria de cibersegurança e melhorarem as informações a disponibilizar ao público através da elaboração de **rótulos de segurança** ou marcas de garantia de qualidade que ajudem o consumidor a orientar-se no mercado.

Promover os investimentos em I&D e em inovação

A investigação e desenvolvimento (I&D) pode dar solidez à política industrial, promover a confiança na indústria europeia das TIC, desenvolver o mercado interno e reduzir a dependência da Europa em relação às tecnologias estrangeiras. A I&D deve corrigir as lacunas tecnológicas na segurança das TIC, preparar os sistemas para os novos desafios que se colocarão à segurança, ter em conta a constante evolução das necessidades dos utilizadores e tirar partido das tecnologias de dupla utilização (civil e militar). Deve igualmente continuar a apoiar o desenvolvimento da criptografia. Esse trabalho tem de ser complementado por esforços para traduzir os resultados da I&D em soluções comerciais, através do fornecimento dos incentivos necessários e da criação das condições políticas apropriadas.

A UE deve aproveitar da melhor forma o programa-quadro de investigação e inovação Horizonte 2020[29], que será lançado em 2014. A proposta da Comissão contém objetivos específicos para tornar as TIC fiáveis, assim como para combater a cibercriminalidade, que se alinham com a presente estratégia. O Horizonte 2020 apoiará a investigação sobre segurança em relação com as tecnologias TIC emergentes, fornecerá soluções para sistemas, serviços e aplicações TIC seguros de extremo a extremo, concederá incentivos para a implantação e a adoção das soluções existentes e procurará resolver o problema da interoperabilidade das redes e dos sistemas informáticos. A nível da UE chamar-se-á a atenção especificamente para a necessidade de otimizar e coordenar melhor os diferentes programas de financiamento (o Horizonte 2020, o Fundo para a Segurança Interna, a investigação levada a cabo pela Agência Europeia de Defesa, incluindo o Quadro Europeu de Cooperação).

[29] O programa Horizonte 2020 é o instrumento financeiro que implementa a União da Inovação, uma iniciativa emblemática da estratégia Europa 2020, que visa assegurar a competitividade da Europa na arena mundial. O novo programa-quadro de investigação e inovação da UE, para o período de 2014-2020, será um dos instrumentos para o crescimento e a criação de novos postos de trabalho na Europa.

A Comissão irá:

- Utilizar o programa Horizonte 2020 para abordar diversos aspetos da privacidade e da segurança nas TIC, partindo da I&D para chegar à inovação e à implantação. O Horizonte 2020 desenvolverá também ferramentas e instrumentos para combater as atividades criminosas e terroristas que visem o ciberespaço.
- Estabelecer mecanismos para uma melhor coordenação das agendas de investigação das instituições da União Europeia e dos Estados-Membros, e incentivar os Estados-Membros a investirem mais em I&D.

A Comissão convida os Estados-Membros a:

- Desenvolverem, até ao final de 2013, boas práticas na utilização do **poder de compra das administrações públicas** (através, por exemplo, dos contratos públicos), a fim de estimular o desenvolvimento e a implantação de características de segurança nos produtos e serviços TIC.
- Promoverem o envolvimento precoce das empresas e das universidades no desenvolvimento e na coordenação das soluções. Para tal, há que tirar o maior partido possível da base industrial da Europa e das inovações tecnológicas desenvolvidas graças às respetivas atividades de I&D, e coordenar as agendas de investigação das organizações civis e militares.

A Comissão pede à Europol e à ENISA que:

- Identifiquem as novas tendências e necessidades face à evolução dos padrões da cibercriminalidade e da cibersegurança, de modo a desenvolver ferramentas e tecnologias digitais adequadas para fins forenses.

A Comissão convida as partes interessadas dos setores público e privado a:

- Desenvolverem, em cooperação com o setor dos seguros, **uma métrica harmonizada para o cálculo dos prémios de risco**, que permitirá às empresas que tenham feito investimentos na segurança beneficiar de prémios de risco mais baixos.

2.5. Definir uma política internacional coerente em matéria de ciberespaço para a União Europeia e promover os valores fundamentais da UE

A preservação de um ciberespaço aberto, livre e seguro é um desafio de dimensão mundial a que a UE deve responder conjuntamente com os parceiros e organizações internacionais relevantes, com o setor privado e com a sociedade civil.

Na sua política internacional relativa ao ciberespaço, a UE procurará promover a abertura e a liberdade da Internet, encorajar os esforços tendentes a estabelecer normas de comportamento e aplicar as leis internacionais em vigor no ciberespaço. A UE também tudo fará para reduzir a clivagem digital e participará ativamente nos esforços internacionais para construir capacidade de cibersegurança. O envolvimento internacional da UE nas questões que dizem respeito ao ciberespaço pautar-se-á pelos valores fundamentais da UE, a saber, a dignidade humana, a liberdade, a democracia, a igualdade, o Estado de direito e o respeito pelos direitos fundamentais.

Integrar as questões do ciberespaço nas relações externas e na política externa e de segurança comum (PESC) da UE

A Comissão, a Alta Representante e os Estados-Membros devem articuladamente definir para a UE uma política internacional coerente em matéria de ciberespaço que vise um maior empenhamento e o reforço das relações com os principais parceiros e organizações internacionais, bem como com a sociedade civil e o setor privado. As consultas de parceiros internacionais sobre as questões do ciberespaço devem ser concebidas, coordenadas e efetuadas com o intuito de acrescentar valor aos atuais diálogos bilaterais entre os Estados-Membros da UE e os países terceiros. A UE atribuirá uma importância renovada ao diálogo com os países terceiros, com especial destaque para os parceiros com os quais exista sintonia de ideias e que partilhem os valores da UE. Procurará assegurar um nível elevado de proteção dos dados, nomeadamente em caso de transferência de dados pessoais para um país terceiro. Para responder aos desafios que o ciberespaço enfrenta à escala mundial, a UE procurará uma cooperação mais estreita com as organizações ativas neste domínio, como o Conselho da Europa, a OCDE, a ONU, a OSCE, a NATO, a UA, a ASEAN e OEA. A nível bilateral, a cooperação com os Estados Unidos é particularmente importante e será mais desenvolvida, nomeadamente no contexto do Grupo de Trabalho UE-EUA para a Cibersegurança e a Cibercriminalidade.

Um dos principais elementos da política internacional da UE no domínio do ciberespaço será a promoção do mesmo como espaço de liberdade e de direitos fundamentais. O alargamento do acesso à Internet deverá fazer avançar as reformas democráticas e a sua promoção em todo o mundo. O aumento da conectividade mundial não deve ser acompanhado de censura ou de vigilância das populações. A UE deve promover a responsabilidade social das empresas[30] e lançar iniciativas internacionais para melhorar a coordenação a nível mundial neste domínio.

A responsabilidade pelo aumento da segurança do ciberespaço é de todos os atores da sociedade da informação a nível mundial, desde os cidadãos até aos governos. A UE apoia os esforços para definir normas de conduta para o ciberespaço, a que todas as partes interessadas devem aderir. Da mesma maneira que, na UE, os cidadãos devem cumprir os seus deveres cívicos, assumir as suas responsabilidades sociais e respeitar as leis em linha, assim também os Estados devem respeitar as normas e leis existentes. Em questões de segurança internacional, a UE incentiva a elaboração de medidas que promovam a confiança no campo da cibersegurança, de modo a aumentar a transparência e reduzir o risco de mal-entendidos quanto ao comportamento dos Estados.

A UE não apela à criação de novos instrumentos jurídicos internacionais para as questões do ciberespaço.

As obrigações legais consagradas no Pacto Internacional sobre os Direitos Civis e Políticos, na Convenção Europeia dos Direitos do Homem e na Carta dos Direitos Fundamentais da União Europeia devem ser igualmente respeitadas no universo em linha. A UE concentrar-se-á nos meios de garantir que essas medidas sejam também aplicadas no ciberespaço.

[30] Responsabilidade social das empresas: uma nova estratégia da UE para o período de 2011-2014; COM(2011) 681 final.

Para combater a cibercriminalidade, a Convenção de Budapeste é um instrumento aberto à adoção pelos países terceiros. Fornece um modelo para a elaboração de legislação nacional sobre cibercriminalidade e constitui uma base para a cooperação internacional neste domínio.

Se os conflitos armados se estenderem ao ciberespaço, aplicar-se-á ao caso vertente o Direito Internacional Humanitário e, se for caso disso, a legislação sobre os direitos do homem.

Reforço das capacidades em matéria de cibersegurança e desenvolvimento de infraestruturas informáticas resilientes nos países terceiros

O bom funcionamento das infraestruturas subjacentes que fornecem e facilitam os serviços de comunicações beneficiará de uma cooperação internacional acrescida, que inclua o intercâmbio das melhores práticas, a partilha de informações, exercícios de alerta precoce e de gestão conjunta de incidentes, etc. A UE contribuirá para a consecução deste objetivo intensificando os esforços internacionais em curso para reforçar as redes de cooperação entre os governos e o setor privado que visam a proteção das infraestruturas críticas da informação (PICI).

Nem todas as regiões do mundo beneficiam dos efeitos positivos da Internet, devido à inexistência de acesso aberto, seguro, interoperável e fiável. A União Europeia continuará, pois, a apoiar os esforços dos países no sentido de alargarem o acesso à Internet e a utilização da mesma pelas suas populações, garantirem a integridade e a segurança da rede e combaterem eficazmente a cibercriminalidade.

Em cooperação com os Estados-Membros, a Comissão e a Alta Representante irão:

- Trabalhar no sentido de definir para a UE uma política internacional coerente em matéria de ciberespaço, que vise aprofundar a colaboração com os principais parceiros e organizações internacionais, integrar as questões do ciberespaço na PESC e melhorar a coordenação das questões da cibersegurança que tenham dimensão mundial;
- Apoiar a elaboração de normas de comportamento e o estabelecimento de medidas que visem reforçar a confiança no campo da cibersegurança. Facilitar o diálogo sobre a forma de aplicar o direito internacional vigente no ciberespaço e promover a Convenção de Budapeste para combater a cibercriminalidade;
- Apoiar a promoção e a proteção dos direitos fundamentais, incluindo o acesso à informação e a liberdade de expressão, com os seguintes enfoques: a) estabelecer novas orientações públicas sobre a liberdade de expressão em linha e fora de linha; b) controlar a exportação de produtos ou serviços suscetíveis de serem utilizados para a censura ou a vigilância em linha das populações; c) conceber medidas e ferramentas destinadas a alargar o acesso à Internet e a sua abertura e resiliência para resolver o problema da censura ou da vigilância das populações através das tecnologias da comunicação; d) dar autonomia às partes interessadas para utilizarem as tecnologias das

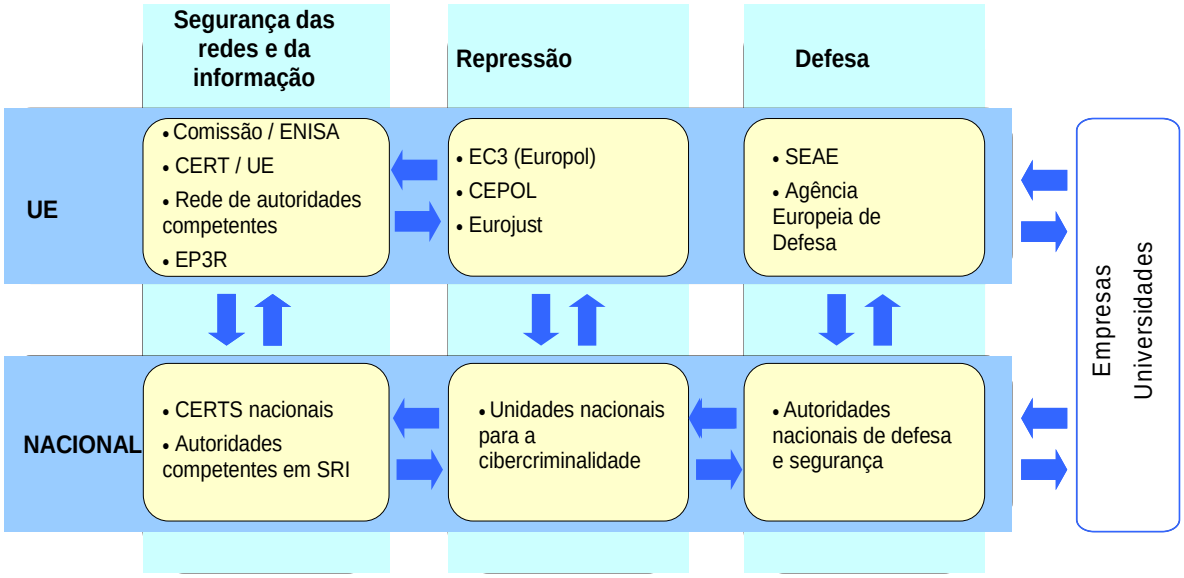
comunicações para promoverem os direitos fundamentais;

- Colaborar com os parceiros e as organizações internacionais, o setor privado e a sociedade civil para ajudar os países terceiros a desenvolverem capacidades que permitam melhorar o acesso à informação e a uma Internet aberta, prevenir e combater as ameaças informáticas, incluindo acontecimentos acidentais, a cibercriminalidade e o ciberterrorismo, e reforçar a coordenação entre os doadores para canalizar os esforços nesse sentido;
- Utilizar os diferentes instrumentos de ajuda da UE para a criação de capacidades no domínio da cibersegurança, incluindo a assistência à formação das forças policiais e judiciárias e do pessoal técnico para lidarem com as ciberameaças, assim como apoiar a criação de políticas, estratégias e instituições nacionais neste domínio em países terceiros;
- Intensificar a coordenação das políticas e a partilha de informações através das redes internacionais de proteção das infraestruturas críticas da informação, como a rede Meridian, assim como a cooperação entre as autoridades competentes em matéria de SRI e outras.

3. FUNÇÕES E RESPONSABILIDADES

Numa economia e numa sociedade digitais interconectadas, os incidentes informáticos não se detêm nas fronteiras. Todos os intervenientes, desde as autoridades competentes em matéria de SRI, as CERT e as autoridades policiais até à indústria, devem assumir responsabilidades quer a nível nacional quer a nível da UE, e trabalhar em conjunto para reforçar a cibersegurança. Como isso pode implicar o confronto com diferentes quadros legais e jurisdições, um dos principais desafios para a UE consiste em clarificar os papéis e as responsabilidades dos muitos atores envolvidos.

Dada a complexidade da questão e a diversidade de atores envolvidos, uma supervisão europeia centralizada não é a resposta adequada. Os governos nacionais estão em melhor posição para organizar a prevenção e a resposta aos incidentes e ataques informáticos e para estabelecer contactos e redes com o setor privado e o grande público através dos canais estabelecidos e dos quadros legais. Ao mesmo tempo, devido à natureza sem fronteiras potencial ou real dos riscos, uma resposta nacional eficaz exige o envolvimento da UE. Para tratar dos problemas da cibersegurança de modo completo, as atividades devem articular-se em torno de três pilares fundamentais — a SRI, a repressão e a defesa — que também são regidos por quadros legais diferentes:



3.1. Coordenação entre as autoridades competentes em matéria de SRI/CERT, as autoridades policiais e o setor da defesa

Nível nacional

Os Estados-Membros devem dispor, já hoje ou como resultado da presente estratégia, de estruturas preparadas para garantir a resiliência do ciberespaço, combater a cibercriminalidade e prover à defesa e devem atingir o nível de capacidade necessário para lidar com incidentes informáticos. Contudo, uma vez que podem ser várias as entidades responsáveis operacionalmente pelas diferentes dimensões da cibersegurança, e dada a importância de envolver o setor privado, é necessário a nível nacional otimizar a coordenação entre os diferentes ministérios. Os Estados-Membros devem definir, nas suas estratégias nacionais de cibersegurança, o papel e as responsabilidades das suas várias entidades nacionais.

A partilha de informações entre as entidades nacionais e com o setor privado deve ser encorajada, para que os Estados-Membros e o setor privado possam manter uma visão global das diferentes ameaças e compreender melhor as novas tendências e técnicas utilizadas quer para perpetrar ciberataques quer para reagir aos mesmos mais prontamente. No estabelecimento dos planos nacionais de cooperação em matéria de SRI que devem ser ativados em caso de incidentes informáticos, os Estados-Membros devem poder atribuir claramente os papéis e as responsabilidades e otimizar as ações de resposta.

Nível da UE

Como para o nível nacional, existem a nível da UE diversos atores que se ocupam da cibersegurança, designadamente, a ENISA, a Europol/EC3 e a Agência Europeia de Defesa (AED) - três agências ativas respetivamente no campo da SRI, da repressão e da defesa. Estas agências têm conselhos de administração em que estão representados os Estados-Membros e constituem plataformas de coordenação a nível da UE.

A coordenação e a colaboração entre a ENISA, a Europol/EC3 e a AED numa série de domínios em que estão conjuntamente envolvidas serão encorajadas, nomeadamente no que

respeita à análise das tendências, à avaliação dos riscos, à formação e à partilha das melhores práticas. As três devem colaborar, preservando simultaneamente as suas especificidades. Estas agências, conjuntamente com a equipa CERT-UE, a Comissão e os Estados-Membros, devem apoiar o desenvolvimento de uma comunidade de confiança de peritos técnicos e políticos neste domínio.

Os canais informais de coordenação e colaboração serão complementados por ligações mais estruturais. O pessoal militar da UE e a equipa do projeto de ciberdefesa da AED podem servir de vetor para a coordenação da defesa. O Conselho de Programa da Europol/EC3 (Centro Europeu da Cibercriminalidade) reunirá entre outros o EUROJUST, a CEPOL, os Estados-Membros[31], a ENISA e a Comissão oferecendo-lhes a possibilidade de partilharem os seus diferentes conhecimentos e técnicas e garantir que as ações do EC3 sejam realizadas em parceria, reconhecendo as competências acrescidas e respeitando os mandatos de todas as partes interessadas. O novo mandato da ENISA deve permitir-lhe estabelecer uma maior ligação à Europol e reforçar as ligações com as partes interessadas da indústria. Mais importante ainda, a proposta legislativa da Comissão sobre a SRI estabelecerá um quadro de cooperação através de uma rede de autoridades nacionais competentes nessa matéria e regulará a partilha de informações entre essas autoridades e as autoridades policiais/judiciais.

Nível internacional

A Comissão e a Alta Representante garantem, juntamente com os Estados-Membros, uma ação internacional coordenada no domínio da cibersegurança. Ao fazê-lo, empenhar-se-ão na defesa dos valores fundamentais da UE e na promoção de uma utilização pacífica, aberta e transparente das cibertecnologias. A Comissão, a Alta Representante e os Estados-Membros participam no diálogo político com os seus parceiros internacionais e com organizações internacionais como o Conselho da Europa, as Nações Unidas, a NATO, a OSCE e a OCDE.

3.2. Apoio da UE em caso de incidente ou ataque informático importante

Os grandes incidentes ou ataques informáticos são suscetíveis de ter impacto nas administrações, nas empresas e nos cidadãos da UE. Como resultado da presente estratégia, e em particular da proposta de diretiva relativa à SRI, a prevenção, a deteção e a resposta a incidentes informáticos deverão melhorar e os Estados-Membros e a Comissão deverão manter-se mutuamente mais bem informados sobre os grandes incidentes ou ataques informáticos. No entanto, os mecanismos de resposta variarão consoante a natureza, a magnitude e as implicações transfronteiras dos incidentes.

Se o incidente tiver consequências graves para a continuidade das atividades das empresas, a Diretiva SRI propõe que os planos de cooperação nacionais ou da União Europeia em matéria de SRI sejam acionados, dependendo da natureza transfronteiras do incidente. A rede de autoridades competentes em matéria de SRI será utilizada nesse contexto para a partilha de informações e apoio. Isto permitirá a preservação e/ou a restauração das redes e serviços afetados.

Se o incidente parecer estar associado a um crime, a Europol/o EC3 devem ser informados para que - juntamente com as autoridades policiais dos países afetados – possam iniciar uma

[31] Através da representação na Task Force da UE para a cibercriminalidade, que é constituída pelos chefes das unidades nacionais para a cibercriminalidade.

investigação, preservar as provas, identificar os autores e, em última instância, garantir que sejam alvo de processo judicial.

Se o incidente estiver aparentemente relacionado com espionagem informática ou houver suspeitas de se tratar de um ataque comanditado por um Estado, ou tiver implicações na segurança nacional, as autoridades nacionais de segurança e de defesa alertarão as suas congéneres, para que estas saibam que estão a ser atacadas e se possam defender. Os mecanismos de alerta precoce serão então ativados e, se necessário, também os procedimentos de gestão de crises ou outros. Um incidente ou ataque informático particularmente grave pode constituir razão suficiente para um Estado-Membro invocar a cláusula de solidariedade da União Europeia (artigo 222.° do Tratado sobre o Funcionamento da União Europeia).

Se o incidente tiver aparentemente comprometido dados pessoais, as autoridades nacionais de proteção de dados ou a autoridade reguladora nacional devem, nos termos da Diretiva 2002/58/CE, ser envolvidas no processo.

Finalmente, para o tratamento dos ciberincidentes e dos ciberataques serão preciosas as redes de contactos e o apoio dos parceiros internacionais, que pode consistir na atenuação dos efeitos por meios técnicos, na investigação criminal ou na ativação dos mecanismos de resposta e gestão de crises.

4. CONCLUSÕES E SEGUIMENTO

A presente proposta de estratégia da União Europeia para a cibersegurança, apresentada pela Comissão e pela Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, define a visão da UE e as ações necessárias, fundadas numa proteção e numa promoção eficazes dos direitos dos cidadãos, para tornar o ambiente em linha na UE o mais seguro do mundo[32].

Esta visão apenas pode ser concretizada através de uma verdadeira parceria entre os numerosos intervenientes, que assuma a responsabilidade e responda aos desafios que se perfilam.

A Comissão e a Alta Representante convidam pois o Conselho e o Parlamento Europeu a aprovarem a estratégia e a contribuírem para a realização das ações descritas. É igualmente necessário um apoio e empenhamento decididos por parte do setor privado e da sociedade civil, que são atores fundamentais para aumentar o nosso nível de segurança e proteger os direitos dos cidadãos.

Chegou o momento de passar à ação. A Comissão e a Alta Representante estão determinadas a trabalhar em conjunto com todos os atores para garantir a segurança necessária à Europa.

[32] O financiamento da estratégia far-se-á dentro dos limites dos montantes previstos para cada um dos domínios políticos relevantes (CEF, Horizonte 2020, Fundo para a Segurança Interna, PESC e Cooperação Externa, nomeadamente o Instrumento de Estabilidade), como indicado na proposta da Comissão relativa ao quadro financeiro plurianual para 2014-2020 (sob reserva da aprovação pela autoridade orçamental e dos montantes definitivos do QFP adotado para 2014-2020). No que respeita à necessidade de assegurar a compatibilidade geral com o número de postos disponíveis para as agências descentralizadas e o subteto máximo para as agências descentralizadas em cada rubrica de despesas do próximo quadro financeiro plurianual, as agências (Academia Europeia de Polícia (CEPOL), a AED, a ENISA, a Eurojust e a Europol/EC3) que passam a assumir novas tarefas nos termos da presente comunicação serão incentivadas a fazê-lo na medida em que tenha sido estabelecida a sua capacidade real para absorver os recursos suplementares e em que tenham sido identificadas todas as possibilidades de reafetação.

Para que a estratégia seja posta em prática rapidamente e avaliada em função das eventuais evoluções, reunirão todas as partes interessadas numa conferência de alto nível e avaliarão os progressos efetuados em 12 meses.