COMISSÃO
EUROPEIA

Bruxelas, 5.7.2016
COM(2016) 410 final

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

Reforçar o sistema de ciberresiliência da Europa e promover uma indústria de cibersegurança competitiva e inovadora

1. INTRODUÇÃO/CONTEXTO

Todos os dias, os incidentes de cibersegurança causam graves prejuízos económicos para as empresas europeias e para a economia em geral. Estes incidentes comprometem a confiança dos cidadãos e das empresas na sociedade digital. O roubo de segredos e informações comerciais e dados pessoais, a perturbação de serviços - incluindo serviços essenciais - e das infraestruturas, pode resultar em perdas económicas de centenas de milhares de milhões de euros por ano[1]. Podem também ter consequências para os direitos fundamentais dos cidadãos e para a sociedade em geral.

A Estratégia da União Europeia para a Cibersegurança de 2013[2] (a seguir designada Estratégia da UE para a Cibersegurança), e o seu principal resultado - a Diretiva relativa à Segurança das Redes e da Informação (SRI)[3], que será adotada em breve - bem como a Diretiva 2013/40/UE relativa a ataques contra os sistemas de informação, constituem o núcleo da resposta política da União Europeia a estes desafios em matéria de cibersegurança. Além disso, a UE também dispõe de entidades especializadas, como a Agência da União Europeia para a Segurança das Redes e da Informação (ENISA), o Centro Europeu da Cibercriminalidade (EC3) da Europol e a Equipa de resposta a emergências informáticas (CERT-UE). Recentemente, foi igualmente lançada uma série de iniciativas setoriais (por exemplo no domínio da energia e dos transportes), a fim de aumentar a cibersegurança em vários setores críticos.

No entanto, apesar destes resultados positivos, a UE mantém-se vulnerável aos ciberincidentes. Tal poderá comprometer o mercado único digital e a vida económica e social no seu conjunto. O seu impacto poderá ir além da economia. No caso de ameaças híbridas[4], os ciberataques podem ser utilizados de forma coordenada com outras atividades para desestabilizar um país ou pôr em causa as instituições políticas.

Neste contexto, poderá ser difícil para a UE lidar com os ciberincidentes em grande escala, que envolvam simultaneamente vários Estados-Membros. Em sinergia com as comunicações sobre a luta contra as ameaças híbridas, bem como sobre a realização da Agenda Europeia para a Segurança[5], a Comissão está a estudar formas de abordar a realidade de uma cibersegurança em evolução e a avaliar novas medidas que possam ser necessárias para reforçar a capacidade de resistência e de resposta da UE a incidentes de cibersegurança.

Além disso, a Comissão também está a abordar a questão das capacidades da indústria da cibersegurança da UE. Apesar de ser impossível controlar toda a cadeia de valor das tecnologias digitais na Europa, é necessário, pelo menos, manter e desenvolver as capacidades essenciais. O fornecimento de produtos e serviços que oferecem o mais elevado nível de cibersegurança é uma oportunidade para a indústria europeia e poderá tornar-se uma forte

[1] *Perdas líquidas: estimativa dos custos globais da cibercriminalidade e impacto económico da cibercriminalidade II («Net Losses: estimating the Global Cost of Cybercrime Economic impact of cybercrime II»); Centro de Estudos Internacionais e Estratégicos, junho de 2014.*
[2] JOIN(2013) 1.
[3] COM(2013) 48.
[4] JOIN(2016) 18.
[5] COM(2016) 230.

vantagem competitiva. Prevê-se que o mercado mundial da cibersegurança estará entre os segmentos de crescimento mais rápido do setor das TIC[6]. Para conferir à UE um papel de liderança neste domínio, há que assegurar uma forte cultura de segurança dos dados, nomeadamente dos dados pessoais, e uma resposta eficaz aos incidentes. Este é um forte argumento para investir na UE, contribuindo assim para atingir os ambiciosos objetivos do mercado único digital a nível da criação crescimento e emprego.

Para atingir estes fins é necessário um forte empenho, nomeadamente através:

i) Do reforço da cooperação para melhorar o estado de preparação e lidar com os incidentes informáticos

Os mecanismos de cooperação existentes e acordados têm de ser reforçados para aumentar a resiliência e a preparação da UE, incluindo para uma eventual crise pan-europeia de cibersegurança. Estes mecanismos de cooperação devem ser exaustivos, abrangendo o ciclo de vida de um incidente, desde a prevenção até à sanção. Uma cooperação eficaz entre os Estados-Membros e a aplicação prática dos requisitos de segurança para os operadores críticos também vai exigir a procura soluções técnicas robustas por parte da indústria da cibersegurança.

Ao mesmo tempo, para assegurar a resiliência dos ativos informáticos críticos em toda a UE, são necessários esforços contínuos para encontrar sinergias entre os setores e integrar os requisitos de cibersegurança em todas as políticas relevantes da UE. A Comissão vai avaliar a necessidade de atualizar a Estratégia da UE para a Cibersegurança de 2013 num futuro próximo.

ii) Da resposta aos desafios que a Europa enfrenta em matéria de mercado único da cibersegurança

O Estratégia para o Mercado Único Digital[7] reconheceu que ainda existem lacunas específicas neste domínio tecnológico em rápida evolução das tecnologias e soluções para a segurança das redes. Ao mesmo tempo, os estudos de mercado mostram que o mercado interno da UE está ainda geograficamente fragmentado no que respeita ao fornecimento de produtos e serviços de cibersegurança[8]. A presente comunicação define uma série de medidas setoriais orientadas para o mercado para enfrentar estes desafios e lacunas do mercado único.

iii) Do desenvolvimento das capacidades industriais no domínio da cibersegurança

Na Estratégia da UE para a Cibersegurança e na Estratégia para o Mercado Único Digital, a Comissão comprometeu-se a promover o aumento da oferta de produtos e serviços de cibersegurança pela indústria da UE. Por conseguinte, a Comissão irá também adotar uma decisão que abre caminho a um acordo de parceria público-privada contratual (PPPc) em matéria de cibersegurança, que procurará promover a investigação europeia de vanguarda para a cibersegurança e a agenda de inovação para estímulo da competitividade.

[6] Ver SWD(2016) 216.
[7] COM(2015) 192.
[8] Ver SWD(2016) 216.

2. ELEVAR A COOPERAÇÃO, OS CONHECIMENTOS E AS CAPACIDADES PARA O NÍVEL SUPERIOR

A Estratégia da UE para a Cibersegurança, nomeadamente a futura Diretiva SRI[9], abrirá caminho para melhorar a cooperação a nível da UE entre os Estados-Membros. A transposição rápida e eficaz da diretiva será fundamental tendo em conta a crescente digitalização da vida económica e social (tendo também em conta a computação em nuvem, a Internet das coisas e a comunicação máquina-máquina), a crescente interligação transfronteiriça e a rápida evolução das ciberameaças[10]. Neste contexto, a UE tem de se preparar para a possibilidade de ocorrerem cibercrises em grande escala[11], incluindo, por exemplo, ataques simultâneos a sistemas informáticos críticos em vários Estados-Membros[12].

Por conseguinte, a cooperação à escala da UE é essencial para lidar tanto com os ciberincidentes de menor envergadura, mas com potencial de proliferação, como com possíveis ciberataques em grande escala, em vários Estados-Membros. A UE tem de integrar os aspetos de ciberdefesa nos atuais mecanismos de gestão de crises. Precisa também de assegurar uma cooperação eficaz e mecanismos de intercâmbio rápido de informação entre setores e Estados-Membros, para dar resposta e conter tais incidentes. Além disso, esses mecanismos devem funcionar de forma coerente, contribuindo assim para a luta contra o terrorismo, a criminalidade organizada e a cibercriminalidade. Tal aumentaria a capacidade da UE para se coordenar com os seus parceiros internacionais, a fim de dar uma resposta eficaz às ameaças e incidentes globais.

2.1. Aproveitar plenamente os mecanismos de cooperação em matéria de SRI e avançar para a ENISA 2.0

Uma parte essencial das capacidades nacionais exigidas pela Diretiva SRI são as equipas de resposta a incidentes informáticos (CSIRT) responsáveis pela reação rápida às ciberameaças e ciberincidentes. Estas equipas vão constituir a rede CSIRT para promover uma cooperação operacional eficaz sobre os incidentes de cibersegurança e a partilha de informações sobre os riscos. Além disso, a diretiva criará um Grupo de Cooperação para apoiar e facilitar a cooperação estratégica e reforçar a confiança entre os Estados-Membros.

Tendo em conta a natureza e a variedade das ciberameaças, a Comissão incentiva os Estados-Membros a tirarem o máximo partido dos mecanismos de cooperação em matéria de SRI e a reforçarem a cooperação transfronteiriça relacionada com a preparação para ciberincidentes em grande escala. Essa cooperação adicional relativa a ciberincidentes graves beneficiaria de uma abordagem coordenada para a cooperação em situações de crise entre os diversos elementos do ecossistema da cibersegurança. Tal abordagem pode ser objeto de um «roteiro» que deve igualmente assegurar as sinergias e a coerência com os atuais mecanismos de gestão

[9] A Diretiva SRI exigirá que os Estados-Membros identifiquem um leque de operadores de serviços essenciais em domínios como a energia, os transportes, as finanças e a saúde, para prevenir riscos para a cibersegurança e garantir igualmente que determinados prestadores de serviços digitais tomam as medidas adequadas para fazer face a esses riscos.
[10] Ver SWD(2016) 216.
[11] Ver, por exemplo, o relatório da ENISA: *Common practices of EU-level crisis management and applicability to cyber crises* (práticas comuns a nível da UE em matéria de gestão de crises e aplicabilidade às cibercrises (abril de 2016).
[12] Ver SWD(2016) 216.

de crises[13]. Deve então ser testada regularmente em exercícios de gestão de crises no ciberespaço e outras. Incluiria a definição do papel dos organismos a nível da UE, como a ENISA, a CERT-UE e o Centro Europeu da Cibercriminalidade (EC3) da Europol, e utilizaria as ferramentas desenvolvidas no âmbito da rede CSIRT. No primeiro semestre de 2017, a Comissão apresentará esse roteiro de cooperação ao Grupo de Cooperação, à rede CSIRT e às outras partes interessadas relevantes.

Atualmente, os conhecimentos e as competências em matéria de cibersegurança estão disponíveis a nível da UE, mas de uma forma dispersa e não estruturada. A fim de apoiar os mecanismos de cooperação em matéria de SRI, a informação deve ser reunida numa «plataforma de informação» que a torne facilmente acessível, mediante pedido, a todos os Estados-Membros. Esta plataforma tornar-se-ia um recurso central para permitir que as instituições e os Estados-Membros da UE troquem informações, conforme adequado. Um acesso mais fácil à informação melhor estruturada sobre cibersegurança, riscos e soluções potenciais deverá ajudar os Estados-Membros a aumentar as suas capacidades e adaptar as suas práticas, melhorando a resiliência global aos ataques. A Comissão, com o apoio da ENISA, da CERT-EU e das competências do seu Centro Comum de Investigação, vai promover a criação e assegurar a sustentabilidade da plataforma.

Além disso, deverá ser criado a nível da UE um Grupo Consultivo de alto nível sobre Cibersegurança[14], composto por peritos e decisores da indústria, do meio académico, da sociedade civil e de outras organizações relevantes. Este grupo permitirá à Comissão obter, de forma aberta e transparente, competências especializadas externas e contribuições para as suas políticas estratégicas de cibersegurança e ações a nível regulamentar ou de outras políticas públicas. Irá complementar e cooperar com outras estruturas em matéria de cibersegurança[15].

Além disso, a Comissão deve, até 20 de junho de 2018, proceder à avaliação da ENISA e a eventual alteração ou renovação do mandato da ENISA deve ser adotada até 19 de junho de 2020[16]. Tendo em conta o atual panorama em matéria de cibersegurança, a Comissão pretende antecipar a avaliação e, sob reserva dos seus resultados, apresentar uma proposta o mais rapidamente possível.

Ao avaliar a eventual necessidade de modificar o mandato da ENISA, a Comissão terá em conta os desafios para a cibersegurança acima descritos e o esforço global no sentido de intensificar a cooperação e a partilha de conhecimentos. Este processo constituirá uma oportunidade para analisar a possível melhoria das capacidades da Agência e as suas capacidades para apoiar os Estados-Membros, de forma sustentável, com vista a promover a resiliência a nível da cibersegurança. A reflexão sobre o mandato da ENISA deve, além disso, ter em conta as novas responsabilidades da Agência ao abrigo da Diretiva SRI, os novos objetivos políticos de apoio à indústria da cibersegurança (a estratégia para o mercado único

[13] Nomeadamente o Mecanismo Integrado da UE de Resposta Política a Situações de Crise, incluindo a decisão relativa às regras de execução pela União da cláusula de solidariedade (de 24 de julho de 2014), e os processos de tomada de decisão da Política Comum de Segurança e Defesa.
[14] Os grupos de peritos da Comissão estão sujeitos às regras horizontais estabelecidas na Decisão C(2016) 3301 da Comissão.
[15] Por exemplo, a Plataforma SRI, a PPPc em matéria de cibersegurança e as plataformas setoriais como a Plataforma de cibersegurança para peritos no domínio da energia (EECSP). Deverá igualmente contribuir para a mesa redonda de alto nível anunciado na comunicação sobre a digitalização da indústria europeia: COM(2016) 180.
[16] Regulamento (UE) n.º 526/2013 que revoga o Regulamento (CE) n.º 460/2004.

digital e, em especial, a PPPc), a evolução das necessidades de segurança dos setores críticos, bem como os novos desafios associados aos incidentes transfronteiriços, incluindo a resposta coordenada às cibercrises.

A Comissão irá:

- apresentar, no primeiro semestre de 2017, um projeto de cooperação para fazer face aos ciberincidentes em grande escala a nível da UE;
- facilitar a criação de uma «plataforma de informação» para apoiar o intercâmbio de informações entre os órgãos da UE e os Estados-Membros;
- criar um Grupo Consultivo de alto nível sobre Cibersegurança; bem como
- concluir a avaliação da ENISA até ao final de 2017. Essa avaliação terá em conta a necessidade de alterar ou de alargar o mandato da ENISA, tendo em vista apresentar uma eventual proposta o mais rapidamente possível.

2.2 Aumentar as atividades de ensino, formação e exercícios no domínio da cibersegurança

Dispor das competências e formação adequadas, tanto quanto à prevenção e ao tratamento dos incidentes de cibersegurança e como da atenuação dos seus impactos, é um dos principais aspetos da resiliência em matéria de cibersegurança.

Atualmente, a ENISA e o Grupo Europeu de Ensino e Formação sobre Cibercriminalidade (ECTEG), em colaboração com o Centro Europeu da Cibercriminalidade da Europol e a Academia Europeia de Polícia (CEPOL), desempenham um papel importante na prestação de apoio à criação de capacidades no domínio da cibersegurança, incluindo sobre ciência forense - através do desenvolvimento de manuais e da organização de ações de formação e de exercícios de cibersegurança.

Ao mesmo tempo, o ciberespaço está a evoluir rapidamente, cabendo às capacidades de dupla utilização um papel essencial. Por conseguinte, é necessário desenvolver a cooperação e as sinergias entre civis e militares através de ações de formação e exercícios, para aumentar a resiliência e as capacidades de resposta da UE a incidentes.

Para responder a esta necessidade, e na sequência da adoção da Diretiva SRI e do Quadro Estratégico da UE para a Ciberdefesa[17], os serviços da Comissão, em cooperação com os Estados-Membros, o Serviço Europeu para a Ação Externa (SEAE), a ENISA e outros organismos relevantes da UE em matéria de cibersegurança[18], será estabelecida uma plataforma de ensino e formação, que promoverá as sinergias entre a formação civil e da Defesa.

A Comissão irá:

- trabalhar em estreita cooperação com os Estados-Membros, a ENISA, o SEAE e outros organismos relevantes da UE para estabelecer uma plataforma de formação em

[17] Adotada pelo Conselho dos Negócios Estrangeiros da União Europeia, de 18 de novembro de 2014, doc. 15585/14.
[18] Como a Academia Europeia de Segurança e Defesa, a EC3, a Academia Europeia de Polícia (CEPOL) e a Agência Europeia de Defesa.

matéria de cibersegurança.

2.3. Abordar as interdependências intersetoriais e a resiliência da infraestrutura de rede pública

Um importante elemento a ter em conta para avaliar o risco e o impacto dos incidentes informáticos em grande escala é o grau de interdependência transfronteiriça e intersetorial. Os incidentes informáticos graves num setor ou num Estado-Membro podem, direta ou indiretamente, afetar - ou propagar-se - a outros setores ou outros Estados-Membros.

A cooperação transfronteiriça e transetorial facilita o intercâmbio de informações e de conhecimentos especializados e, consequentemente, aumenta a capacidade de preparação e resiliência. A Comissão tem vindo a apoiar atividades em diversos setores, a fim de compreender melhor as interdependências, através da aplicação do Programa Europeu para a Proteção das Infraestruturas Críticas[19].

Ao mesmo tempo, um pré-requisito necessário para enfrentar os riscos intersetoriais é a capacidade de cada setor identificar, preparar e responder a ciberincidentes. A Comissão irá avaliar o risco resultante de ciberincidentes nos setores altamente interdependentes dentro e através das fronteiras nacionais, em particular nos setores abrangidos pela Diretiva SRI, tendo igualmente em conta a evolução da situação a nível internacional[20]. Na sequência desta avaliação, a Comissão vai ponderar se são necessárias novas regras e/ou orientações específicas sobre cibersegurança e preparação para os riscos nesses setores críticos.

A nível europeu, os centros setoriais de partilha e análise de informações[21] (ISAC) e as CSIRT correspondentes podem desempenhar um papel fundamental na preparação e resposta a incidentes informáticos. Para assegurar a eficácia dos fluxos de informação sobre novas ameaças e facilitar a resposta aos ciberincidentes, os ISAC devem ser estimulados a colaborar com a rede CSIRT, ao abrigo da Diretiva SRI, e com o Centro Europeu da Cibercriminalidade da Europol, a CERT-UE, bem como com os organismos responsáveis pela aplicação da lei.

O intercâmbio de informações entre as partes interessadas e com as autoridades ao longo do ciclo de vida de riscos requer um clima de confiança entre os participantes, que lhes garanta que não serão responsabilizados. A Comissão registou uma série de preocupações, que impedem as empresas de partilhar informações as com as suas congéneres, entre setores ou com as autoridades e, em especial, transfronteiras. A Comissão procurará abordar e esclarecer estas questões, no interesse de um maior intercâmbio de informações sobre ciberameaças.

Canais de comunicação fiáveis, que garantam a confidencialidade, também são vitais para incentivar as empresas a comunicarem o roubo informático de segredos comerciais. Tal permitiria monitorizar e avaliar os danos sofridos pela indústria europeia (que resultam também na perda de vendas e empregos) e os organismos de investigação. Isto contribuiria igualmente para ajudar a conceber as respostas políticas adequadas. Com o apoio da ENISA,

[19] SWD(2013) 318.
[20] Por exemplo, o roteiro para a cibersegurança adotado pela Agência Europeia para a Segurança da Aviação, os trabalhos da Organização da Aviação Civil Internacional e da Organização Marítima Internacional.
[21] Ver, por exemplo, o ISAC do setor europeu da energia (http://www.ee-isac.eu).

do Instituto da Propriedade Intelectual da União Europeia (EUIPO) e do EC3 da Europol, a Comissão irá - em diálogo com as partes interessadas do setor privado - criar canais de confiança para a comunicação voluntária do roubo informático de segredos comerciais. Desta forma, será possível compilar dados anonimizados e agregados a nível da UE. Estes dados podem ser partilhados com os Estados-Membros para alimentar os esforços diplomáticos e as ações de sensibilização para ajudar a proteger os ativos intangíveis da UE dos ciberataques.

Para apoiar a cibersegurança a nível setorial, a Comissão irá também promover a incorporação da cibersegurança no desenvolvimento de várias políticas setoriais da UE com interesse para a cibersegurança.

Por último, mas não menos importante, as autoridades públicas têm um papel a desempenhar na verificação da integridade das principais infraestruturas da Internet para detetar problemas, informar a parte responsável por estas redes e - sempre que necessário - prestar assistência para solucionar as vulnerabilidades detetadas. As autoridades reguladoras nacionais poderão utilizar as capacidades das CSIRT para analisar regularmente as infraestruturas da rede pública. Nesta base, poderiam incentivar os operadores a colmatar lacunas ou resolver as vulnerabilidades que tais análises venham a identificar.

Por conseguinte, a Comissão irá analisar as condições legais e organizativas necessárias a fim de permitir às autoridades reguladoras nacionais, em cooperação com as autoridades nacionais de cibersegurança, solicitar às CSIRT que realizarem de forma regular controlos da vulnerabilidade das infraestruturas da rede pública. As CSIRT nacionais devem ser incentivadas a cooperar no âmbito da rede CSIRT sobre melhores práticas de monitorização de redes, facilitando assim a prevenção de incidentes em grande escala.

A Comissão irá:

- promover a emergência da cooperação europeia através de centros de partilha e análise de informações setoriais, apoiar a sua colaboração com as CSIRT e procurar eliminar os obstáculos que impedem os participantes no mercado de partilhar informações;
- realizar um estudo dos riscos estratégicos e sistémicos resultantes de ciberincidentes nos setores altamente interdependentes no interior e através das fronteiras nacionais;
- avaliar a necessidade e, se for caso disso, elaborar regras e/ou orientações adicionais sobre a preparação para a cibersegurança em setores críticos;
- criar, com a ENISA, o EUIPO e o EC3 canais fiáveis para a comunicação voluntária do roubo informático de segredos comerciais;
- promover a incorporação de medidas de cibersegurança nas políticas setoriais europeias; bem como
- examinar as condições necessárias para permitir que as autoridades nacionais solicitem às CSIRT a realização de controlos regulares nas principais infraestruturas de rede.

3. DAR RESPOSTA AOS DESAFIOS QUE A EUROPA ENFRENTA EM MATÉRIA DE MERCADO ÚNICO DA CIBERSEGURANÇA

A Europa precisa de produtos e soluções de cibersegurança de elevada qualidade, a preços acessíveis e interoperáveis. No entanto, o fornecimento de produtos e serviços de segurança informática no mercado único continua a estar muito fragmentado do ponto de vista geográfico. Por um lado, esta situação torna difícil para as empresas europeias concorrer a nível nacional, europeu e mundial; por outro, reduz a escolha de tecnologias de cibersegurança viáveis e utilizáveis a que os cidadãos e as empresas têm acesso[22].

Com efeito, o setor da cibersegurança na Europa desenvolveu-se essencialmente com base na procura governamental nacional, incluindo para o setor da defesa. A maioria dos contratantes do setor europeu da defesa criaram departamentos de cibersegurança[23]. Em paralelo, surgiu um grande número de PME inovadoras tanto nos mercados especializados/nichos de mercado (por exemplo, sistemas de cifragem) como em mercados bem estabelecidos, com novos modelos de negócio (por exemplo, software antivírus).

No entanto, as empresas enfrentam dificuldades para crescerem fora do seu mercado nacional. A falta de confiança nas soluções propostas «transfronteiras» é o fator essencial que se destaca, de forma clara, de todas as consultas realizadas pela Comissão[24]. Em consequência, a adjudicação de contratos ainda ocorre num determinado Estado-Membro e muitas empresas lutam para alcançar as economias de escala que lhes permitiriam ser mais competitivas, tanto no mercado interno como a nível mundial.

A falta de soluções interoperáveis (normas técnicas), práticas (regras processuais) e mecanismos de certificação à escala da UE são outras lacunas que afetam o mercado único da cibersegurança. Neste contexto, a cibersegurança foi identificada como uma das prioridades de normalização das TIC para o mercado único digital[25].

As limitadas perspetivas de crescimento para as empresas no mercado único da cibersegurança resultam de um grande número de fusões e aquisições por parte de investidores não europeus[26]. Embora esta tendência demonstre a capacidade de inovação dos empresários europeus em matéria de cibersegurança, também pode conduzir à perda de conhecimentos e competências, e a uma «fuga de cérebros».

É urgente tomar medidas para promover uma maior integração do mercado único dos produtos e serviços de cibersegurança que facilite a aplicação de soluções mais práticas e acessíveis.

O défice de confiança entre os intervenientes institucionais e industriais europeus pode ser ultrapassado através da promoção da cooperação na fase inicial do ciclo de vida da inovação: no âmbito da própria indústria da cibersegurança, entre fornecedores e compradores; e numa

[22] Ver SWD(2016) 216.
[23] Ver SWD(2016) 216.
[24] Ver SWD(2016) 215.
[25] COM(2016) 176/2.
[26] Ver SWD(2016) 216.

dimensão intersetorial, envolvendo as indústrias que já sejam ou se devam tornar-se clientes de soluções de cibersegurança.

Ao mesmo tempo, o desenvolvimento de produtos, serviços e tecnologias de dupla utilização está a ganhar cada vez mais importância na Europa. Um número crescente de soluções está a ser transferido do setor civil para o mercado europeu da defesa[27]. No futuro Plano de ação europeu no domínio da defesa, a Comissão pretende identificar medidas para reforçar as sinergias civis/militares a nível europeu.

3.1 Certificação e rotulagem

A certificação desempenha um papel importante na promoção da confiança e segurança dos produtos e serviços. O mesmo é válido para os novos sistemas baseados nas tecnologias digitais e que exigem um elevado nível de segurança, tais como os automóveis conectados e a saúde eletrónica, os sistemas industriais de automatização e controlo ou as redes inteligentes.

Estão a ser lançadas iniciativas nacionais destinadas a estabelecer requisitos de cibersegurança para componentes informáticos de alto nível para as infraestruturas tradicionais, incluindo requisitos de certificação. Embora sejam importantes, estas iniciativas criam o risco de fragmentação do mercado único e levantam questões de interoperabilidade. Só alguns Estados-Membros dispõem de regimes eficazes de certificação da segurança dos produtos informáticos[28]. Assim, uma empresa informática pode ter de se submeter a vários processos de certificação para poder vender em vários Estados-Membros. Na pior das hipóteses, um produto ou serviço informático destinado a satisfazer necessidades de cibersegurança num Estado-Membro não pode ser colocado no mercado de outro Estado-Membro.

Para se atingir um mercado único da cibersegurança, um eventual quadro de certificação de segurança dos produtos e serviços informáticos deveria ter por objetivo: (i) abranger uma ampla gama de sistemas, produtos e serviços informáticos; (ii) assegurar a sua aplicabilidade nos 28 Estados-Membros; e (iii) incluir qualquer nível de cibersegurança; tendo simultaneamente em conta a evolução a nível internacional.

Para este efeito, a Comissão criará um grupo de trabalho específico sobre a certificação de segurança dos produtos e serviços informáticos, composto por peritos dos Estados-Membros e da indústria. O seu objetivo será desenvolver, em cooperação com a ENISA e o Centro Comum de Investigação, até ao final de 2016, um roteiro que explore a possibilidade de criação de um quadro europeu de certificação de segurança informática, a propor até ao final de 2017. Neste contexto, a Comissão terá igualmente em consideração o Regulamento (CE) n.º 2008/765 e disposições relativas à certificação constantes do Regulamento geral sobre a proteção de dados 2016/679[29]

[27] Em 2013, as exportações de produtos de dupla utilização já representavam cerca de 20 % do total de exportações da UE (em termos de valor). Tal inclui o comércio intra-UE.

[28] Ver em SWD(2016) 216 o Grupo de Altos Funcionários para os sistemas informáticos (Decisão 92/242/CEE do Conselho, de 31 de março de 1992) e outros regimes, como por exemplo a *Commercial Product Assurance* no Reino Unido ou a *Certification Sécuritaire de Premier Niveau* em França.

[29] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, prevê tanto a criação de códigos de conduta destinados a contribuir para a correta aplicação das normas de proteção de dados como de mecanismos de certificação em matéria de proteção de dados, abrangendo todos os princípios, incluindo nomeadamente a segurança do tratamento de dados pessoais.

O processo incluirá uma ampla consulta e avaliação de impacto. Tal permitirá à Comissão estudar diferentes opções para a criação do quadro de certificação dos produtos e serviços informáticos. A Comissão vai igualmente estudar a certificação de segurança informática nos setores das infraestruturas (por exemplo, no domínio da aviação, caminhos de ferro, setor automóvel), e os mecanismos específicos de certificação e validação de tecnologia «pronta a usar» (por exemplo, cibersegurança dos sistemas industriais de automatização e controlo[30], da Internet das coisas ou da computação em nuvem). Abordará também as lacunas identificadas no âmbito do regime europeu de certificação de segurança informática acima referido.

Tanto quanto possível, os esforços de certificação basear-se-ão em normas internacionalmente reconhecidas e serão desenvolvidos com parceiros internacionais.

A Comissão vai igualmente explorar opções sobre a melhor forma de integrar a certificação de segurança informática na futura legislação setorial, também relacionada com aspetos de segurança.

Para além de possíveis opções regulamentares, a Comissão explorará igualmente a criação de um sistema de rotulagem europeu para a segurança dos produtos informáticos, orientado para os aspetos comerciais, voluntário e simples. Destinado a complementar a certificação, este sistema visa aumentar a legibilidade da cibersegurança nos produtos comerciais, de modo a aumentar a sua competitividade no mercado único e a nível mundial. Serão tidas em devida conta as iniciativas horizontais e setoriais em curso lançadas pela indústria, tanto ao nível da oferta como da procura.

As administrações públicas serão estreitamente associadas de modo a permitir a utilização de especificações e referências comuns da certificação no domínio dos contratos públicos. A Comissão irá igualmente acompanhar e elaborar um relatório sobre a utilização de requisitos de certificação relevantes em matéria de contratos públicos, a nível nacional, em particular nos sistemas setoriais (energia, transportes, saúde, administração pública, etc.)

A Comissão irá:

- desenvolver, até ao final de 2016, um roteiro para uma eventual proposta de quadro de certificação de segurança informática, a apresentar até ao final de 2017, e avaliar a viabilidade e o impacto de um quadro europeu de rotulagem de cibersegurança;
- explorar a necessidade e, se for caso disso, colmatar lacunas na certificação de segurança informática no âmbito dos atuais mecanismos setoriais específicos de validação/certificação;
- incluir, quando adequado, a integração da certificação de segurança dos produtos informáticos nas futuras propostas legislativas setoriais;
- estimular a participação das administrações públicas para facilitar a utilização de sistemas de certificação e de especificações comuns na contração pública; bem como
- acompanhar a utilização dos requisitos de certificação nos contratos públicos e

[30] Ver grupo temático da ERNCIP sobre «Cibersegurança dos sistemas industriais de controlo», disponível em https://erncip-project.jrc.ec.europa.eu/download-area/category/16-case-studies-for-industrial-automation-and-control-systems.

privados e elaborar um relatório sobre a situação do mercado no prazo de três anos.

3.2. Reforçar o investimento em cibersegurança na Europa e apoiar as PME

Embora a inovação em matéria de cibersegurança seja setor em grande crescimento na Europa, ainda não existe na UE uma cultura de investimento em matéria de cibersegurança. Existem muitas PME inovadoras neste domínio mas, muitas vezes, estas são incapazes de prosseguir as suas operações. Tal deve-se, nomeadamente, à falta de financiamento disponível para as apoiar nas fases iniciais de desenvolvimento. As empresas também têm um acesso limitado ao capital de risco na Europa e o seu orçamento disponível para marketing destinado a melhorar a sua visibilidade, ou para lidar com diferentes conjuntos de requisitos de normalização e conformidade, não é adequado.

Ao mesmo tempo, a cooperação entre os intervenientes da cibersegurança é bastante desigual e são necessários esforços suplementares para aumentar a concentração económica e desenvolver novas cadeias de valor[31].

Para aumentar o investimento em cibersegurança na Europa e apoiar as PME, é necessário facilitar o acesso ao financiamento. Deve ser igualmente apoiado o desenvolvimento de aglomerados industriais (*clusters*) de cibersegurança competitivos a nível mundial e de centros de excelência em ecossistemas regionais favoráveis ao crescimento digital. Esse apoio deve estar associado à execução de estratégias de especialização inteligente e de outros instrumentos da UE, para que a indústria europeia de cibersegurança tire o melhor partido dessas oportunidades.

A abordagem da Comissão será aumentar a sensibilização da comunidade da cibersegurança para as oportunidades de financiamento a nível europeu, nacional e regional (tanto relativas aos instrumentos horizontais como a concursos específicos[32]), mediante a utilização dos instrumentos e canais existentes, por exemplo, a rede europeia de empresas.

A Comissão complementará estes esforços avaliando com o Banco Europeu de Investimento (BEI) e o Fundo Europeu de Investimento (FEI) formas de facilitar o acesso ao financiamento. Tal pode assumir a forma de investimentos em capitais próprios ou quase-capital, empréstimos, garantias para projetos ou contragarantias para intermediários, por exemplo, através da criação de uma plataforma de investimento em cibersegurança no âmbito do Fundo Europeu para Investimentos Estratégicos[33].

Além disso, a Comissão irá também analisar a possibilidade de desenvolver, com os Estados-Membros e as regiões interessadas, uma plataforma de especialização inteligente para a cibersegurança[34]. Tal contribuiria para coordenar e planificar estratégias de cibersegurança e

[31] Ver SWD(2016) 216.

[32] Ver, por exemplo, o convite multissetorial à apresentação de propostas de 2016 no âmbito do programa «Mecanismo Interligar a Europa», e os convites à apresentação de propostas COSMO 2016 relativos ao Programa de Internacionalização de Clusters.

[33] No âmbito do Fundo Europeu para Investimentos Estratégicos, os projetos individuais podem ser financiados, direta ou indiretamente, através de plataformas de investimento. Essas plataformas de investimento podem contribuir para financiar projetos de menor dimensão e reunir fundos provenientes de diferentes fontes para permitir investimentos diversificados segundo um critério temático ou geográfico.

[34] Ver instrumentos de especialização inteligente (RIS3): http://s3platform.jrc.ec.europa.eu/.

estabelecer uma colaboração estratégica das partes interessadas nos ecossistemas regionais. Esta abordagem deverá também contribuir para mobilizar o potencial dos Fundos Europeus Estruturais e de Investimento para o setor de cibersegurança.

De um modo mais geral, a Comissão irá promover uma abordagem de segurança de raiz. A Comissão procurará garantir que os requisitos de cibersegurança são sistematicamente abordados em todos os grandes investimentos em infraestruturas que tenham uma componente digital e que sejam cofinanciados pelos fundos europeus. Para tal, irá introduzir gradualmente os requisitos relevantes em matéria de contratos públicos e das regras dos programas.

A Comissão irá:

- utilizar os instrumentos de apoio às PME, a fim de sensibilizar a comunidade da cibersegurança para os mecanismos de financiamento existentes;
- reforçar a utilização de ferramentas e instrumentos da UE de apoio às PME inovadoras, explorando as sinergias entre os mercados da cibersegurança civil e de defesa[35];
- explorar, juntamente com o BEI e o FEI, a viabilidade de facilitar o acesso ao investimento, por exemplo, através de uma plataforma de investimento em cibersegurança ou de outros instrumentos;
- desenvolver uma plataforma de especialização inteligente para a cibersegurança, com vista a ajudar os Estados-Membros e as regiões interessadas a investir no setor da cibersegurança (RIS3); bem como
- promover uma abordagem de segurança de raiz para os grandes investimentos em infraestruturas que tenham uma componente digital e sejam cofinanciados por fundos da UE.

4. ESTIMULAR E REFORÇAR A INDÚSTRIA EUROPEIA DA CIBERSEGURANÇA ATRAVÉS DA INOVAÇÃO — CRIAÇÃO DA PPPC PARA A CIBERSEGURANÇA

Para estimular a competitividade e a inovação da indústria da cibersegurança europeia, será criada uma parceria público-privada contratual (PPPc) para a cibersegurança. A PPPc reunirá recursos da indústria e públicos para atingir a excelência na investigação e na inovação.

A PPPc visa reforçar a confiança entre os Estados-Membros e fomentar a cooperação industrial na fase inicial do processo de investigação e de inovação. Visa também contribuir para alinhar os setores da procura e da oferta. Tal deverá permitir que a indústria conheça as exigências futuras dos utilizadores finais e dos setores que são consumidores importantes de soluções de cibersegurança (por exemplo, energia, saúde, transportes, financeiro). Tal

[35] Por exemplo, a rede europeia de empresas e a rede europeia de regiões ligadas à defesa proporcionará novas oportunidades para as regiões explorarem a cooperação transfronteiras no domínio da dupla utilização, incluindo no domínio da cibersegurança, e para as PME participarem nessas atividades.

facilitará o seu envolvimento na definição comum dos requisitos de segurança digital e de proteção da privacidade e dos dados nos respetivos setores.

A PPPc para a cibersegurança ajudará também a maximizar a utilização dos fundos disponíveis. Este objetivo será alcançado, em primeiro lugar, através de uma maior coordenação com os Estados-Membros. Em segundo lugar, haverá uma melhor concentração num pequeno número de prioridades técnicas, para ajudar a indústria a obter novos avanços tecnológicos e a dominar as tecnologias futuras em matéria de cibersegurança. Neste contexto, o desenvolvimento de software de fonte aberta e normas abertas pode contribuir para fomentar a confiança, a transparência e a inovação disruptiva, devendo, por conseguinte, fazer também parte dos investimentos realizados pela PPPc.

O trabalho realizado no âmbito da PPPc para a cibersegurança deverá igualmente beneficiar de sinergias com outros projetos europeus, nomeadamente quando estes abordam aspetos de segurança. Estas incluem as PPP relativas às fábricas do futuro, edifícios eficientes do ponto de vista energético, 5G e grandes volumes de dado[36]s e outras PPP setoriais[37], bem como a iniciativa para a Internet das coisas[38]. Além disso, será promovido um estreito alinhamento com a Nuvem Europeia para a Ciência Aberta e a iniciativa de supercomputação europeia para as cibertecnologias quânticas (por exemplo, inovação na distribuição de chaves quânticas, investigação sobre computação quântica).

A PPPc para a cibersegurança é lançada no âmbito do programa Horizonte 2020[39], o programa-quadro da UE de investigação e inovação para o período 2014-2020. Irá dinamizar o financiamento dos dois pilares do programa: «Liderança em tecnologias facilitadoras e industriais» e «Desafios societais - sociedades seguras». O orçamento total da PPPc ascenderá a 450 milhões de euros com um triplo efeito de alavanca do lado da indústria. A cibersegurança também deve ser aplicada e coordenada com outras partes do programa Horizonte 2020 (por exemplo, a energia, os transportes e a saúde, os desafios societais e a excelência no contexto do Programa-Quadro Horizonte 2020). Tal contribuirá para os objetivos da PPPc em matéria de cibersegurança. Esta coordenação deve igualmente ser assegurada logo na fase de conceção de estratégias setoriais.

A PPPc será executada de forma transparente, com uma governação aberta e flexível adaptada ao contexto em rápida evolução da cibersegurança. A Comissão terá em consideração a necessidade dos Estados-Membros debaterem a forma como a evolução das tecnologias afeta o funcionamento seguro das infraestruturas nacionais e transfronteiras. Do mesmo modo, os resultados da parceria devem ser sustentáveis ao longo de vários anos, para garantir que os seus objetivos possam ser atingidos.

A PPPc será apoiada pela Organização Europeia de Cibersegurança (ECSO), cuja composição deverá refletir a diversidade do mercado da cibersegurança na Europa. Incluirá também administrações públicas nacionais, regionais e locais, centros de investigação, universidades e outras partes interessadas.

[36] A parceria público-privada para a infraestrutura 5G e a parceria público-privada para os grandes volumes de dados.
[37] O SESAR ou a parceria público-privada «*Shift to Rail*», por exemplo.
[38] A Aliança para a Inovação da Internet das Coisas (AIIDC).
[39] http://ec.europa.eu/programmes/horizon2020/en/official-documents.

A Comissão irá:

- assinar com a indústria uma Parceria Público-Privada contratual para a Cibersegurança que entrará em atividade no terceiro trimestre de 2016;
- lançar, no primeiro trimestre de 2017, convites à apresentação de propostas no âmbito do programa Horizonte 2020 relacionados com a PPPc para a cibersegurança; bem como
- assegurar a coordenação da PPPc para a cibersegurança com as estratégias setoriais relevantes, os instrumentos do programa Horizonte 2020 e as PPP setoriais.

5. CONCLUSÃO

A presente comunicação apresenta medidas destinadas a reforçar a resiliência do ciberespaço e de promover uma indústria europeia da cibersegurança competitiva e inovadora, tal como anunciado na Estratégia da UE para a Cibersegurança e na Estratégia para o Mercado Único Digital. A Comissão convida o Parlamento Europeu e o Conselho a apoiarem esta abordagem.