COMISSÃO
EUROPEIA

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

Bruxelas, 13.9.2017
JOIN(2017) 450 final

COMUNICAÇÃO CONJUNTA AO PARLAMENTO EUROPEU E AO CONSELHO

Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE

1. INTRODUÇÃO

A cibersegurança é essencial tanto para a prosperidade como para a nossa segurança. Atendendo a que a vida quotidiana e as nossas economias dependem cada vez mais de tecnologias digitais, vamos ficando gradualmente mais expostos. Os incidentes de cibersegurança estão a diversificar-se tanto no que se refere aos responsáveis como aos objetivos que pretendem atingir. As ciberatividades maliciosas ameaçam não apenas as nossas economias e o avanço para o mercado único digital, como também o próprio funcionamento das democracias, as liberdades e os valores que defendemos. A nossa segurança futura depende da transformação da capacidade para protegermos a UE contra ciberameaças: tanto as infraestruturas civis como as capacidades militares dependem da segurança dos sistemas digitais. Este facto foi reconhecido pelo Conselho Europeu de junho de 2017[1], bem como na estratégia global para a política externa e de segurança da União Europeia[2].

Os riscos estão a aumentar exponencialmente. Alguns estudos sugerem que o impacto económico da cibercriminalidade aumentou cinco vezes, entre 2013 e 2017, e poderá ainda quadruplicar até 2019[3]. O recurso ao *software* de sequestro (*ransomware*)[4] registou um aumento considerável, sendo que os recentes ataques[5] refletem um aumento drástico das atividades no âmbito da cibercriminalidade. No entanto, o *software* de sequestro está longe de ser a única ameaça.

As ciberameaças surgem de intervenientes estatais e não estatais: são frequentemente de origem criminosa, motivadas pelo lucro, mas também podem ser de natureza política e estratégica. A ameaça criminosa é reforçada pela definição pouco clara do limite entre a cibercriminalidade e o crime «tradicional», uma vez que os criminosos utilizam a Internet quer como uma forma de intensificarem as suas atividades, quer como uma fonte para encontrarem novos métodos e ferramentas para a prática de crimes[6]. Contudo, na grande maioria dos casos, as hipóteses de localizar os criminosos são muito escassas e as de instaurar uma ação penal são ainda mais reduzidas.

Ao mesmo tempo, os intervenientes estatais cumprem cada vez mais os seus objetivos geopolíticos não só por intermédio de instrumentos tradicionais, como a força militar, mas também de instrumentos digitais mais discretos, inclusive interferindo em processos democráticos internos. A utilização do ciberespaço como um campo de batalha, isoladamente ou no âmbito de uma abordagem híbrida, é agora amplamente reconhecida. As campanhas de desinformação, as notícias falsas e as ciberoperações destinadas a atingir infraestruturas críticas são cada vez mais comuns e exigem uma resposta. Por esta razão, a Comissão sublinhou, no seu documento de reflexão sobre o futuro da defesa europeia[7], a importância da cooperação em matéria de ciberdefesa.

---

1 http://www.consilium.europa.eu/en/press/press-releases/2017/06/23-euco-conclusions/.

2 http://europa.eu/globalstrategy/.

3 Ver, por exemplo, o estudo da McAfee e do Centre for Strategic and International Studies (Centro de Estudos Estratégicos e Internacionais), intitulado «Net Losses: Estimating the Global Cost of Cybercrime», 2014.

4 O *software* de sequestro é um tipo de programa malicioso *(malware)* que impede ou restringe o acesso dos utilizadores ao respetivo sistema, seja pelo bloqueio do ecrã do sistema seja pelo bloqueio dos ficheiros dos utilizadores, a não ser que estes paguem um resgate.

5 Em maio de 2017, o ataque com recurso ao *software* de sequestro Wannacry afetou mais de 400 000 computadores de mais de 150 países. Um mês depois, o ataque com recurso ao *software* de sequestro Petya atingiu a Ucrânia e diversas empresas em todo o mundo.

6 Avaliação da Ameaça da Criminalidade Grave e Organizada, Europol, 2017.

7 https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_en.pdf.

Se não melhorarmos substancialmente a nossa cibersegurança, o risco aumentará a par com a transformação digital. Até 2020, espera-se que dezenas de milhares de milhões de dispositivos venham a estar ligados à Internet no âmbito da «Internet das coisas», mas a cibersegurança ainda não constitui uma prioridade na sua conceção[8]. A incapacidade de proteger os dispositivos que controlarão as nossas redes de energia, automóveis e redes de transportes, fábricas, finanças, hospitais e lares poderá ter consequências devastadoras e causar enormes danos à confiança dos consumidores nas tecnologias emergentes. O risco de ataques de natureza política contra alvos civis e de falhas na ciberdefesa militar agrava ainda mais esse perigo.

A abordagem definida na presente comunicação conjunta dará à UE melhores condições para fazer face às referidas ameaças. Permitirá criar uma maior resiliência e autonomia estratégica, aumentando as capacidades em termos de tecnologia e de competências, e contribuindo para criar um mercado único forte. Para tal, é necessário dispor das infraestruturas adequadas para criar uma cibersegurança sólida e reagir sempre que necessário, com a plena participação de todos os intervenientes principais. A abordagem contribuirá também para dissuadir o mais possível os ciberataques, por via da intensificação dos esforços no sentido de detetar, localizar e levar à justiça os responsáveis. Reconhecerá igualmente a dimensão global do problema, desenvolvendo a cooperação internacional como uma plataforma para a liderança da UE em matéria de cibersegurança. Estas medidas baseiam-se nas abordagens do mercado único digital, da estratégia global, da Agenda Europeia para a Segurança[9], do quadro comum em matéria de luta contra as ameaças híbridas[10] e na comunicação «Lançar o Fundo Europeu de Defesa»[11][12].

A UE está já a trabalhar em várias destas questões: é agora tempo de conjugar as diversas vertentes de trabalho. Em 2013, a UE definiu uma estratégia para a cibersegurança, lançando um conjunto de vertentes de trabalho essenciais para melhorar a ciber-resiliência[13]. Os principais objetivos e princípios da estratégia, que são fomentar um ciberecossistema fiável, seguro e aberto, permanecem válidos. Mas o cenário de ameaças em constante evolução e agravamento requer novas medidas para resistir e impedir ataques no futuro[14].

A UE está bem posicionada para abordar as questões da cibersegurança, dado o âmbito das suas políticas e os instrumentos, estruturas e capacidades à sua disposição. Embora os Estados-Membros continuem a ser responsáveis pela segurança nacional, a escala e a natureza transfronteiriça da ameaça constituem um forte argumento a favor da ação da UE no sentido de proporcionar incentivos e apoio aos Estados-Membros para que desenvolvam e mantenham mais e melhores capacidades nacionais em matéria de cibersegurança, reforçando ao mesmo tempo as capacidades a nível da UE. Esta abordagem destina-se a mobilizar todos os intervenientes, ou seja, a UE, os Estados-Membros, a indústria e os cidadãos, para que deem à

---

8 «SMART 2013/0037 Cloud and IoT combination», IDC and TXT Solutions, 2014, estudo encomendado pela Comissão Europeia.

9 COM(2015) 185 final.

10 JOIN(2016) 18 final.

11 COM(2017) 295.

12 A abordagem fundamenta-se igualmente em pareceres científicos independentes fornecidos pelo Grupo de Alto Nível de Conselheiros Científicos no âmbito do Mecanismo de Aconselhamento Científico da Comissão Europeia (para referências, ver *infra*).

13 JOIN(2013) 1 final. Uma avaliação desta estratégia encontra-se disponível no documento de trabalho SWD(2017) 295.

14 Salvo indicação em contrário, as propostas apresentadas na presente comunicação são neutras do ponto de vista orçamental. Qualquer iniciativa com incidência orçamental seguirá devidamente o processo orçamental anual e não poderá prejudicar o próximo quadro financeiro plurianual pós-2020.

cibersegurança a prioridade necessária para criar resiliência e proporcionar uma melhor resposta da UE aos ciberataques. Traduzir-se-á em medidas concretas para ajudar a detetar e investigar qualquer tipo de ciberincidente contra a UE e os seus Estados-Membros e a responder de forma adequada, nomeadamente agindo judicialmente contra os criminosos. A abordagem contribuirá para que a ação externa da UE promova eficazmente a cibersegurança a nível mundial. O resultado será uma mudança de atitude por parte da UE, de uma política reativa para uma abordagem pró-ativa, a fim de proteger a prosperidade, a sociedade e os valores europeus, bem como os direitos e liberdades fundamentais, mediante a resposta às ameaças, atuais e futuras.

2. DESENVOLVER A RESILIÊNCIA DA UE AOS CIBERATAQUES

Uma ciber-resiliência forte requer uma abordagem coletiva e global. Para tal, são precisas estruturas mais robustas e eficazes para promover a cibersegurança e responder aos ciberataques nos Estados-Membros, mas também nas próprias instituições, agências e organismos da UE. Para reforçar a ciber-resiliência e a autonomia estratégica, é igualmente necessária uma abordagem transversal mais abrangente, aliada a um mercado único forte, avanços importantes na capacidade tecnológica da UE e um número muito maior de peritos qualificados. No cerne desta questão está uma aceitação mais generalizada de que a cibersegurança é um desafio comum da sociedade, para que seja possível contar com o envolvimento de vários níveis da administração pública, da economia e da sociedade.

2.1 Reforçar a Agência da União Europeia para a Segurança das Redes e da Informação

A **Agência da União Europeia para a Segurança das Redes e da Informação** (ENISA) tem um papel fundamental a desempenhar no reforço da ciber-resiliência e da capacidade de resposta da UE, mas está limitada pelo seu atual mandato. Por conseguinte, a Comissão apresenta uma proposta de reforma ambiciosa, que inclui um **mandato permanente para a Agência**[15]. Esse mandato irá assegurar a possibilidade de a ENISA prestar apoio aos Estados-Membros, bem como às instituições da UE e a empresas em domínios fundamentais, incluindo na aplicação da Diretiva relativa à segurança das redes e da informação[16] («Diretiva SRI») e do quadro de certificação da cibersegurança proposto.

Após a reformulação, a Agência assumirá uma função importante de aconselhamento no que respeita à elaboração e execução de políticas, incluindo a promoção da coerência entre iniciativas setoriais e a Diretiva SRI e o apoio à criação de centros de partilha e análise de informações em setores essenciais. A ENISA elevará a fasquia e reforçará o estado de preparação da Europa, mediante a organização anual de exercícios pan-europeus de cibersegurança que combinem diferentes níveis de resposta. Apoiará também o desenvolvimento de políticas da UE no que respeita à certificação de tecnologias da informação e das comunicações (TIC) em matéria de cibersegurança, e assumirá um papel importante no reforço não só da cooperação operacional como também da gestão de crises em toda a UE. A agência funcionará igualmente como um ponto de contacto para o intercâmbio de informações e de conhecimentos entre a comunidade da cibersegurança.

[15] COM(2017) 477.

[16] Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

A perceção rápida e o entendimento comum de ameaças e incidentes à medida que se vão desenrolando é uma condição prévia para decidir sobre a necessidade de adotar medidas conjuntas de atenuação ou de resposta apoiadas pela UE. Essa troca de informações exige o envolvimento de todos os agentes pertinentes, ou seja, dos organismos e agências da UE, bem como dos Estados-Membros, a nível técnico, operacional e estratégico. A ENISA, em cooperação com os organismos competentes a nível dos Estados-Membros e da UE, nomeadamente a rede de equipas de resposta a incidentes de segurança informática[17], a CERT-UE, a Europol e o Centro de Situação e de Informações da UE (INTCEN), contribuirá também para o conhecimento da situação a nível da UE. Este conhecimento pode ser incorporado na elaboração de políticas e nas informações sobre ameaças, no âmbito do acompanhamento regular do cenário de ameaças e da cooperação operacional efetiva, bem como na resposta a incidentes transfronteiriços em grande escala.

2.2 Rumo a um mercado único da cibersegurança

O crescimento do mercado da cibersegurança na UE, em termos de produtos, serviços e processos, é dificultado de várias formas. Um aspeto fundamental é a inexistência de sistemas de certificação da cibersegurança reconhecidos em toda a UE que permitam criar normas de resiliência mais exigentes para os produtos e fomentar a confiança do mercado à escala da UE. Por conseguinte, a Comissão apresenta uma proposta para a criação de **um quadro de certificação da cibersegurança a nível da UE**[18]. Este quadro estabelecerá o procedimento para a criação de sistemas de certificação da cibersegurança à escala da UE, abrangendo produtos, serviços e/ou sistemas, que adaptem o nível de garantia à utilização em causa (quer se trate de infraestruturas críticas, quer de dispositivos para consumidores)[19]. O novo quadro proporcionará benefícios claros para as empresas que operam no comércio transfronteiras, que deixarão de ter de passar por vários processos de certificação, reduzindo dessa forma custos administrativos e financeiros. O recurso a sistemas desenvolvidos no âmbito do presente quadro contribuirá também para reforçar a confiança dos consumidores, facultando certificados de conformidade para informar e tranquilizar os compradores e utilizadores sobre as características de segurança dos produtos e serviços que compram e utilizam. Assim, estes padrões elevados de cibersegurança deverão constituir uma fonte de vantagem concorrencial. Daqui resultará uma maior resiliência, já que os produtos e serviços de TIC serão sujeitos a uma avaliação oficial, de acordo com um conjunto definido de normas de cibersegurança, que poderão ser desenvolvidas em estreita ligação com os trabalhos mais amplos em curso relativos às normas no domínio das TIC[20].

Os sistemas previstos no quadro serão facultativos e não imporão quaisquer obrigações regulamentares imediatas aos vendedores ou prestadores de serviços. Os sistemas não estão em contradição com os requisitos legais aplicáveis, como, por exemplo, a legislação da UE em matéria de proteção de dados.

Uma vez estabelecido o quadro, a Comissão convidará as partes interessadas a concentrarem-se em três domínios prioritários:

[17] Tal como previsto no artigo 9.º da Diretiva SRI.
[18] COM(2017) 477.
[19] O nível de garantia indica o grau de rigor da avaliação da segurança, e é geralmente adequado ao nível de risco associado a estes domínios de aplicação ou funções (ou seja, exige-se um nível de garantia mais elevado para produtos ou serviços de TIC utilizados em domínios de aplicação ou funções de alto risco).
[20] COM(2016) 176.

- Segurança em aplicações essenciais ou de alto risco[21]: os sistemas dos quais dependemos nas atividades quotidianas, dos automóveis aos equipamentos industriais, dos sistemas de grande dimensão, como os aviões ou as centrais elétricas, aos mais diminutos, como os dispositivos médicos, são cada vez mais digitais e interligados. Por conseguinte, os componentes essenciais de TIC utilizados em tais produtos e sistemas exigirão uma avaliação rigorosa em termos de segurança.

- Cibersegurança de produtos, redes, sistemas e serviços digitais instalados em larga escala, utilizados tanto pelo setor público como pelo privado para a defesa contra ataques e para a aplicação de obrigações regulamentares[22], tais como sistemas de cifragem de correio eletrónico, barreiras de segurança (*firewalls*) e redes privadas virtuais; é fundamental que o uso generalizado dessas ferramentas não conduza a novas fontes de risco ou a novas vulnerabilidades.

- Utilização de métodos de «segurança desde a conceção» em dispositivos digitais interligados, de baixo custo, destinados ao grande consumo, que constituem a chamada «Internet das coisas»: os sistemas ao abrigo do quadro poderão ser utilizados para indicar que os produtos são fabricados seguindo os métodos de desenvolvimento mais modernos e seguros, que foram sujeitos a testes de segurança adequados e que os vendedores se comprometeram a atualizar os respetivos suportes lógicos (*software*) no caso de descoberta de novas ameaças ou vulnerabilidades.

Estas prioridades devem ter em conta, em especial, a evolução do cenário de ameaças de ciberataques, bem como a importância de serviços essenciais como os transportes, a energia, a saúde, os serviços bancários, as infraestruturas do mercado financeiro, a água potável ou as infraestruturas digitais[23].

Embora nenhum produto, sistema ou serviço de TIC possa ser garantidamente seguro na sua totalidade, existem vários defeitos bem conhecidos e documentados a nível da conceção dos produtos de TIC que podem ser aproveitados para ataques. A adoção de uma abordagem de «segurança desde a conceção» por parte dos produtores de dispositivos conectados, suportes lógicos e equipamentos informáticos permitiria garantir que a cibersegurança é tida em conta antes da comercialização de novos produtos. Este aspeto pode inserir-se no «dever de diligência», a desenvolver de forma mais aprofundada juntamente com a indústria, contribuindo para reduzir as vulnerabilidades de produtos ou suportes lógicos, mediante a aplicação de um conjunto de métodos, desde a fase de conceção à fase de ensaios e verificação, incluindo a verificação formal, se for caso disso, a manutenção a longo prazo e a utilização de processos de desenvolvimento seguros com base no ciclo de vida útil, bem como o desenvolvimento de atualizações e correções para dar resposta a vulnerabilidades não detetadas previamente e permitir a sua rápida atualização e reparação[24]. Além disso, contribuiria para aumentar a confiança dos consumidores nos produtos digitais.

---

[21] Exceto nos casos em que a certificação obrigatória ou voluntária se rege por outros atos da União.

[22] Por exemplo, a Diretiva (UE) 2016/1148, o Regulamento (UE) 2016/679, a Diretiva (UE) 2015/2366 e outras propostas de atos legislativos, como o Código Europeu das Comunicações Eletrónicas, estipulam que as organizações devem pôr em prática medidas de segurança adequadas para enfrentar riscos de cibersegurança relevantes.

[23] Os setores abrangidos pelo âmbito de aplicação da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

[24] Cibersegurança no âmbito do mercado único digital europeu, Grupo de Alto Nível de Conselheiros Científicos, março de 2017.

Importa também reconhecer o papel fundamental das investigações em matéria de segurança realizadas por terceiros, no que se refere à descoberta de vulnerabilidades em produtos e serviços existentes, e criar condições que permitam a divulgação concertada de vulnerabilidades[25] em todos os Estados-Membros, com base nas melhores práticas[26] e nas normas pertinentes[27].

Ao mesmo tempo, há **setores específicos** que enfrentam problemas específicos e que devem ser incentivados a desenvolverem a sua própria abordagem. Desta forma, as estratégias de cibersegurança globais serão complementadas por estratégias de cibersegurança setoriais, em domínios como os serviços financeiros[28], a energia, os transportes e a saúde[29].

A Comissão já identificou as questões específicas relativas à **responsabilidade** suscitadas pelas novas tecnologias digitais[30], estando em curso trabalhos para analisar as suas implicações. As próximas etapas serão concluídas até junho de 2018. A cibersegurança levanta questões relativas à imputação de prejuízos às empresas e cadeias de abastecimento e a incapacidade para resolver estas questões impedirá o desenvolvimento de um mercado único forte de produtos e serviços de cibersegurança.

Por último, o desenvolvimento do mercado único da UE depende também da integração da cibersegurança na política de comércio e investimento. Os efeitos das aquisições por estrangeiros nas tecnologias críticas, de que a cibersegurança é um exemplo importante, são um aspeto fundamental no âmbito da **verificação do investimento direto estrangeiro na União Europeia**[31], que visa permitir a verificação de investimentos provenientes de países terceiros com base em motivos de segurança e de ordem pública. Do mesmo modo, os requisitos de cibersegurança já criaram entraves ao comércio de bens e serviços da UE em setores importantes de diversas economias de países terceiros. O quadro de certificação da cibersegurança a nível da UE reforçará a posição da Europa no plano internacional e deve ser complementado por esforços continuados no sentido do desenvolvimento de normas de alta segurança à escala mundial e de acordos de reconhecimento mútuo.

2.3 Aplicação, na íntegra, da Diretiva relativa à segurança das redes e da informação

Atendendo a que os principais instrumentos para garantir a cibersegurança funcionam atualmente a nível nacional, a UE reconheceu a necessidade de elevar o nível das normas. Os incidentes de cibersegurança em larga escala raramente afetam apenas um Estado-Membro, devido à natureza cada vez mais globalizada, interligada e dependente do digital de setores fundamentais como a atividade bancária, a energia ou os transportes.

---

[25] A divulgação concertada de vulnerabilidades é uma forma de cooperação que facilita e permite aos investigadores no domínio da segurança comunicarem as vulnerabilidades de segurança ao proprietário ou vendedor do sistema de informação, dando à organização a oportunidade de diagnosticar e corrigir as vulnerabilidades, de forma correta e atempada, antes de serem divulgadas informações pormenorizadas a terceiros ou ao público a esse respeito.

[26] Por exemplo, *Good Practice Guide on Vulnerability Disclosure*. *From challenges to recommendations*, ENISA, 2016.

[27] ISO/IEC 29147:2014, Tecnologias da informação — Técnicas de segurança — Divulgação de vulnerabilidades.

[28] Os futuros trabalhos da Comissão sobre tecnologia financeira contemplarão a cibersegurança no setor financeiro.

[29] No setor da energia, por exemplo, combinar tecnologias da informação muito antigas e tecnologias de ponta, nomeadamente com as necessidades em tempo real da rede de energia.

[30] COM(2017) 228.

[31] COM(2017) 478.

A Diretiva relativa à segurança das redes e da informação («Diretiva SRI») é o primeiro ato legislativo a nível da UE em matéria de cibersegurança[32]. Destina-se a reforçar a resiliência melhorando as capacidades nacionais em matéria de cibersegurança, promovendo uma melhor cooperação entre os Estados-Membros e obrigando as empresas de setores económicos importantes a adotarem práticas eficazes de gestão dos riscos e a comunicarem incidentes graves às autoridades nacionais. Estas obrigações também se aplicam a três tipos de prestadores de serviços essenciais da Internet: computação em nuvem, motores de pesquisa e mercados em linha. A diretiva visa uma abordagem mais sólida e mais sistemática e um melhor fluxo de informação.

A aplicação integral da diretiva por todos os Estados-Membros, até maio de 2018, é essencial para a ciber-resiliência da UE. O processo está a ser apoiado pelo trabalho coletivo dos Estados-Membros, do qual resultarão, no outono de 2017, diretrizes destinadas a apoiar uma aplicação mais harmonizada, nomeadamente no que respeita aos operadores de serviços essenciais. A Comissão emite igualmente uma comunicação[33], como parte do presente pacote de cibersegurança, para apoiar os esforços dos Estados-Membros mediante a disponibilização das suas melhores práticas pertinentes para a aplicação da diretiva e de orientações sobre a forma como a diretiva deve funcionar na prática.

Uma área em que a diretiva deverá ser completada é o fluxo de informação. Por exemplo, a diretiva apenas abrange setores estratégicos fundamentais, mas, como é lógico, seria necessária uma abordagem semelhante por parte de todos os intervenientes afetados por ciberataques para permitir uma avaliação sistemática das vulnerabilidades e dos pontos de entrada dos autores desses ataques. Além disso, a cooperação e a partilha de informações entre os setores público e privado enfrentam uma série de obstáculos. Os governos e as autoridades públicas mostram relutância em partilhar informações relevantes em matéria de cibersegurança, por receio de comprometerem a segurança nacional ou a competitividade. As empresas privadas sentem relutância em partilhar informações sobre as suas vulnerabilidades a ciberataques e prejuízos daí resultantes, por receio de comprometerem informações comerciais sensíveis, porem em risco a sua reputação ou violarem as regras de proteção de dados[34]. É necessário reforçar a confiança a fim de promover parcerias público-privadas que apoiem a cooperação mais vasta e a partilha de informações entre um maior número de setores. O papel dos centros de partilha e análise de informações é particularmente importante na criação das relações de confiança necessárias para a partilha de informações entre os setores público e privado. Foram dados alguns passos iniciais no que respeita a determinados setores críticos como a aviação, com a criação do Centro Europeu para a Cibersegurança da Aviação[35], e a energia, com o desenvolvimento de centros de partilha e análise de informações[36]. A Comissão contribuirá na íntegra para esta abordagem, com o apoio da

---

[32] Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

[33] COM(2017) 476.

[34] Cibersegurança no âmbito do mercado único digital europeu, Grupo de Alto Nível de Conselheiros Científicos, março de 2017. Os segredos comerciais constituem uma questão específica, sendo que a comunicação de julho de 2016, intitulada «Reforçar o sistema de ciber-resiliência da Europa e promover uma indústria de cibersegurança competitiva e inovadora», regista a relutância em comunicar o roubo informático de segredos comerciais e a importância de canais de comunicação fiáveis, que garantam a confidencialidade.

[35] https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa.

[36] Tratam-se de organizações sem fins lucrativos, dirigidas pelos respetivos membros, constituídas por entidades públicas e privadas para fins de partilha de informações sobre ciberameaças, riscos, prevenção, atenuação e resposta. Ver, por exemplo, os centros europeus de partilha e análise de informações sobre energia (http://www.ee-isac.eu).

ENISA e com a celeridade necessária, em especial no que diz respeito aos setores que prestam serviços essenciais, identificados na Diretiva SRI.

2.4 A resiliência mediante a rápida resposta a emergências

Na ocorrência de um ciberataque, uma resposta rápida e eficaz pode atenuar o seu impacto. Essa capacidade de resposta pode igualmente demonstrar que as autoridades públicas não permanecem impotentes face a ciberataques, contribuindo para a criação de confiança. No que diz respeito à resposta das instituições da UE, numa primeira fase, os aspetos de cibersegurança devem ser integrados nos atuais mecanismos de gestão de crises da UE: o Mecanismo Integrado de Resposta Política a Situações de Crise, coordenado pela Presidência do Conselho[37], e os sistemas gerais de alerta rápido[38]. A necessidade de reagir a um incidente de cibersegurança ou ciberataque particularmente grave pode constituir uma razão suficiente para que um Estado-Membro invoque a cláusula de solidariedade da União[39].

Uma resposta rápida e eficaz assenta também num mecanismo célere de intercâmbio de informações entre os principais intervenientes a nível nacional e da UE, o que, por sua vez, exige clareza sobre as respetivas competências e responsabilidades. A Comissão consultou as instituições e os Estados-Membros sobre um «plano de ação» destinado a proporcionar um processo eficaz de resposta operacional, a nível da União e dos Estados-Membros, a ciberincidentes em grande escala. O **plano**, apresentado numa recomendação[40] que faz parte do presente pacote, explica como a cibersegurança é integrada nos atuais mecanismos de gestão de crises a nível da UE e define os objetivos e formas de cooperação entre os Estados-Membros, e entre os Estados-Membros e as instituições, serviços, agências e organismos competentes da UE[41] na resposta a incidentes em grande escala e crises de cibersegurança. A recomendação solicita também aos Estados-Membros e às instituições da UE que estabeleçam um quadro de resposta da UE a crises de cibersegurança, a fim de tornar o plano de ação operacional. O plano será ensaiado regularmente no âmbito de exercícios de gestão de crises de cibersegurança e noutros domínios[42] e, se necessário, será atualizado.

Dado que os incidentes de cibersegurança podem afetar significativamente o funcionamento das economias e o quotidiano dos cidadãos, uma opção seria ponderar a criação de um **Fundo de Resposta de Emergência para a Cibersegurança**, seguindo o exemplo de outros mecanismos de gestão de crises em outros domínios de ação da UE. Tal permitiria que os Estados-Membros procurassem ajuda a nível da UE, durante a ocorrência ou na sequência de um incidente grave, desde que tivessem instaurado um sistema prudente de cibersegurança antes do incidente, nomeadamente por via da aplicação integral da Diretiva SRI e do desenvolvimento de quadros de supervisão e de gestão dos riscos a nível nacional. O referido Fundo, em complemento dos atuais mecanismos de gestão de crises a nível da UE, poderia criar uma capacidade de resposta rápida, numa perspetiva de solidariedade, e financiar ações específicas de resposta de emergência, como a substituição de equipamentos violados ou a

---

37 Este mecanismo permite coordenar respostas ao mais alto nível político, em caso de graves crises transetoriais.

38 Estes permitem a partilha interna de informações e a coordenação em caso de crises multissetoriais emergentes, ou de ameaças previsíveis ou iminentes que exijam uma ação a nível da UE.

39 Ao abrigo do artigo 222.º do Tratado sobre o Funcionamento da União Europeia.

40 C(2017) 6100.

41 Incluindo a Europol, a ENISA, a Equipa de Resposta a Emergências Informáticas para as instituições e agências da UE (CERT-UE) e o Centro de Situação e de Informações da UE (INTCEN).

42 Por exemplo, os realizados pela ENISA: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

utilização de instrumentos de atenuação ou de resposta, com base nas experiências nacionais, à semelhança do Mecanismo de Proteção Civil da UE.

2.5 Rede de competências em matéria de cibersegurança dotada de um Centro Europeu de Investigação e de Competências

As ferramentas tecnológicas de cibersegurança são ativos estratégicos, além de serem tecnologias essenciais para o crescimento no futuro. É do interesse estratégico da UE assegurar que mantém e desenvolve as capacidades fundamentais para garantir a segurança da sua economia, sociedade e democracia digitais, para proteger o material informático e os suportes lógicos de importância crítica e para prestar serviços essenciais de cibersegurança.

A parceria público-privada para a cibersegurança[43], criada em 2016, constituiu um primeiro passo importante, gerando até 1 800 milhões de EUR de investimento até 2020. No entanto, a escala do investimento em curso noutras partes do mundo[44] sugere que a UE precisa de fazer mais, em termos de investimento, e de pôr termo à fragmentação das capacidades, que se encontram disseminadas pelo seu território.

A UE poderá proporcionar um valor acrescentado, tendo em conta o grau de sofisticação da tecnologia de cibersegurança, a dimensão avultada do investimento exigido e a necessidade de encontrar soluções que funcionem em todo o seu território. Com base no trabalho dos Estados-Membros e na parceria público-privada, a etapa seguinte consistirá em reforçar a capacidade da UE em matéria de cibersegurança por intermédio de uma **rede de centros de competências em matéria de cibersegurança**[45] constituída em torno de um **Centro Europeu de Investigação e de Competências em matéria de Cibersegurança**. Esta rede e o respetivo centro estimularão o desenvolvimento e a implantação de tecnologias de cibersegurança e complementarão os esforços no sentido de reforçar as capacidades neste domínio, a nível da UE e a nível nacional. A Comissão procederá a uma avaliação de impacto para analisar as opções disponíveis, incluindo a possibilidade de criar uma empresa comum, com vista a estabelecer esta estrutura em 2018.

Num primeiro momento e para fornecer informações para futura reflexão, a Comissão proporá o lançamento de uma fase-piloto no âmbito do programa Horizonte 2020, para congregar e constituir uma rede de centros nacionais com vista a criar uma nova dinâmica em matéria de competências em cibersegurança e de desenvolvimento tecnológico. Para o efeito, a Comissão tenciona propor um aumento de financiamento a curto prazo no valor de 50 milhões de EUR. Esta atividade complementará o estabelecimento da parceria público-privada para a cibersegurança em curso.

A congregação e a definição dos esforços de investigação serão o núcleo central da rede e o objetivo inicial do Centro. O Centro poderá desempenhar a função de gestor de projetos com capacidades para gerir projetos multinacionais, a fim de apoiar o desenvolvimento de capacidades industriais. Tal permitiria igualmente dar um novo ímpeto à inovação e competitividade da indústria da UE no plano mundial, para desenvolver a próxima geração de tecnologias digitais, incluindo a inteligência artificial, a computação quântica, a tecnologia de cifragem progressiva (*blockchain*) e a identificação digital segura, e para assegurar o acesso

[43] C(2016) 4400 final.

[44] Os EUA investirão 19 000 milhões de USD em cibersegurança só em 2017, um aumento de 35 % em relação a 2016. Casa Branca, Gabinete do Secretário de Imprensa: «Ficha informativa: Plano de ação nacional para a cibersegurança», 9 de fevereiro de 2016.

[45] A rede deverá incluir centros existentes e futuros dedicados à cibersegurança, criados nos Estados-Membros, cujos membros serão, em princípio, organizações e laboratórios de investigação públicos.

das empresas estabelecidas na UE a uma grande quantidade de dados, elementos decisivos para a cibersegurança no futuro. O Centro beneficiará também do trabalho da UE no sentido de reforçar a infraestrutura de computação de alto desempenho: esta é essencial para a análise de grandes quantidades de dados, a cifragem e a decifragem rápida de dados, a verificação de identidades, a simulação de ciberataques, e a análise de material vídeo[46].

A rede de centros de competências poderá também ter capacidades para apoiar a indústria por meio de ensaios e simulações que apoiem a certificação da cibersegurança descrita no ponto 2.2. A participação do Centro em toda a atividade da UE em matéria de cibersegurança deverá assegurar uma permanente atualização dos seus objetivos de acordo com as necessidades. O Centro promoverá normas muito rigorosas relativas à cibersegurança, não só em tecnologia e sistemas de cibersegurança, mas também no desenvolvimento de competências de ponta para profissionais, proporcionando soluções e modelos a aplicar nos esforços nacionais de promoção das competências digitais. Nessa medida, deverá reforçar também as capacidades em matéria de cibersegurança a nível da UE e explorar sinergias, nomeadamente com a ENISA, a CERT-UE, a Europol, o eventual Fundo de Resposta de Emergência para a Cibersegurança e as CSIRT nacionais.

Uma das vertentes específicas do trabalho da rede de competências deverá incidir sobre a falta de capacidades a nível europeu no que respeita à **cripto-análise** de produtos e serviços utilizados pelos cidadãos, pelas empresas e pelos governos, no âmbito do mercado único digital. A cifragem forte constitui a base da segurança dos sistemas de identificação digital, que desempenham um papel crucial na eficácia da cibersegurança[47]; mantém também a segurança da propriedade intelectual dos cidadãos e permite garantir a proteção de direitos fundamentais, como a liberdade de expressão e a proteção de dados pessoais, bem como a segurança do comércio em linha[48].

Visto que os mercados da cibersegurança da sociedade civil e da defesa da UE partilham desafios comuns[49] e tecnologias de dupla utilização que exigem uma estreita colaboração em domínios essenciais, uma segunda fase da rede e do seu centro poderia ser alargada com uma dimensão de ciberdefesa, no pleno respeito das disposições do Tratado relacionadas com a política comum de segurança e defesa. A dimensão de defesa, bem como a sua orientação tecnológica, poderá contribuir para a cooperação entre os Estados-Membros no domínio da ciberdefesa, incluindo a partilha de informações, o conhecimento da situação, o reforço do conhecimento e da coordenação das respostas e o apoio aos Estados-Membros no desenvolvimento de capacidades comuns. Poderá funcionar igualmente como uma plataforma que permita aos Estados-Membros definirem as prioridades para a ciberdefesa da UE, por via da identificação de soluções comuns, da contribuição para o desenvolvimento de estratégias comuns, da simplificação da formação, de exercícios e de ensaios no domínio da ciberdefesa a nível da UE e do apoio a trabalhos relativos a normas e taxinomias em matéria de ciberdefesa, contando com o apoio e o aconselhamento prestado pelo Centro. Para prosseguir as atividades acima referidas, o Centro terá de trabalhar em estreita colaboração e em plena complementaridade com a Agência Europeia de Defesa no domínio da ciberdefesa, bem como

---

[46] COM(2012) 45 final e COM(2016) 178 final.

[47] A Comissão lançará, no âmbito do programa Horizonte 2020, um novo desafio para a atribuição do prémio Horizon, no valor de 4 milhões de EUR, à melhor solução inovadora para métodos de autenticação em linha sem descontinuidades..

[48] Cibersegurança no âmbito do mercado único digital europeu, Grupo de Alto Nível de Conselheiros Científicos, março de 2017.

[49] «Study on synergies between the civilian and the defence cybersecurity markets», Optimity; SMART 2014-0059.

com a ENISA no domínio da ciber-resiliência. Esta dimensão de defesa terá em conta o processo lançado pelo documento de reflexão sobre o futuro da defesa europeia.

O elevado nível de resiliência necessária em matéria de ciberdefesa exige esforços de investigação e tecnologia especificamente orientados. Os projetos ou tecnologias de ciberdefesa desenvolvidos por empresas poderão beneficiar de financiamento do Fundo Europeu de Defesa, quer no que respeita à fase de investigação quer à de desenvolvimento[50]. Neste contexto, podem ser especialmente relevantes algumas áreas específicas, como os sistemas de cifragem baseados em tecnologias quânticas, o conhecimento da situação da cibercriminalidade, os sistemas de controlo biométrico de acesso, os sistemas de deteção de ameaças avançadas persistentes, ou a exploração de dados. A Alta Representante, a Agência Europeia de Defesa e a Comissão apoiarão os Estados-Membros na identificação dos domínios em que projetos de cibersegurança comuns possam ser considerados para efeitos de financiamento pelo Fundo Europeu de Defesa.

2.6 Criar uma sólida base de cibercompetências na UE

Existe uma forte dimensão formativa no que respeita à cibersegurança. A eficácia da cibersegurança depende em grande parte das competências das pessoas em causa. No entanto, prevê-se que o défice de profissionais com competências de cibersegurança para trabalhar no setor privado, na Europa, chegará aos 350 000 até 2022[51]. A formação em cibersegurança deve ser desenvolvida a todos os níveis, da formação regular de mão de obra no domínio da cibersegurança, à formação complementar para todos os especialistas de TIC e a novos currículos específicos em matéria de cibersegurança. Importa criar centros de competências académicas sólidas para satisfazer as necessidades prementes de educação e formação, os quais podem beneficiar de orientações de um Centro Europeu de Investigação e de Competências em matéria de Cibersegurança e da ENISA. O objetivo será que a incorporação dos princípios de segurança desde o início da conceção de produtos e sistemas de TIC passe a ser natural. A educação para a cibersegurança não deve ser limitada aos profissionais de informática, mas deve ser integrada em currículos de outras áreas, como a engenharia, a gestão de empresas ou o direito, bem como em vias de ensino para setores específicos. Por último, os professores e alunos do ensino primário e secundário devem ser sensibilizados para a cibercriminalidade e a cibersegurança aquando da aquisição de competências digitais nas escolas.

A UE, juntamente com os Estados-Membros, deverá igualmente contribuir para este esforço recorrendo ao trabalho da Coligação para a criação de competências e emprego na área digital[52] e pondo em prática, por exemplo, programas de aprendizagem em matéria de cibersegurança para as PME.

2.7 Promover a ciber-higiene e a sensibilização para a cibersegurança

Considerando que cerca de 95 % dos incidentes são alegadamente possibilitados por «algum tipo de erro humano, intencional ou não»[53], verifica-se a existência de uma forte componente humana a este respeito. Por conseguinte, a cibersegurança é da responsabilidade de todos. Isto significa que a atitude dos cidadãos, das empresas e das administrações públicas tem de

[50] O programa europeu de desenvolvimento da indústria de defesa dará, desde já, prioridade a projetos de ciberdefesa, e este será um dos objetos do convite à apresentação de propostas a ser lançado em 2018.

[51] Global Information Security Workforce Study, 2017. O défice a nível mundial é de 1,8 milhões de profissionais.

[52] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.

[53] «Cybersecurity Intelligence Index», IBM, 2014, referido na Securitymagazine.com, em 19 de junho de 2014.

mudar, para assegurar que todos compreendem a ameaça e se munem das ferramentas e das competências necessárias para identificarem rapidamente a situação e se protegerem de forma ativa contra ataques. Os cidadãos devem desenvolver hábitos de ciber-higiene e as empresas e organizações devem adotar programas de cibersegurança adequados baseados nos riscos e proceder periodicamente à sua atualização, de acordo com a evolução do cenário de risco.

A Diretiva SRI não estabelece apenas as responsabilidades dos Estados-Membros quanto ao intercâmbio de informações sobre ciberataques a nível da UE, como põe também em prática estratégias nacionais de cibersegurança devidamente desenvolvidas, e quadros em matéria de segurança das redes e sistemas de informação. As administrações públicas a nível da UE e a nível nacional devem desempenhar um papel de liderança acrescido na prossecução destes esforços.

Em primeiro lugar, os Estados-Membros devem maximizar a disponibilidade de instrumentos de cibersegurança para as empresas e os cidadãos. É necessário, em especial, desenvolver mais esforços para prevenir e atenuar o impacto da cibercriminalidade sobre os utilizadores finais. Um exemplo já existente é o trabalho da Europol com a campanha «NoMoreRansom»[54], criada em cooperação estreita entre as autoridades responsáveis pela aplicação da lei e as empresas de cibersegurança para ajudar os utilizadores a evitarem infeções por *software* de sequestro e a decifrarem dados se forem vítimas de ataques. Esses programas devem ser utilizados para outros tipos de *software* mal intencionado (*malware*) em diferentes domínios, e a UE deve desenvolver um **portal único para reunir todos esses instrumentos num balcão único** que preste aconselhamento aos utilizadores sobre prevenção e deteção de *software* mal intencionado e facilite ligações para os mecanismos de alerta.

Em segundo lugar, os Estados-Membros devem acelerar a **utilização de instrumentos com maior nível de cibersegurança, no âmbito do desenvolvimento da administração pública em linha,** e aproveitar ao máximo a rede de competências. Deve promover-se a adoção de meios de identificação seguros, com base no quadro da UE em matéria de identificação eletrónica e serviços de confiança para transações eletrónicas no mercado interno, em vigor desde 2016 e que proporciona um quadro regulamentar previsível para permitir interações eletrónicas seguras e sem descontinuidades entre as empresas, os cidadãos e as autoridades públicas[55]. Além disso, as instituições públicas, especialmente as que prestam serviços essenciais, devem garantir a formação do seu pessoal em áreas relacionadas com a cibersegurança.

Em terceiro lugar, os Estados-Membros devem estabelecer o ciberconhecimento como uma prioridade **em campanhas de sensibilização**, nomeadamente em ações dirigidas a escolas, a universidades, à comunidade empresarial e a organismos de investigação. O mês da cibersegurança, que tem lugar todos os anos em outubro sob a coordenação da ENISA, será reformulado de modo a alargar o alcance da sua ação de comunicação comum a nível nacional e da UE. A sensibilização para as **campanhas de desinformação e de falsas notícias** nas redes sociais digitais, especificamente destinadas a fragilizar os processos democráticos e os valores europeus, é igualmente importante. Embora a principal responsabilidade continue a ser imputada a nível nacional, incluindo no caso das eleições para o Parlamento Europeu, a

[54] https://www.nomoreransom.org/.

[55] O Regulamento (UE) n.º 910/2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno (regulamento eIDAS), adotado em 23 de julho de 2014. Além disso, a Comissão Europeia está a fornecer módulos e ferramentas para assegurar a interoperabilidade da identificação eletrónica e da assinatura eletrónica (por exemplo, listas de navegadores aprovados) por intermédio do programa do Mecanismo Interligar a Europa.

congregação de conhecimentos e a partilha de experiências a nível europeu revelou-se uma mais-valia ao permitir definir vertentes prioritárias de ação[56].

Existe igualmente um papel importante a desempenhar pela **indústria** em geral, mas com especial atenção para os fabricantes e os prestadores de serviços digitais. É necessário apoiar os utilizadores (particulares, empresas e administrações públicas) por meio de ferramentas que lhes permitam assumir a responsabilidade pelas suas próprias ações em linha, tornando claro que a manutenção da ciber-higiene básica é uma componente indispensável da oferta aos consumidores[57]. Para detetar e eliminar as vulnerabilidades, a indústria deve esforçar-se por dispor de processos internos que assegurem a investigação, triagem e resolução de vulnerabilidades, independentemente de a origem da potencial vulnerabilidade ser externa ou interna à empresa em causa.

Ações-chave

- Aplicação, na íntegra, da diretiva relativa à segurança das redes e da informação;
- Adoção rápida, pelo Parlamento Europeu e pelo Conselho, do regulamento que estabelece um novo mandato para a ENISA e um quadro europeu para a certificação[58];
- Iniciativa conjunta da Comissão e da indústria para definir um princípio de «dever de diligência» a fim de reduzir as vulnerabilidades dos produtos/suportes lógicos e promover a «segurança desde a conceção»;
- Execução rápida do plano de ação para a resposta a incidentes transfronteiriços em grande escala;
- Avaliação de impacto para estudar a possibilidade de uma proposta da Comissão, em 2018, para a criação de uma rede de centros de competências em matéria de cibersegurança e de um Centro Europeu de Investigação e de Competências em matéria de Cibersegurança, partindo de uma fase-piloto imediata;
- Apoio aos Estados-Membros na identificação dos domínios em que projetos de cibersegurança comuns possam ser considerados para efeitos de financiamento pelo Fundo Europeu de Defesa;
- Criação de um «balcão único» a nível da UE para ajudar as vítimas de ciberataques, prestando informações sobre as ameaças mais recentes e reunindo recomendações práticas e instrumentos de cibersegurança;
- Adoção, pelos Estados-Membros, de medidas para integrar a cibersegurança em programas de competências, na administração pública em linha e em campanhas de sensibilização;
- Adoção, pela indústria, de medidas destinadas a intensificar a formação em matéria de cibersegurança para o seu pessoal e adotar o princípio da «segurança desde a conceção» para os seus produtos, serviços e processos.

[56] Um exemplo é o Grupo de Trabalho East StratCom criado em 2015 pelos Estados-Membros e pela Alta Representante para dar resposta às campanhas de desinformação em curso por parte da Rússia. A equipa está empenhada no desenvolvimento de produtos e campanhas de comunicação que pretendem explicar as políticas da UE na região da Parceria Oriental.

[57] Alguns fabricantes já estão familiarizados com este conceito, uma vez que alguns atos legislativos relativos a produtos (como a Diretiva 2006/42/CE relativa às máquinas) determinam princípios para a «segurança desde a conceção».

[58] COM(2017) 477.

3. CRIAR UMA CIBERDISSUASÃO EFICAZ A NÍVEL DA UE

Por dissuasão eficaz entende-se pôr em prática um quadro de medidas que sejam credíveis e tenham um efeito dissuasor para os potenciais cibercriminosos e autores de ataques. Enquanto os autores de ciberataques, estatais ou não estatais, nada tiverem a recear, além do insucesso, terão pouco incentivo para pararem de tentar. Uma resposta mais eficaz por via da aplicação da lei, centrada na deteção, identificação e ação penal contra os cibercriminosos é fulcral para se criar uma dissuasão eficaz. Acresce ainda a necessidade de a UE apoiar os Estados-Membros no desenvolvimento de capacidades de cibersegurança de dupla utilização. Só poderemos começar a inverter o cenário atual de ciberataques quando aumentarmos as probabilidades de deteção de infrações e de aplicação de sanções a quem as praticar. Os ciberataques devem ser imediatamente investigados e os seus autores levados à justiça, ou devem ser tomadas medidas no sentido de permitir uma resposta política ou diplomática adequada. Em caso de crise grave com uma importante dimensão internacional e a nível da defesa, a Alta Representante poderá apresentar opções ao Conselho para uma resposta adequada.

Já foi dado um passo importante no sentido de melhorar a resposta do direito penal aos ciberataques, com a adoção, em 2013, da Diretiva relativa a ataques contra os sistemas de informação[59]. Esta estabelece regras mínimas relativas à definição das infrações penais e das sanções no domínio dos ataques contra os sistemas de informação e prevê medidas operacionais para melhorar a cooperação entre autoridades. A diretiva conduziu a progressos substanciais no âmbito da criminalização dos ciberataques a um nível comparável em todos os Estados-Membros, o que favorece a cooperação transfronteiriça entre as autoridades responsáveis pela aplicação da lei que investigam estes tipos de infrações. Contudo, ainda existe uma margem até que a diretiva atinja todo o seu potencial, caso os Estados-Membros apliquem todas as suas disposições na íntegra[60]. A Comissão continuará a apoiar os Estados-Membros na execução da diretiva e não considera, atualmente, necessário propor alterações à mesma.

3.1 Identificar intervenientes mal intencionados

Para aumentarmos as possibilidades de levar os autores à justiça, é urgente melhorar a nossa capacidade de identificar os responsáveis pelos ciberataques. Encontrar informações úteis para a investigação da cibercriminalidade, principalmente sob a forma de rastos digitais, constitui um enorme desafio para as autoridades responsáveis pela aplicação da lei. Por conseguinte, temos de aumentar a nossa capacidade tecnológica para investigar eficazmente a cibercriminalidade, nomeadamente mediante o reforço da unidade da Europol dedicada a esse domínio com peritos em cibersegurança. A Europol tornou-se um interveniente fundamental no apoio às investigações plurijurisdicionais dos Estados-Membros. A Europol deve tornar-se num centro de conhecimentos especializados sobre investigações em linha e informática forense para fins de aplicação da lei por parte dos Estados-Membros.

A prática generalizada de atribuir o mesmo endereço IP a múltiplos utilizadores, por vezes milhares, torna tecnicamente muito difícil a investigação de comportamentos maliciosos em linha. Por outro lado, também obriga muitas vezes, por exemplo, no caso de crimes graves como o abuso sexual de crianças, a investigar um grande número de utilizadores para identificar um interveniente mal intencionado. Por conseguinte, a UE incentivará a adoção do

[59] Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho.

[60] COM(2017) 474.

novo protocolo IPv6, uma vez que este apenas permite a atribuição de um único utilizador por endereço IP, trazendo assim benefícios claros para a aplicação da lei e as investigações em matéria de cibersegurança. Como primeira medida para incentivar esta adoção, a Comissão integrará o requisito de transição para o IPv6 em todas as suas políticas, incluindo os requisitos em matéria de contratos públicos, de financiamento de projetos e de investigação, e apoiará a elaboração dos materiais de formação necessários. Além disso, os Estados-Membros devem ponderar a celebração de acordos voluntários com fornecedores de serviços de Internet, para dar um impulso à adoção do IPv6.

A Bélgica lidera, à escala mundial[61]*, a taxa de adoção do IPv6, graças também à cooperação entre os setores público e privado: as partes interessadas relevantes ponderaram limitar a atribuição de um endereço IP a um máximo de 16 utilizadores como parte de uma medida voluntária de autorregulação, o que incentivou a transição para o IPv6*[62].

De um modo mais geral, é necessário promover ainda mais a responsabilização em linha. Tal implica promover medidas destinadas a prevenir a utilização abusiva de nomes de domínio para a distribuição de mensagens não solicitadas ou ataques de mistificação da interface (*phishing*). Para este efeito, a Comissão trabalhará no sentido de melhorar o funcionamento, a disponibilidade e a exatidão das informações constantes do Sistema de Nomes de Domínio e do IP WHOIS[63] em consonância com os esforços da Sociedade da Internet para os Nomes e Números Atribuídos[64].

3.2 Reforçar a aplicação coerciva da lei

A eficácia da **investigação** e da **ação penal** contra a criminalidade possibilitada pelo ciberespaço é um importante elemento dissuasor de ciberataques. No entanto, o atual quadro processual deve ser melhor adaptado à era da Internet[65]. A velocidade dos ciberataques pode ultrapassar os procedimentos em vigor, e criar necessidades específicas de rápida cooperação transfronteiras. Para este efeito, e tal como anunciado no âmbito da Agenda Europeia para a Segurança, a Comissão apresentará propostas, no início de 2018, destinadas a **facilitar o acesso transfronteiriço a provas eletrónicas**. Paralelamente, a Comissão está a pôr em prática medidas para melhorar o acesso transfronteiriço a provas eletrónicas no âmbito de investigações criminais, incluindo o financiamento de formação sobre cooperação transfronteiriça, o desenvolvimento de uma plataforma eletrónica para intercâmbio de informações na UE, e a normalização dos formulários utilizados para a cooperação judiciária entre os Estados-Membros.

Outro obstáculo a uma ação penal efetiva são os diferentes procedimentos forenses para a recolha de provas eletrónicas nas investigações de cibercriminalidade nos Estados-Membros. Tal poderia ser atenuado, trabalhando no sentido da criação de normas forenses comuns. Além disso, para apoiar a rastreabilidade e a atribuição de autoria, é necessário reforçar as

---

61 https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

62 http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf.

63 Protocolo de consulta e resposta amplamente utilizado para pesquisar bases de dados que armazenam as informações dos utilizadores registados ou dos titulares de um recurso da Internet.

64 A Sociedade da Internet para os Nomes e Números Atribuídos (ICANN — Internet Corporation for Assigned Names and Numbers) é uma organização sem fins lucrativos responsável pela coordenação da manutenção e dos procedimentos de várias bases de dados relacionadas com os espaços de nomes da Internet.

65 Para citar apenas um exemplo, o servidor de comando e controlo central (virtual) do *botnet* Avalanche transferia os servidores e os domínios físicos de cinco em cinco minutos.

capacidades forenses. Uma das medidas possíveis consistiria em reforçar as capacidades da Europol a nível forense, adaptando os atuais recursos orçamentais e humanos do Centro Europeu da Cibercriminalidade da Europol, a fim de dar resposta à crescente necessidade de apoio operacional a investigações de cibercriminalidade transfronteiriça. Outra medida seria replicar a orientação tecnológica acima exposta em relação à cifragem, analisando a forma como a sua utilização abusiva por parte de criminosos cria desafios significativos na luta contra a grande criminalidade, nomeadamente o terrorismo e a cibercriminalidade. A Comissão apresentará os resultados das atuais reflexões sobre o **papel da cifragem nas investigações criminais**[66] até outubro de 2017[67].

Dada a natureza sem fronteiras da Internet, o quadro de cooperação internacional previsto pela **Convenção de Budapeste sobre o Cibercrime**[68] do Conselho da Europa oferece a possibilidade de utilizar, entre um grupo diversificado de países, a norma jurídica ideal para as diferentes legislações nacionais que tratam da cibercriminalidade. Está a ser estudado o eventual aditamento de um protocolo à Convenção[69], o que poderá também proporcionar uma oportunidade para abordar a questão do acesso transfronteiriço a provas eletrónicas num contexto internacional. Em vez da criação de novos instrumentos jurídicos internacionais para as questões da cibercriminalidade, a UE apela para que todos os países elaborem legislação nacional adequada e prossigam a cooperação no âmbito do quadro internacional existente.

A disponibilidade generalizada de ferramentas de anonimização permite que os criminosos se possam facilmente esconder. A «**Internet obscura» (*darknet*)**[70] criou novos meios de os criminosos acederem a materiais relativos a abusos sexuais de crianças, a drogas ou a armas de fogo, frequentemente com um risco reduzido de serem apanhados[71]. Atualmente, é também a principal origem das ferramentas utilizadas no âmbito da cibercriminalidade, tais como *software* mal intencionado e ferramentas de pirataria informática. A Comissão, em conjunto com as partes interessadas, analisará abordagens nacionais com vista à identificação de novas soluções. A Europol deve facilitar e apoiar investigações sobre a Internet obscura, analisar as ameaças e ajudar a determinar a competência jurisdicional e a dar prioridade aos casos de alto risco, podendo a UE desempenhar um papel de liderança na coordenação das ações a nível internacional[72].

Uma área de crescente atividade cibercriminosa é a utilização fraudulenta dos dados de cartões de crédito ou de outros meios de pagamento eletrónico. As credenciais de pagamento

---

66 Presidência do Conselho, Resultados da reunião do Conselho (Justiça e Assuntos Internos) de 8 e 9 de dezembro de 2016, documento n.º 15391/16.

67 Oitavo relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz, de 29 de junho de 2017, COM(2017) 354 final.

68 A Convenção é o primeiro tratado internacional sobre crimes cometidos por meio da Internet e de outras redes informáticas, estando especialmente relacionada com violações dos direitos de autor, fraude informática, pornografia infantil e violações da segurança da rede. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. Em 2017, 55 governos tinham ratificado ou aderido à Convenção do Conselho da Europa sobre o Cibercrime.

69 Termos de referência para a elaboração de um projeto de 2.º Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime, T-CY (2017)3.

70 A Internet obscura consiste em conteúdos em redes sobrepostas que utilizam a Internet, mas que exigem suportes lógicos, configurações ou autorizações específicas de acesso. A Internet obscura representa apenas uma pequena parte da *Web* invisível, a parte da *Web* não indexada por motores de pesquisa.

71 Uma exceção notável é a recente remoção de dois dos mais importantes mercados ilegais das redes obscuras, as plataformas AlphaBay e Hansa: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

72 A Europol desempenha já um papel importante neste domínio. Para um exemplo recente, ver: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

obtidas em ciberataques contra lojas virtuais ou outras empresas legítimas são posteriormente negociadas em linha, podendo ser utilizadas por criminosos para cometerem fraudes[73]. A Comissão apresenta uma proposta para reforçar a dissuasão por intermédio de uma **Diretiva relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário**[74]. Esta visa atualizar as regras existentes neste domínio e reforçar a capacidade das autoridades responsáveis pela aplicação da lei para lutar contra esta forma de criminalidade.

As capacidades de investigação da cibercriminalidade das autoridades policiais dos Estados-Membros devem também ser melhoradas, bem como os conhecimentos dos magistrados do Ministério Público e do sistema judiciário sobre a criminalidade possibilitada pelo ciberespaço e as opções de investigação. A Eurojust e a Europol contribuem para este objetivo e para o reforço da coordenação, em estreita cooperação com os grupos consultivos especializados do Centro de Cibercriminalidade da Europol e com as redes dos chefes das unidades de cibercriminalidade e dos magistrados do Ministério Público especializados em cibercriminalidade. A Comissão vai consagrar 10,5 milhões de EUR de financiamento para lutar contra a cibercriminalidade, principalmente no âmbito do seu **Programa Polícia do Fundo de Segurança Interna**. A formação é um elemento importante, pelo que o Grupo Europeu de Formação e Educação em Cibercrime desenvolveu um conjunto de materiais úteis para esse efeito. Estes devem agora ser amplamente disponibilizados aos profissionais responsáveis pela aplicação da lei, com o apoio da Agência da União Europeia para a Formação Policial (CEPOL).

3.3 Cooperação entre os setores público e privado contra a cibercriminalidade

A eficácia dos mecanismos tradicionais de aplicação da lei é posta em causa pelas características do mundo digital, que consiste maioritariamente em infraestruturas privadas e numerosos intervenientes numa grande variedade de jurisdições. Por conseguinte, a cooperação com o setor privado, incluindo a indústria e a sociedade civil, é fundamental para permitir que autoridades públicas combatam eficazmente a criminalidade. Neste contexto, o setor financeiro é também fundamental, pelo que importa intensificar a cooperação neste domínio. Por exemplo, é necessário reforçar o papel das Unidades de Informação Financeira[75] no âmbito da cibercriminalidade.

Alguns Estados-Membros já tomaram medidas essenciais. Nos Países Baixos, as instituições financeiras e as autoridades policiais trabalham lado a lado para fazer face à fraude em linha e à cibercriminalidade no grupo de trabalho sobre criminalidade eletrónica. O centro alemão de competências contra a cibercriminalidade constitui a plataforma operacional para os seus membros procederem ao intercâmbio de informações, em estreita colaboração com o Serviço Federal de Polícia Judiciária Alemã, e elaborarem medidas para garantir a proteção contra a cibercriminalidade. Dezasseis Estados-Membros[76] criaram centros de excelência contra a cibercriminalidade para facilitar a cooperação entre as autoridades responsáveis

[73] Os produtos das fraudes são uma importante fonte de rendimento para a criminalidade organizada e, por conseguinte, um fator que contribui para outras atividades criminosas, tais como o terrorismo, o tráfico de droga e o tráfico de seres humanos.

[74] COM(2017) 489.

[75] As Unidades de Informação Financeira funcionam como centros nacionais para a receção e análise de comunicações de operações suspeitas e outras informações pertinentes relativas a branqueamento de capitais, infrações subjacentes associadas e financiamento do terrorismo, e para a divulgação dos resultados dessa análise.

[76] Bélgica, Bulgária, República Checa, Alemanha, Estónia, Irlanda, Grécia, Espanha, França, Chipre, Lituânia, Áustria, Polónia, Roménia, Eslovénia, e Reino Unido.

pela aplicação da lei, os meios académicos e os parceiros privados para o desenvolvimento e o intercâmbio de boas práticas, a formação e o reforço das capacidades.
A Comissão apoia a criação de parcerias público-privadas e de mecanismos de cooperação por intermédio de projetos específicos, como o centro de ciberdefesa e rede de peritos contra fraudes em linha[77]*, que introduzem modelos e normas de partilha de informações, com vista a analisar e atenuar os riscos de crimes eletrónicos e fraudes em linha.*

No contexto da cibercriminalidade, as empresas privadas devem ter a possibilidade de partilhar informações sobre incidentes concretos com as autoridades responsáveis pela aplicação da lei, incluindo dados pessoais, no pleno respeito das normas de proteção de dados. A reforma do regime de proteção de dados na UE, que entrará em vigor em maio de 2018, prevê um conjunto de regras comuns que estabelecem as condições ao abrigo das quais as autoridades responsáveis pela aplicação da lei e as entidades privadas podem cooperar. A Comissão Europeia trabalhará com o Comité Europeu para a Proteção de Dados e as partes interessadas relevantes para identificar as melhores práticas neste domínio e, se for caso disso, fornecer orientações sobre essa matéria.

3.4 Reforçar a resposta política

O recém-adotado **quadro para uma resposta diplomática conjunta da UE às ciberatividades maliciosas**[78] («instrumentos de ciberdiplomacia») estabelece as medidas no âmbito da política externa e de segurança comum, incluindo medidas restritivas, que podem ser utilizadas para reforçar a resposta da UE a atividades que lesem os seus interesses políticos, económicos e de segurança. O quadro constitui um passo importante para o desenvolvimento de capacidades de sinalização e de reação a nível da UE e dos Estados-Membros. Permitirá igualmente aumentar a capacidade de atribuição da autoria de ciberatividades maliciosas, com o objetivo de influenciar o comportamento de potenciais autores, tendo simultaneamente em conta a necessidade de garantir respostas adequadas. A atribuição a um interveniente estatal ou não estatal continua a ser uma decisão política soberana baseada em informações provenientes de todas as fontes. O trabalho de aplicação do quadro está atualmente em curso nos Estados-Membros e deverá também ser estreitamente coordenado com o plano de ação para uma resposta a ciberincidentes em grande escala[79]. O conhecimento da situação, necessário para recorrer a medidas no âmbito do quadro, deve ser concentrado, analisado e partilhado pelo INTCEN[80], em estreita colaboração com os Estados-Membros e as instituições da UE.

3.5 Reforçar a vertente de dissuasão da cibersegurança por intermédio das capacidades de defesa dos Estados-Membros

Os Estados-Membros estão já a desenvolver capacidades em matéria de ciberdefesa. Além disso, tendo em conta a definição pouco clara dos limites entre ciberdefesa e cibersegurança e a natureza de dupla utilização das ferramentas e tecnologias do ciberespaço, bem como a

[77] A iniciativa EU-OF2CEN tem por objetivo permitir a partilha sistemática, à escala da UE, de informações relacionadas com fraudes na Internet, entre os bancos e os serviços responsáveis pela aplicação da lei, com vista à prevenção de pagamentos a autores de fraudes e internautas ligados à lavagem de dinheiro e para a investigação e ação penal contra os intervenientes envolvidos. A iniciativa é cofinanciada pela UE (Programa Polícia do Fundo para Segurança Interna).

[78] http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.

[79] C(2017) 6100.

[80] JOIN(2016) 018 final.

grande diversidade entre as abordagens dos Estados-Membros, a UE está bem colocada para ajudar a promover sinergias entre os esforços civis e militares[81].

Os Estados-Membros que disponham de capacidades de cibersegurança mais avançadas e que estejam dispostos a articulá-las em conjunto poderão ponderar, com o apoio da Alta Representante, da Comissão e da Agência Europeia de Defesa, a inclusão da ciberdefesa no âmbito de um quadro de cooperação estruturada permanente (PESCO). Essa iniciativa poderá ser apoiada pelo trabalho descrito acima, para incentivar as capacidades industriais e a autonomia estratégica da UE. A UE pode igualmente promover a interoperabilidade, nomeadamente facilitando o desenvolvimento de capacidades, a coordenação da formação e educação e os esforços no sentido da normalização da dupla utilização.

Deve ainda ser aproveitado plenamente o quadro comum para responder a ameaças híbridas, que muitas vezes envolvem ciberataques, nomeadamente por intermédio da célula de fusão da UE contra as ameaças híbridas e do recém-criado Centro Europeu de Luta contra as Ameaças Híbridas, em Helsínquia, cuja missão consiste em incentivar o diálogo estratégico e em realizar trabalhos de investigação e análise.

A UE dará um novo destaque ao Quadro Estratégico da UE para a Ciberdefesa[82], de 2014, como um instrumento para integrar a cibersegurança e a ciberdefesa na política comum de segurança e defesa (PCSD). A ciber-resiliência das próprias missões e operações da PCSD é essencial: serão desenvolvidos procedimentos normalizados e capacidades técnicas que poderão apoiar as missões e operações civis e militares destacadas, bem como as respetivas estruturas de capacidade de planeamento e condução e os prestadores de serviços de tecnologia da informação do SEAE. A fim de promover a cooperação entre os Estados-Membros e permitir uma melhor orientação dos esforços da UE neste domínio, a Agência Europeia de Defesa e o SEAE, em cooperação com os serviços da Comissão, facilitarão o compromisso a nível estratégico entre os decisores políticos dos Estados-Membros em matéria de ciberdefesa. A UE apoiará também o desenvolvimento de soluções europeias de cibersegurança no âmbito dos seus esforços no sentido de criar uma base industrial e tecnológica de defesa europeia. Tal inclui igualmente a promoção de polos regionais de excelência no domínio da cibersegurança e da defesa.

Os serviços da Comissão, em estreita cooperação com o SEAE, os Estados-Membros e outros organismos competentes da UE, estabelecerão até 2018 **uma plataforma de formação e educação em matéria de ciberdefesa** para colmatar o atual défice de competências nesse domínio. Esta plataforma complementará o trabalho da Agência Europeia de Defesa neste domínio, contribuindo para colmatar a atual escassez de competências em matéria de cibersegurança e de ciberdefesa.

Ações-chave

- Iniciativa da Comissão para o acesso transfronteiriço a provas eletrónicas (início de 2018);
- Adoção rápida, pelo Parlamento Europeu e pelo Conselho, da proposta de diretiva relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário;
- Introdução de requisitos relativos ao IPv6 nos concursos públicos e no financiamento de investigação e de projetos por parte da UE; celebração de acordos voluntários entre os Estados-Membros e os fornecedores de serviços de Internet para promover a adoção do

[81] A UE entende o ciberespaço como um domínio de operações semelhante aos da terra, ar e mar. Os esforços de ciberdefesa incluem igualmente a proteção e a resiliência dos meios espaciais e das infraestruturas em terra conexas.

[82] www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515.

IPv6;
- Ênfase renovada e alargada da Europol no domínio da informática forense e da monitorização da Internet obscura (*darknet*);
- Aplicação do quadro para uma resposta diplomática conjunta da UE às ciberatividades maliciosas;
- Reforço do apoio financeiro a projetos nacionais e transnacionais para a melhoria da justiça penal no ciberespaço.
- Criação, em 2018, de uma plataforma de formação em matéria de cibersegurança para fazer face ao atual défice de competências em matéria de cibersegurança e de ciberdefesa.

4. REFORÇO DA COOPERAÇÃO INTERNACIONAL EM MATÉRIA DE CIBERSEGURANÇA

Sendo guiada pelos valores e direitos fundamentais da UE, tais como a liberdade de expressão e o direito à privacidade e à proteção dos dados pessoais, e pela promoção de um ciberespaço aberto, livre e seguro, a política internacional de cibersegurança da UE pretende fazer face ao desafio em constante evolução da promoção da estabilidade do ciberespaço a nível mundial, bem como contribuir para a autonomia estratégica da Europa no ciberespaço.

4.1 Cibersegurança no âmbito das relações externas

Há estudos que indicam que, por todo o mundo, as pessoas consideram que os ciberataques com origem noutros países se encontram entre as principais ameaças para a segurança nacional[83]. Tendo em conta a natureza global da ameaça, o estabelecimento e a manutenção de alianças e parcerias sólidas com países terceiros são fundamentais para a prevenção e dissuasão de ciberataques, objetivos com uma importância cada vez mais central para a estabilidade e a segurança internacional. A UE dará prioridade à criação de um quadro estratégico para a prevenção de conflitos e a promoção da estabilidade do ciberespaço no âmbito dos seus compromissos bilaterais, regionais, multilaterais e com todos as partes interessadas.

A UE defende vivamente a posição de que o direito internacional, em especial a Carta das Nações Unidas, é aplicável ao ciberespaço. Como complemento do direito internacional vinculativo, a UE apoia as normas, regras e princípios não vinculativos e voluntários relativos ao comportamento responsável dos Estados que foram articuladas pelo Grupo de Peritos Governamentais das Nações Unidas[84]; encoraja igualmente o desenvolvimento e aplicação de medidas regionais de reforço da confiança, tanto na Organização para a Segurança e a Cooperação na Europa como em outras regiões.

A nível bilateral, os ciberdiálogos[85] continuarão a ser desenvolvidos e completados por esforços no sentido de facilitar a cooperação com países terceiros a fim de reforçar os princípios de diligência devida e de responsabilidade dos Estados no ciberespaço. A UE dará prioridade às questões de segurança internacional no ciberespaço, no âmbito dos seus compromissos internacionais, assegurando, ao mesmo tempo, que a cibersegurança não se torne um pretexto para a proteção do mercado e a limitação dos direitos e liberdades fundamentais, nomeadamente a liberdade de expressão e o acesso à informação. Uma abordagem global da cibersegurança pressupõe o respeito dos direitos humanos, e a União

[83] *Global Attitudes Survey* (inquérito às atitudes globais), primavera de 2017, Pew Research Centre.
[84] A/68/98 e A/70/174.
[85] Em setembro de 2017, a UE manteve ciberdiálogos com os EUA, a China, o Japão, a República da Coreia e a Índia.

Europeia continuará a defender os seus valores fundamentais a nível mundial, tomando como base as diretrizes da UE em matéria de direitos humanos, relativas à liberdade de expressão em linha[86]. A este respeito, a UE salienta a importância do envolvimento de todas as partes interessadas na governação da Internet.

A Comissão também apresentou uma proposta[87] para modernizar os controlos das exportações da UE, incluindo a introdução de controlos sobre a exportação de tecnologias de cibervigilância críticas que possam dar lugar a violações dos direitos humanos ou ser utilizadas contra a própria segurança da UE, e intensificará o diálogo com os países terceiros no sentido de promover uma convergência global e um comportamento responsável neste domínio.

4.2 Reforço das capacidades no domínio da cibersegurança

A estabilidade do ciberespaço a nível mundial assenta na capacidade local e nacional de todos os países para prevenir e reagir a ciberincidentes e investigar e agir judicialmente contra casos de cibercriminalidade. O apoio aos esforços no sentido de reforçar a resiliência nacional de países terceiros aumentará o nível de cibersegurança a nível mundial, com consequências positivas para a UE. A luta contra ciberameaças em rápida evolução pressupõe a necessidade de formação, de esforços para o desenvolvimento de políticas e de legislação, bem como o bom funcionamento de equipas de resposta a emergências informáticas e unidades dedicadas à cibercriminalidade em todos os países do mundo.

Desde 2013, a UE tem assumido um papel de liderança, a nível internacional, no reforço das capacidades em matéria de cibersegurança e na interligação sistemática entre esses esforços e a sua política de cooperação para o desenvolvimento. A UE continuará a promover um modelo de reforço das capacidades baseado nos direitos, em consonância com a abordagem Digital4Development[88]. As prioridades para o reforço das capacidades incidirão em questões relativas ao rápido incremento da conectividade e à exponenciação das ameaças nos países vizinhos da UE e nos países em desenvolvimento. Os esforços da UE complementarão a agenda de desenvolvimento da UE, à luz da Agenda 2030 para o Desenvolvimento Sustentável e dos esforços globais para o reforço das capacidades institucionais.

A fim de melhorar a capacidade da UE de mobilizar as suas competências especializadas coletivas para apoiar este reforço de capacidades, deve ser criada uma rede da UE dedicada ao reforço das capacidades em matéria de cibersegurança, que reúna o SEAE, as autoridades dos Estados-Membros no domínio da cibersegurança, as agências da UE, os serviços da Comissão, os meios académicos e a sociedade civil. Serão desenvolvidas diretrizes da UE para o reforço das capacidades em matéria de cibersegurança, que permitam prestar melhores orientações políticas e definir prioridades nos esforços de assistência da UE a países terceiros.

A UE trabalhará igualmente em conjunto com os outros doadores neste domínio, a fim de evitar a duplicação de esforços e facilitar o reforço de capacidades mais específicas em diferentes regiões.

4.3 COOPERAÇÃO UE-OTAN

Com base nos progressos significativos já realizados, a UE vai aprofundar a sua cooperação com a OTAN em matéria de cibersegurança, ameaças híbridas e defesa, tal como previsto na

[86] Diretrizes da UE em matéria de direitos humanos, relativas à liberdade de expressão em linha e fora de linha.
[87] COM(2016) 616.
[88] SWD(2017) 157.

declaração conjunta de 8 de julho de 2016[89]. As prioridades incidem na promoção da interoperabilidade por via de normas e requisitos de ciberdefesa coerentes, no reforço da cooperação em matéria de formação e de exercícios e na harmonização dos requisitos de formação.

A UE e a OTAN promoverão também a cooperação para a investigação e a inovação em matéria de ciberdefesa e desenvolverão o atual acordo técnico sobre a partilha de informações de cibersegurança entre os respetivos organismos de cibersegurança[90]. Os recentes esforços conjuntos na luta contra as ameaças híbridas, nomeadamente a cooperação entre a célula de fusão da UE contra as ameaças híbridas e a célula de análise de ameaças híbridas da OTAN, devem ser ainda melhorados de modo a reforçar a resiliência e a resposta às crises de cibersegurança. Será promovida uma maior cooperação entre a UE e a OTAN por meio de exercícios de ciberdefesa, com a participação do SEAE e de outras entidades da UE e dos respetivos homólogos daquela organização, incluindo o Centro de Excelência Cooperativo para a Ciberdefesa da OTAN, sediado em Taline. A OTAN e a UE efetuarão, pela primeira vez, exercícios paralelos e coordenados de resposta a um cenário híbrido, tendo a OTAN assumido a liderança do exercício de 2017, ao que a UE responderá de forma análoga em 2018. O próximo relatório sobre a cooperação UE-OTAN, a apresentar aos respetivos Conselhos em dezembro de 2017, oferecerá uma oportunidade para analisar as possibilidades de expandir a cooperação, nomeadamente garantindo meios de comunicação comuns, seguros e sólidos entre todas as instituições e organismos competentes envolvidos, incluindo a ENISA.

Ações-chave

- Avançar com o quadro estratégico para a prevenção de conflitos e a estabilidade do ciberespaço;
- Desenvolver uma nova rede de reforço das capacidades para apoiar a capacidade de resposta dos países terceiros às ciberameaças, e elaborar diretrizes da UE para o reforço das capacidades em matéria de cibersegurança que permitam definir melhor as prioridades dos esforços da UE;
- Reforçar a cooperação entre a UE e a NATO, incluindo a participação em exercícios paralelos e coordenados e uma maior interoperabilidade das normas relativas à cibersegurança.

5. CONCLUSÃO

A preparação da UE em termos de cibersegurança é essencial tanto para o mercado único digital como para a União da Segurança e da Defesa. É imperioso reforçar a cibersegurança e combater as ameaças tanto contra alvos civis como militares.

A próxima Cimeira Digital, organizada pela Presidência estónia, em 29 de setembro de 2017, oferece uma oportunidade de mostrar uma determinação comum para colocar a cibersegurança no centro do debate da UE, enquanto sociedade digital. No âmbito deste compromisso comum, a Comissão convida os Estados-Membros a comprometerem-se com a forma como pretendem atuar em domínios em que são os principais responsáveis. Tal deverá incluir o reforço da cibersegurança, nomeadamente:

[89] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/.
[90] A CERT-UE e a Capacidade de Resposta a Incidentes Informáticos da OTAN (NCIRC).

- Garantindo a aplicação plena e efetiva da Diretiva SRI até 9 de maio de 2018, bem como os recursos necessários para que as autoridades públicas responsáveis pela cibersegurança desempenhem eficazmente as suas tarefas;
- Aplicando as mesmas regras às administrações públicas, tendo em conta o papel que desempenham na sociedade e na economia em geral;
- Providenciando formação em matéria de cibersegurança na administração pública;
- Dando prioridade aos conhecimentos sobre o mundo virtual em campanhas de informação e integrando a cibersegurança nos programas curriculares académicos e de formação profissional;
- Utilizando iniciativas ao abrigo da cooperação estruturada permanente (PESCO) e do Fundo Europeu de Defesa para apoiar o desenvolvimento de projetos de ciberdefesa.

A presente comunicação conjunta definiu a dimensão do desafio e o conjunto de medidas que a UE pode tomar. Precisamos de uma Europa que seja resiliente e capaz de proteger os seus cidadãos de forma eficaz, antecipando possíveis incidentes de cibersegurança, criando uma sólida proteção das suas estruturas e comportamentos, recuperando rapidamente de eventuais ciberataques, e dissuadindo os responsáveis por tais práticas. A presente comunicação apresenta medidas específicas que reforçarão as estruturas e capacidades de cibersegurança da UE de forma coordenada, com a plena cooperação dos Estados-Membros e das diferentes estruturas da UE nesse domínio, e no respeito das suas competências e responsabilidades. A sua execução proporcionará uma clara demonstração de que a UE e os Estados-Membros trabalharão em conjunto para pôr em prática um nível de cibersegurança equivalente ao crescente número de desafios que a Europa enfrenta atualmente.