TRIBUNAL DE CONTAS EUROPEU

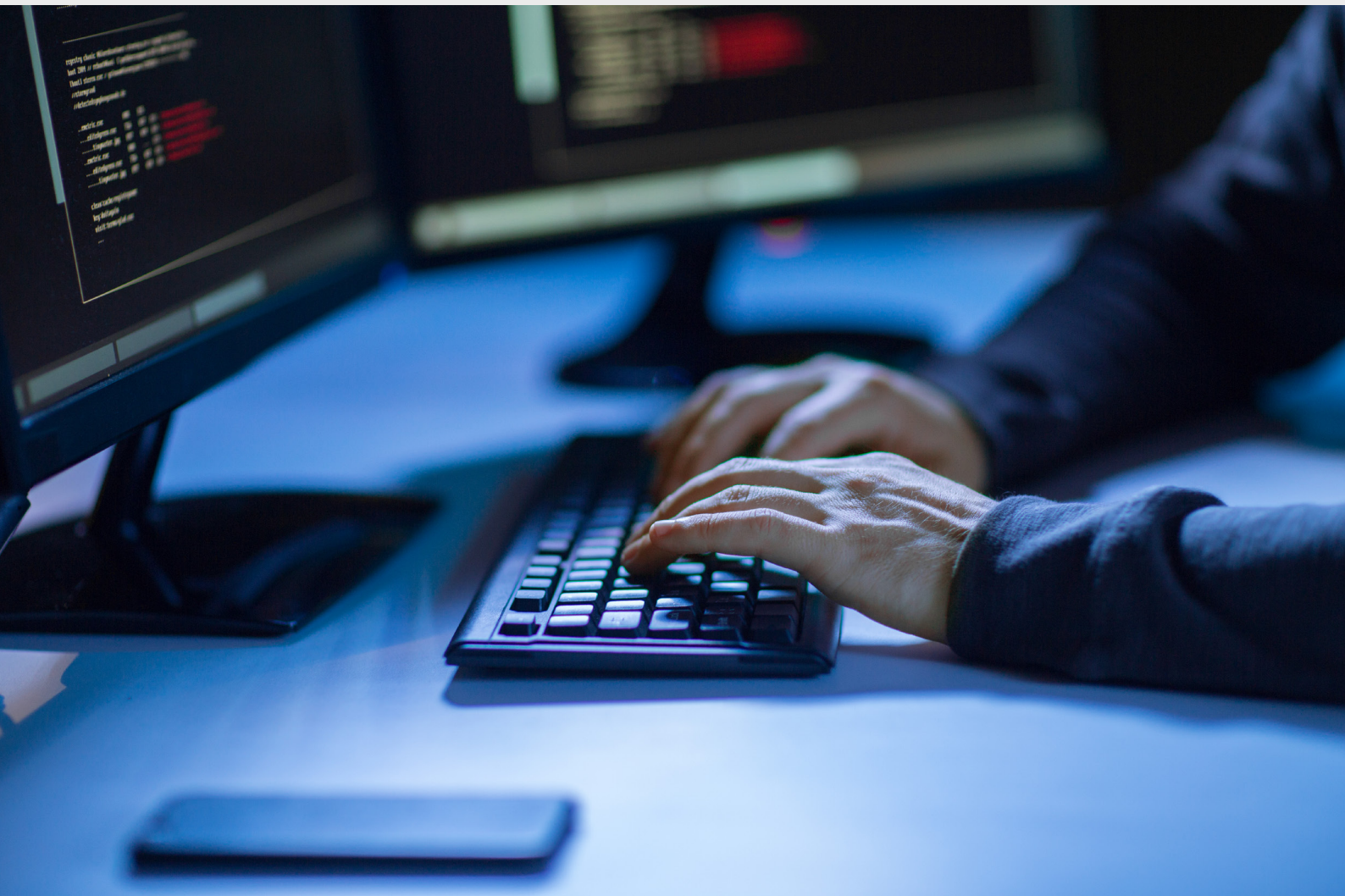
PT

2019

Desafios à eficácia da política de cibersegurança da UE

Documento informativo

Março de 2019



Sobre este documento informativo:

O presente documento informativo, que não constitui um relatório de auditoria, visa dar uma visão geral do complexo panorama da política da UE em matéria de cibersegurança e assinalar os principais desafios à sua execução eficaz. Abrange a segurança das redes e das informações, a cibercriminalidade, a ciberdefesa e a desinformação e servirá igualmente de referência para eventuais futuros trabalhos de auditoria neste domínio.

O Tribunal baseou a sua apreciação numa análise documental das informações disponíveis ao público em documentos oficiais, posições escritas e estudos de terceiros. O trabalho de campo foi realizado entre abril e setembro de 2018, sendo tidos em conta os acontecimentos ocorridos até dezembro de 2018. O Tribunal complementou o trabalho com um inquérito às instituições superiores de controlo dos Estados-Membros e com entrevistas às principais partes interessadas das instituições da UE e representantes do setor privado.

Os desafios encontrados são agrupados em quatro grandes temas: i) quadro estratégico; ii) financiamento e despesas; iii) criação de ciber-resiliência; iv) resposta eficaz a ciberincidentes. Conseguir um maior nível de cibersegurança na UE continua a ser um teste determinante. Por esse motivo, o Tribunal termina cada capítulo com várias ideias para que os decisores políticos, os legisladores e os profissionais deste domínio possam prosseguir esta reflexão.

O Tribunal gostaria de agradecer as observações construtivas recebidas dos serviços da Comissão, do Serviço Europeu para a Ação Externa, do Conselho da União Europeia, da ENISA, da Europol, da Organização Europeia de Cibersegurança e das instituições superiores de controlo dos Estados-Membros.

Índice

Síntese

I A tecnologia está a desvelar todo um mundo novo de oportunidades, com novos produtos e serviços que se tornam parte integrante do nosso quotidiano. Por sua vez, o risco de as pessoas serem vítimas da cibercriminalidade ou de um ciberataque está a aumentar, tal como o impacto que daí advém para a sociedade e a economia. O recente impulso dado pela UE, desde 2017, no sentido de acelerar os seus esforços para reforçar a cibersegurança e a sua autonomia digital chegam, assim, num momento crítico.

II O presente documento informativo, que não constitui um relatório de auditoria e se baseia em informações disponíveis ao público, procura apresentar uma visão geral do panorama complexo e desigual da política da UE nesta matéria e apontar os principais desafios à eficácia da sua execução. O seu âmbito abrange a política de cibersegurança da UE, a cibercriminalidade e a ciberdefesa, bem como os esforços de combate à desinformação. Os desafios encontrados pelo Tribunal são agrupados em quatro grandes temas: i) quadro estratégico e legislativo; ii) financiamento e despesas; iii) criação de ciber-resiliência; iv) resposta eficaz a ciberincidentes. Cada capítulo inclui alguns pontos de reflexão sobre os desafios apresentados.

Quadro estratégico e legislativo

III Na ausência de objetivos mensuráveis e dispondo de poucos dados fiáveis, é um verdadeiro desafio desenvolver medidas que se coadunem com os objetivos gerais da estratégia de cibersegurança da UE de a tornar no ambiente digital mais seguro do mundo. Os efeitos raramente são medidos e poucos domínios de intervenção foram avaliados. Um desafio crucial é, assim, **garantir uma verdadeira prestação de contas e avaliação**, através de uma transição para uma cultura de desempenho com práticas de avaliação integradas.

IV O quadro legislativo permanece incompleto, além de que **as lacunas e as diferenças na transposição da legislação da UE** podem dificultar a concretização de todo o seu potencial.

Financiamento e despesas

V **Adaptar os níveis de investimento aos objetivos** é um desafio, exigindo um aumento não só do investimento global em cibersegurança – que tem sido reduzido e fragmentado na UE – mas também do seu impacto, sobretudo no que se refere a

aproveitar melhor os resultados das despesas no domínio da investigação e a garantir que se visam e financiam com eficácia as empresas em fase de arranque.

VI É essencial **dispor de uma visão geral clara das despesas da UE** para que a União e os Estados-Membros determinem as lacunas a colmatar para cumprir os objetivos que declararam. Uma vez que não existe um orçamento específico da UE para financiar a estratégia de cibersegurança, não se dispõe de uma ideia precisa sobre que fundos vão para que destinos.

VII Numa altura em que as prioridades das políticas são crescentemente motivadas pela segurança, as **restrições quanto à atribuição dos recursos adequados às agências da UE com responsabilidades na cibersegurança** podem impedir a UE de concretizar as suas ambições. Para superar este desafio, é necessário descobrir formas de atrair e reter talentos.

Criação de ciber-resiliência

VIII Existem muitas insuficiências na governação da cibersegurança nos setores público e privado em toda a UE e a nível internacional, o que prejudica a capacidade de a comunidade internacional limitar os ciberataques e lhes dar resposta e cria obstáculos a uma estratégia coerente a nível da UE. O desafio é, portanto, **melhorar a governação da cibersegurança**.

IX O **reforço das competências e da consciencialização** em todos os setores e níveis da sociedade é fundamental, face à crescente escassez de competências em matéria de cibersegurança. De momento, existem poucas normas à escala da UE no que se refere a formação, certificação ou avaliação dos riscos de cibersegurança.

X Uma base de confiança é essencial para reforçar a ciber-resiliência geral e a própria Comissão considerou que a coordenação global ainda é insuficiente. **A melhoria do intercâmbio de informações e da coordenação** entre os setores público e privado continua a ser um desafio.

Resposta eficaz a ciberincidentes

XI Os sistemas digitais tornaram-se de tal modo complexos que é impossível impedir todos os ataques, sendo crucial para este desafio a **rapidez de deteção e resposta**. No entanto, a cibersegurança ainda não está plenamente integrada nos mecanismos vigentes a nível da UE para a coordenação da resposta a crises, o que pode limitar a sua capacidade de resposta a ciberincidentes transfronteiriços em grande escala.

XII É essencial **proteger as infraestruturas e funções societais de importância crítica**. As potenciais interferências nos processos eleitorais e as campanhas de desinformação são um desafio crucial.

XIII Os desafios que as ciberameaças colocam de momento à UE e ao mundo requerem o empenho contínuo e a adesão firme e permanente aos valores fundamentais da UE.

Introdução

01 A tecnologia está a desvelar todo um mundo novo de oportunidades. Novos produtos e serviços tornam-se parte integrante do nosso quotidiano à medida que vão surgindo. No entanto, com cada novo desenvolvimento aumenta a nossa dependência tecnológica e também a importância da cibersegurança. Quanto mais dados pessoais colocamos *online* e quanto mais ligados nos tornamos, mais provável é sermos vítimas de alguma forma de cibercriminalidade ou de ciberataque.

O que é a cibersegurança?

02 Não existe uma definição padrão e universalmente aceite de cibersegurança[1]. No sentido lato, abrange todas as garantias e medidas tomadas para defender os sistemas informáticos e os utilizadores de acessos não autorizados, ataques e danos, de forma a assegurar a confidencialidade, a integridade e a disponibilidade dos dados.

03 A cibersegurança implica prevenir e detetar ciberincidentes, reagir a eles e recuperar dos mesmos. Estes incidentes podem ser propositados ou não e vão desde, por exemplo, a divulgação acidental de informações até ataques a empresas e infraestruturas de importância crítica, passando pelo roubo de dados pessoais e até pela interferência nos processos democráticos. Todos eles podem ter amplos efeitos nocivos sobre as pessoas, as organizações e a sociedade.

04 Nos círculos de decisão política da UE, o termo cibersegurança não se limita à segurança das redes e das informações, abrangendo qualquer atividade ilícita que envolva a utilização de tecnologias digitais no ciberespaço. Por conseguinte, pode incluir cibercrimes como o lançamento de ataques de vírus informáticos e a fraude em pagamentos que não em numerário, mas também transpor a fronteira entre sistemas e conteúdo, como sucede com a divulgação *online* de material relacionado com o abuso sexual de menores. Pode ainda cobrir campanhas de desinformação que visam influenciar os debates *online*, bem como suspeitas de interferência eleitoral. Além disso, a Europol considera que a cibercriminalidade e o terrorismo são convergentes[2].

05 Os ciberincidentes são instigados por intervenientes distintos – incluindo Estados, grupos criminosos e "hacktivistas" – com motivações diversas. As consequências destes incidentes fazem-se sentir a nível nacional, europeu e mesmo mundial. No entanto, a natureza da Internet, intangível e em grande medida sem fronteiras, bem

como as ferramentas e táticas utilizadas dificultam muitas vezes a identificação do autor de um ataque (o chamado "problema da atribuição").

06 Os numerosos tipos de ameaças de cibersegurança podem ser classificados em função daquilo que fazem aos dados – divulgação, alteração, destruição ou negação de acesso – ou dos princípios basilares de segurança da informação que violam, como ilustrado na ***figura 1***. A ***caixa 1*** apresenta alguns exemplos de ataques. À medida que aumenta a sofisticação dos ataques aos sistemas informáticos, diminui a eficácia dos nossos mecanismos de defesa[3].

Figura 1 – Tipos de ameaças e princípios de segurança que estas colocam em risco

Fonte: TCE, modificado a partir de um estudo do Parlamento Europeu[4]. Cadeado = sem impacto na segurança; ponto de exclamação = risco para a segurança.

Caixa 1

Tipos de ciberataques

Sempre que um novo dispositivo se liga à Internet ou a outros dispositivos, aumenta a designada "superfície de ataque" de cibersegurança. O crescimento exponencial da Internet das coisas, a computação em nuvem, os megadados e a digitalização da indústria vêm acompanhados pelo aumento da exposição das vulnerabilidades, permitindo que intervenientes mal-intencionados visem cada vez mais vítimas. A variedade dos tipos de ataques e a sua crescente sofisticação fazem com que seja verdadeiramente difícil acompanhar o ritmo[5].

O ***malware*** (*software* malicioso) é concebido para provocar danos em dispositivos ou redes, podendo incluir vírus, cavalos de Troia, *ransomware* (*software* de sequestro), *worms* (vermes), *adware* (*software* de publicidade não solicitada) e *spyware* (*software* espião). O ***ransomware*** (*software* de sequestro) encripta os dados, impedindo que os utilizadores acedam aos ficheiros até que seja pago um resgate, geralmente numa criptomoeda, na falta do qual é desencadeada uma ação. Segundo a Europol, os ataques de *ransomware* são prevalentes a todos os níveis e houve uma explosão na variedade deste tipo de ataque nos últimos anos. Os **ataques distribuídos de negação de serviço** (DDoS), que tornam os serviços ou recursos indisponíveis através do envio em massa de mais pedidos do que esse serviço ou recurso consegue tratar, também estão a aumentar, tendo um terço das organizações enfrentado este tipo de ataques em 2017[6].

Os utilizadores podem ser manipulados para, involuntariamente, realizarem uma ação ou divulgarem informações confidenciais. Este ardil pode ser utilizado para o roubo de dados ou ciberespionagem e é conhecido como **engenharia social**. Existem diferentes formas de o conseguir, sendo um dos método mais comuns o ***phishing***, em que mensagens eletrónicas que aparentemente provêm de uma fonte fidedigna enganam os utilizadores e levam-nos a revelar informações ou clicar em ligações que infetam os dispositivos mediante o descarregamento de *malware*. Mais de metade dos Estados-Membros comunicou investigações sobre ataques a redes[7].

As ameaças mais nefastas são, possivelmente, as **ameaças persistentes avançadas**, em que agressores sofisticados se envolvem a longo prazo na vigilância e roubo de dados, por vezes também com intuitos destrutivos. A sua finalidade nestes casos é manterem-se discretos, sem serem detetados, durante o máximo de tempo possível. Estas ameaças estão muitas vezes associadas a Estados e visam setores particularmente sensíveis como a tecnologia, a defesa e infraestruturas de importância crítica. A ciberespionagem é tida como representando pelo menos um quarto de todos os ciberincidentes e a maioria das despesas[8].

O problema é grave?

07 É difícil apreender o impacto da falta de preparação para um ciberataque, pois não há dados fiáveis. O impacto económico da cibercriminalidade quintuplicou entre 2013 e 2017[9], atingindo tanto governos como empresas, de grande como de pequena dimensão. O crescimento previsto para os prémios de seguro de riscos cibernéticos, de 3 mil milhões de euros em 2018 para 8,9 mil milhões de euros em 2020, espelha esta tendência.

08 Ao mesmo tempo que o impacto financeiro dos ciberataques continua a crescer, existe uma disparidade alarmante entre o custo de lançar um ataque e o custo da prevenção, investigação e reparação. Por exemplo, um ataque DDoS pode custar apenas 15 euros por mês a realizar, mas as perdas incorridas pela empresa visada, incluindo os danos à reputação, são consideravelmente mais elevados[10].

09 Apesar de 80% das empresas da UE terem tido pelo menos um incidente de cibersegurança em 2016[11], a consciencialização sobre os riscos ainda é preocupantemente reduzida. Entre as empresas da UE, 69% não estão cientes da sua exposição a ciberameaças ou estão-no de forma limitada[12] e 60% nunca fizeram uma estimativa das potenciais perdas financeiras[13]. Além disso, de acordo com um inquérito global, um terço das organizações preferiria pagar um resgate ao criminoso informático do que investir na segurança da informação[14].

10 Os ataques à escala global do *ransomware* WannaCry e do *malware* de apagamento NotPetya, em 2017, atingiram em conjunto mais de 320 000 vítimas em cerca de 150 países[15]. Estes incidentes provocaram algo semelhante a um despertar global para a ameaça que os ciberataques representam, criando um novo ímpeto para integrar a cibersegurança na reflexão geral sobre as políticas. Além disso, 86% dos cidadãos da UE consideram agora que o risco de serem vítimas da cibercriminalidade está a aumentar[16].

A ação da UE em matéria de cibersegurança

11 Em 2001, a UE aderiu ao Comité do Conselho da Europa para a Convenção sobre a Cibercriminalidade (a Convenção de Budapeste)[17] na qualidade de observadora e, desde então, tem utilizado as políticas, a legislação e as despesas para reforçar a sua ciber-resiliência. No contexto de um crescente número de grandes ciberataques e incidentes, as atividades intensificaram-se a partir de 2013, como ilustrado pela

figura 2. Ao mesmo tempo, os Estados-Membros adotaram já (e, em alguns casos, já atualizaram) as suas primeiras estratégias nacionais de cibersegurança.

12 A *caixa 2* e o *anexo I* mencionam os principais intervenientes da UE com responsabilidades em matéria de cibersegurança.

Caixa 2

Quem intervém?

A **Comissão Europeia** pretende melhorar as capacidades e a cooperação em matéria de cibersegurança, tornar a UE num interveniente mais forte neste domínio e integrar a cibersegurança noutras políticas da UE. As principais Direções-Gerais (DG) com competências na política de cibersegurança são as DG **CNECT** (cibersegurança) e **HOME** (cibercriminalidade), responsáveis respetivamente pelo Mercado Único Digital e pela União da Segurança. A DG **DIGIT** é responsável pela segurança informática dos sistemas próprios da Comissão.

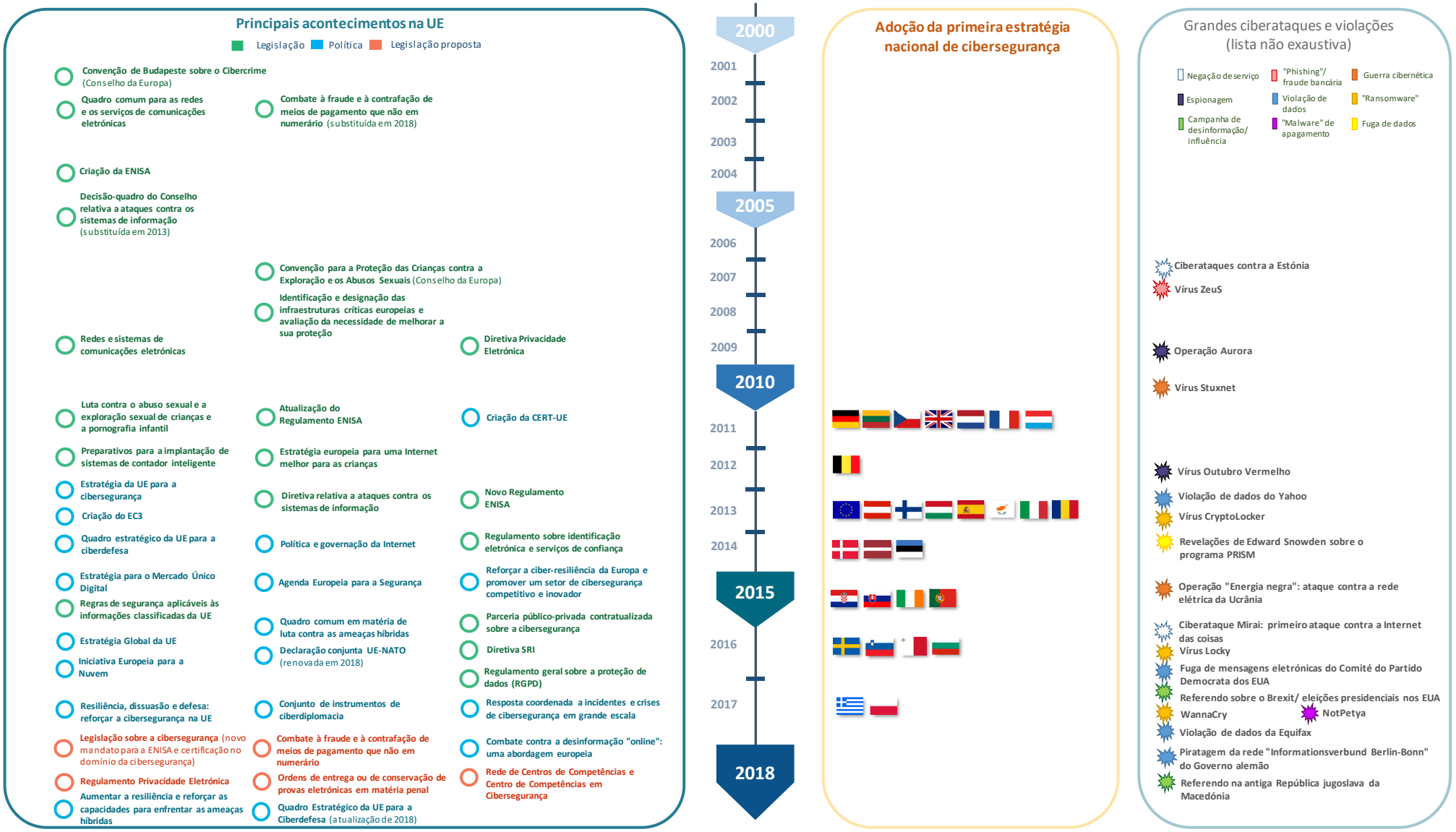
Várias agências da UE prestam apoio à Comissão, designadamente a **ENISA** (Agência da União Europeia para a Segurança das Redes e da Informação), que é a agência da UE para a cibersegurança – um órgão essencialmente consultivo que dá apoio ao desenvolvimento de políticas, ao reforço de capacidades e à sensibilização. O Centro Europeu da Cibercriminalidade da Europol (**EC3**) foi criado para reforçar a resposta das autoridades policiais da UE à cibercriminalidade. A Comissão acolhe ainda uma Equipa de Resposta a Emergências Informáticas (**CERT-UE**), que dá apoio a todas as instituições, organismos e órgãos da União.

O **Serviço Europeu para a Ação Externa** (SEAE) conduz a ciberdefesa, a ciberdiplomacia e a comunicação estratégica, albergando centros de recolha e análise de informações. A **Agência Europeia de Defesa** (AED) tem por finalidade desenvolver as capacidades de ciberdefesa.

Os **Estados-Membros** são os principais responsáveis pela sua própria cibersegurança e, a nível da UE, intervêm através do **Conselho**, que tem uma série de organismos de coordenação e partilha de informações (entre os quais o Grupo Horizontal das Questões do Ciberespaço). O **Parlamento Europeu** intervém enquanto colegislador.

As **organizações do setor privado**, incluindo as empresas, os organismos de governação da Internet e o meio académico, são ao mesmo tempo parceiros e contribuidores para o desenvolvimento e execução das políticas, nomeadamente através de uma **parceria público-privada contratualizada**.

Figura 2 – Intensificação da elaboração das políticas e da legislação (à data de 31 de dezembro de 2018)



Fonte: TCE.

Política

13 O ecossistema cibernético da UE é complexo e multifacetado, sendo transversal a várias políticas internas, como a justiça e os assuntos internos, o mercado único digital e a investigação. Em matéria de política externa, a cibersegurança está patente na diplomacia e é uma parte cada vez maior da nascente política de defesa da UE.

14 A pedra angular da política da UE é a **Estratégia para a Cibersegurança**, de 2013[18], cuja finalidade é tornar o ambiente digital da UE o mais seguro do mundo, defendendo, ao mesmo tempo, os valores e liberdades fundamentais. Tem cinco prioridades estratégicas: i) aumentar a ciber-resiliência; ii) reduzir a cibercriminalidade; iii) desenvolver a política e as capacidades no domínio da ciberdefesa; iv) desenvolver recursos industriais e tecnológicos para a cibersegurança; v) estabelecer uma política internacional em matéria de ciberespaço alinhada com os valores fundamentais da UE.

15 A Estratégia para a Cibersegurança está interligada com três estratégias adotadas posteriormente:

— a **Agenda Europeia para a Segurança** (2015) tem por finalidade melhorar a aplicação da lei e a resposta judicial ao fenómeno da cibercriminalidade, principalmente através da renovação ou atualização das políticas e da legislação em vigor[19]. Pretende ainda detetar os obstáculos às investigações penais sobre cibercriminalidade e estimular as iniciativas de reforço de capacidades em cibercriminalidade;

— a **Estratégia para o Mercado Único Digital**[20] (2015) visa melhorar o acesso a bens e serviços digitais, criando as condições adequadas para maximizar o potencial de crescimento da economia digital. Para este efeito, é essencial reforçar a segurança, a confiança e a inclusão na Internet;

— a **Estratégia Global** de 2016[21] tem por fim reforçar o papel da UE no mundo. A cibersegurança forma um pilar fundamental, graças a um compromisso renovado com as questões nesta matéria, à cooperação com os principais parceiros e à vontade de abordar essas questões em todos os domínios de intervenção, incluindo refutar a desinformação através de comunicação estratégica.

16 Nos últimos anos, o ciberespaço tem sido cada vez mais utilizado para fins militares[22] e apropriado enquanto arma[23], passando a ser encarado como o quinto teatro de guerra[24]. Os sistemas, redes e infraestruturas de importância crítica do ciberespaço são protegidos de ataques através de meios militares e outras medidas de

ciberdefesa. Em 2014, foi adotado um **Quadro Estratégico para a Ciberdefesa**, que foi atualizado em 2018[25]. Na versão atualizada de 2018, são definidas seis prioridades, entre as quais o desenvolvimento de capacidades de ciberdefesa e a proteção das redes de comunicação e informação da Política Comum de Segurança e Defesa (PCSD). A ciberdefesa faz igualmente parte do quadro de Cooperação Estruturada Permanente (CEP) e da cooperação UE-NATO.

17 O **quadro comum da UE em matéria de luta contra as ameaças híbridas** (2016) visa combater as ciberameaças dirigidas às infraestruturas de importância crítica e aos utilizadores privados, salientando que os ciberataques podem ser realizados por meio de campanhas de desinformação nas redes sociais[26]. Nesse documento, regista-se também a necessidade de aumentar o conhecimento sobre a situação e de melhorar a cooperação entre a UE e a NATO, que foi consubstanciada nas Declarações Conjuntas UE-NATO de 2016 e 2018[27].

18 Em 2017, a Comissão apresentou um novo pacote para a cibersegurança, refletindo a crescente urgência de assegurar a proteção digital. Desse pacote constava uma nova comunicação da Comissão que atualiza a estratégia para a cibersegurança de 2013[28] e um plano de ação para uma resposta rápida e coordenada a um ataque de grande envergadura e para a rápida aplicação da Diretiva relativa à segurança das redes e da informação (a Diretiva SRI)[29]. O pacote inclui, além disso, uma série de propostas legislativas (ver o ponto ***22***).

Legislação

19 Desde 2002, tem sido adotada legislação com importância variável para a cibersegurança.

20 Como principal pilar da estratégia para a cibersegurança de 2013, **a Diretiva SRI**[30], de 2016, é o elemento jurídico central e o primeiro ato legislativo à escala da UE em matéria de cibersegurança. A diretiva, com período de transposição até maio de 2018, visa alcançar um nível mínimo de harmonização de capacidades, obrigando os Estados-Membros a adotarem estratégias nacionais em matéria de segurança das redes e dos sistemas de informação e a criarem pontos de contacto únicos e equipas de resposta a incidentes de segurança informática (CSIRT)[31]. Além disso, estabelece requisitos de segurança e de notificação para os operadores de serviços essenciais em setores de importância crítica e para os prestadores de serviços digitais.

21 Paralelamente, em 2016 entrou em vigor o **Regulamento geral sobre a proteção de dados**[32] (RGPD), que é aplicável desde maio de 2018. O seu objetivo é proteger os dados pessoais dos cidadãos europeus, estipulando regras sobre o seu tratamento e divulgação. São conferidos determinados direitos aos titulares de dados e criadas obrigações por parte dos responsáveis pelo tratamento dos dados (prestadores de serviços digitais) sobre a utilização e transferência de informações. O Regulamento impõe igualmente requisitos de notificação em caso de violação e, em alguns casos, prevê a aplicação de coimas. A ***figura 3*** ilustra as complementaridades entre a Diretiva SRI e o RGPD quanto às respetivas finalidades de reforçar a cibersegurança e de salvaguardar a proteção dos dados.

22 Entre as propostas de legislação neste momento em debate estão a proposta de regulamento sobre a cibersegurança, com o fim de reforçar a ENISA e estabelecer um mecanismo de certificação à escala da UE[33], a proposta de regulamento sobre as ordens de entrega ou de conservação de provas eletrónicas[34] e a proposta de diretiva sobre as provas eletrónicas[35]. Faz ainda parte do pacote de 2017 sobre a cibersegurança a proposta de 2018 para a criação do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e da Rede de Centros Nacionais de Coordenação (a seguir designados por "centro de competências de investigação" e "rede de centros de competências em cibersegurança")[36].

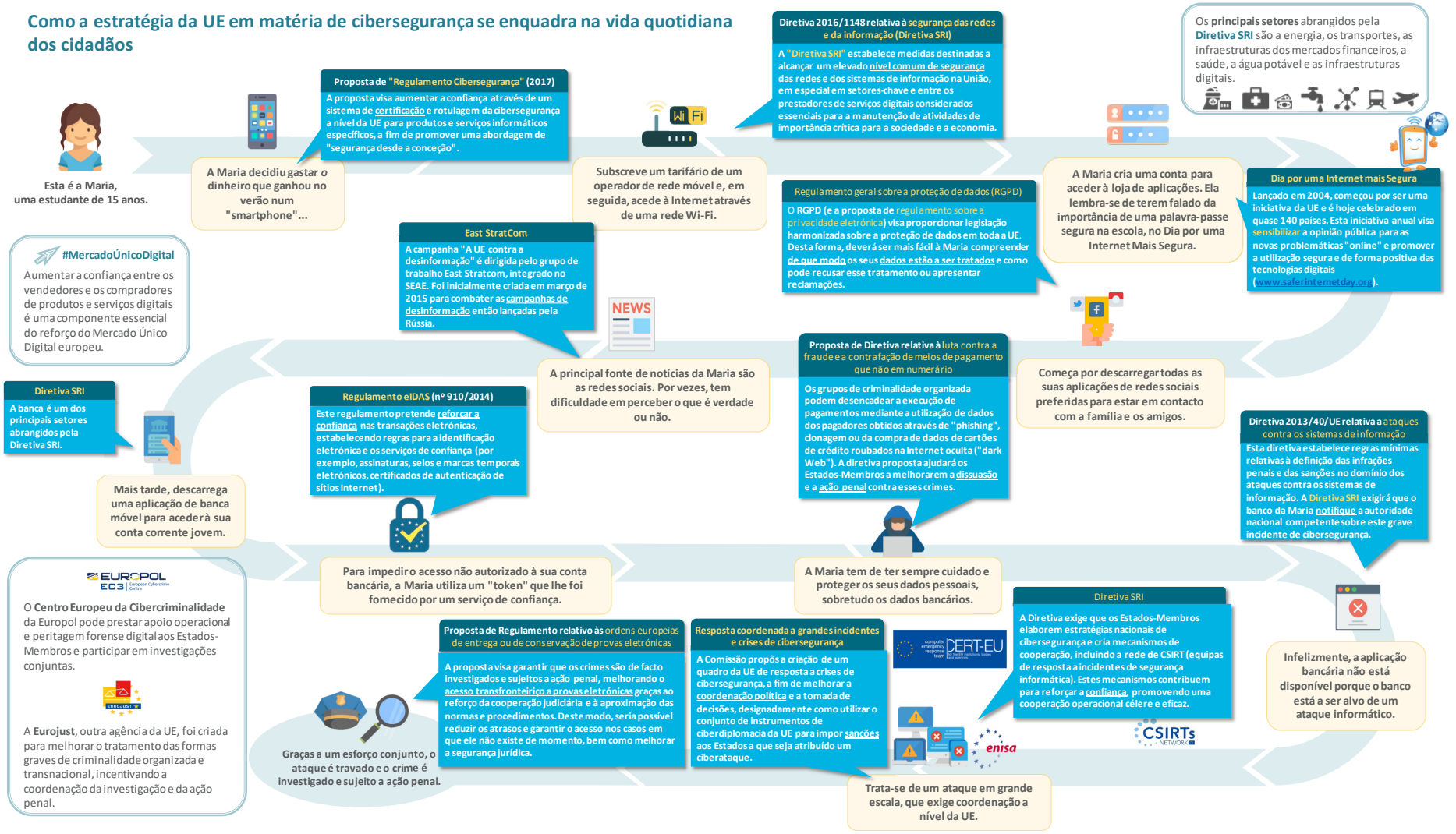
23 Pode ser difícil ter uma noção da amplitude do quadro estratégico e legislativo que se prende com a cibersegurança e a sua incidência na nossa vida quotidiana.

24 A ***figura 4*** é uma tentativa de delinear a forma como os diferentes diplomas legislativos e outras atividades interferem na vida de uma cidadã europeia fictícia.

Figura 3 – Complementaridades entre o RGPD e a Diretiva SRI

Fonte: TCE.

Figura 4 – Como a estratégia da UE em matéria de cibersegurança se enquadra na vida quotidiana dos cidadãos



Fonte: TCE.

Construir um quadro estratégico e legislativo

25 O ecossistema cibernético da UE é complexo e multifacetado, envolvendo muitos intervenientes (ver o ***anexo I***), e reunir todas as suas diferentes partes é um desafio considerável. Desde 2013, tem havido um esforço concertado para dar coerência ao domínio da cibersegurança na UE[37].

Desafio 1: proceder a uma verdadeira avaliação e prestação de contas

26 Como salientou a Comissão, é difícil estabelecer uma relação causal entre a estratégia de 2013 e eventuais mudanças observadas. Os objetivos da estratégia de 2013 foram formulados de forma muito geral, exprimindo uma visão e não uma meta quantificável[38]. Na ausência de objetivos mensuráveis, desenvolver medidas que se coadunem com estes objetivos genéricos constitui um desafio. A versão atual do quadro estratégico de ciberdefesa (2018) procura introduzir objetivos que estabeleçam o nível mínimo de cibersegurança e confiança a atingir. Estes, no entanto, limitar-se-ão à ciberdefesa, pois não foram estabelecidos objetivos que definam o nível desejado de resiliência para a UE como um todo.

27 Os efeitos raramente são medidos e poucos domínios de intervenção foram avaliados[39]. Esta situação deve-se em parte ao facto de a aplicação de muitas das medidas – legislativas ou outras – ser recente, o que dificulta uma avaliação completa do seu impacto. O desafio consiste em definir critérios de avaliação pertinentes que possam ajudar a medir esse impacto. Além disso, uma avaliação rigorosa ainda não se tornou prática geral em matéria de cibersegurança, sendo por isso necessária uma transição para uma cultura de desempenho com práticas de avaliação incorporadas e relatórios normalizados. O atual mandato da ENISA não abrange a avaliação e o acompanhamento do estado da cibersegurança da UE e do seu grau de preparação.

28 A elaboração fundamentada das políticas depende da disponibilidade de dados e estatísticas fiáveis em número suficiente para acompanhar e analisar as tendências e necessidades. A inexistência de um sistema de acompanhamento comum e obrigatório faz com que os dados fiáveis sejam escassos e, muitas vezes, os indicadores não se encontram disponíveis de imediato e são difíceis de definir[40]. Apesar disso, foram desenvolvidos indicadores específicos em certos domínios, designadamente o ciclo de políticas da UE contra a criminalidade grave e organizada.

29 Poucos Estados-Membros recolhem regularmente dados oficiais sobre questões relacionadas com a cibersegurança, o que prejudica a comparabilidade, tendo a UE dado poucas indicações até à data sobre a necessidade de consolidar as estatísticas a nível europeu[41]. Além disso, estão disponíveis poucas análises independentes a nível da UE que abranjam temas importantes como, por exemplo[42]: a economia da cibersegurança, incluindo a componente comportamental (o desalinhamento dos incentivos, as assimetrias de informação); a compreensão do impacto das falhas de cibersegurança e da cibercriminalidade; estatísticas agregadas sobre as tendências da cibersegurança e os desafios previstos; as melhores soluções para combater as ameaças.

30 Tendo em conta a falta de objetivos específicos e a escassez de dados fiáveis e de indicadores bem definidos, a avaliação dos resultados da estratégia tem sido até agora sobretudo qualitativa. Os relatórios intercalares descrevem frequentemente as atividades realizadas ou as metas alcançadas, sem procederem a uma quantificação aprofundada dos resultados, e ainda não foram criados cenários de referência para a avaliação da resiliência dos sistemas. Além disso, devido à ausência de uma definição de cibercriminalidade consignada num código, é praticamente impossível encontrar indicadores europeus pertinentes que contribuam para o seu acompanhamento e avaliação.

31 A supervisão independente da aplicação da política de cibersegurança difere entre os Estados-Membros. O Tribunal realizou um inquérito às instituições superiores de controlo nacionais sobre a sua experiência de auditoria neste domínio, tendo metade dos inquiridos que responderam[43] indicado que nunca realizaram auditorias sobre a matéria. Quanto aos que o tinham feito, as auditorias incidiram sobretudo sobre: a gestão da informação; a proteção das infraestruturas de importância crítica; o intercâmbio de informações e a coordenação entre as principais partes interessadas; o grau de preparação, notificação e resposta a incidentes. Os temas menos frequentemente abrangidos foram, por exemplo, as medidas de sensibilização e o défice de competências digitais. Os resultados dessas auditorias ou avaliações nem sempre são tornados públicos, sob justificações de segurança nacional. No ***anexo III*** é apresentada uma lista de relatórios de auditoria publicados pelas instituições superiores de controlo nacionais.

32 As limitações nas competências relacionadas com a cibersegurança (ver também os pontos ***82 a 90***) e as dificuldades para avaliar os progressos em matéria de cibersegurança foram consideradas como os principais desafios à auditoria das medidas dos governos neste domínio.

Desafio 2: colmatar as lacunas na legislação da UE e na sua desigual transposição

33 A rapidez com que surgem novas tecnologias e ameaças ultrapassa de longe o ritmo de conceção e aplicação da legislação da UE. Os procedimentos da União não foram concebidos com a era digital em mente: desenvolver metodologias inovadoras e flexíveis que garantam um quadro estratégico e jurídico adequado à sua finalidade[44] e permitam assim melhor antecipar e moldar o futuro é uma prioridade fundamental[45].

34 Apesar da procura de maior coerência, o quadro legislativo em matéria de cibersegurança continua incompleto (para alguns exemplos, ver o ***quadro 1***). A fragmentação e as lacunas dificultam a concretização dos objetivos globais das políticas e conduzem a ineficiências. Na sua avaliação da estratégia, a Comissão salientou, entre outras, insuficiências respeitantes à Internet das coisas, ao equilíbrio de responsabilidades entre os utilizadores e os fornecedores de produtos digitais e a alguns aspetos a que a Diretiva SRI não deu solução. A proposta de regulamento sobre a cibersegurança é uma tentativa de resolver em parte este problema, incentivando a segurança desde a conceção mediante um sistema de certificação à escala da UE. Algumas partes interessadas consideram que é gritante a ausência de uma abordagem comum à ciberespionagem e de uma política industrial claramente definida no domínio da cibersegurança[46].

Quadro 1 – Lacunas e transposição desigual do quadro legislativo (lista não exaustiva)

Domínio de intervenção	Exemplos
Mercado único digital	o A atual diretiva relativa à venda de bens de consumo não abrange a cibersegurança. As diretivas propostas sobre conteúdos digitais[47] e vendas *online*[48] visam colmatar esta lacuna. o Os quadros jurídicos dos Estados-Membros da UE relativos ao dever de diligência são limitados e distintos, dando origem a insegurança jurídica e a dificuldades na aplicação de mecanismos de recurso[49]. o As políticas sobre a divulgação das vulnerabilidades de *software* estão a ser desenvolvidas a diferentes ritmos pelos Estados-Membros, sem que exista um quadro jurídico comum a nível da UE que permita uma abordagem coordenada[50].
Reforço da segurança das redes e da informação	o Os Estados-Membros são livres de incluir setores omissos na Diretiva SRI[51]. O setor do alojamento, que não é abrangido, pode ser propício a outros crimes, incluindo o tráfico de estupefacientes e de seres humanos e a imigração clandestina[52].
Luta contra a cibercriminalidade	o Muitos Estados-Membros não estabeleceram ainda uma definição de prova eletrónica na legislação nacional[53] (ver igualmente o ponto ***22***). o A atual decisão-quadro relativa à fraude em pagamentos que não em numerário não menciona expressamente instrumentos de pagamento não físicos, tais como moedas virtuais, dinheiro eletrónico e pagamentos móveis, e não abrange crimes como o *phishing*, a clonagem e a posse e partilha de dados dos pagadores[54]. o A diretiva relativa a ataques contra os sistemas de informação não aborda diretamente a obtenção interna ilegal de dados (isto é, a ciberespionagem), levando a dificuldades em garantir a aplicação da lei[55]. o Na sequência do acórdão do Tribunal de Justiça da União Europeia sobre a conservação de dados[56], as diferenças entre os Estados-Membros na aplicação do quadro jurídico obstruíram a execução da lei, resultando na potencial perda de pistas de investigação e prejudicando a repressão penal efetiva da atividade criminosa *online*[57].

Fonte: TCE.

35 A aplicação de alguns aspetos da legislação continua a ser voluntária, tanto para as autoridades nacionais como para os operadores privados. No âmbito do Grupo de Cooperação, por exemplo, a avaliação das estratégias nacionais de segurança das redes e dos sistemas de informação e da eficácia das CSIRT é facultativa. Além disso, ao abrigo do sistema de certificação previsto na proposta de regulamento sobre a cibersegurança, o pedido de certificação de produtos e serviços informáticos será também facultativo.

36 Na UE, a cibersegurança é uma prerrogativa dos Estados-Membros. Não obstante, a UE tem um papel crucial a desempenhar na criação das condições para o reforço das capacidades dos seus Estados-Membros e para que estes colaborem e gerem confiança. No entanto, dadas as grandes diferenças entre os Estados-Membros em termos de capacidade e de empenho[58], a disponibilização de informações sensíveis (de segurança nacional) continuará a ser facultativa.

37 As diferenças na transposição do direito da União entre os Estados-Membros podem resultar em incoerência jurídica e operacional e impedem a legislação de concretizar todo o seu potencial. A título de exemplo, como os Estados-Membros têm interpretações divergentes sobre o modo de aplicação dos controlos das exportações de produtos de dupla utilização[59], é possível que algumas empresas sediadas na UE estejam a exportar tecnologias e serviços que podem ser utilizados para fins de cibervigilância e violação dos direitos humanos através de censura ou de interceção, uma situação sobre a qual o Parlamento Europeu manifestou a sua preocupação[60].

38 Além disso, proteger a privacidade e a liberdade de expressão exige uma resposta legislativa mais adaptada, a fim de encontrar o equilíbrio necessário entre a defesa dos valores fundamentais e o cumprimento dos imperativos de segurança da UE. Por exemplo, de que modo se pode garantir a encriptação de ponta a ponta e, ao mesmo tempo, encontrar a melhor maneira de apoiar a aplicação da lei? Ou como se pode alcançar os objetivos do RGPD e, em simultâneo, compreender as suas implicações sobre as informações acessíveis ao público acerca de quem regista nomes de domínio e acerca dos titulares de blocos de endereços IP? E de que forma pode este dilema prejudicar as investigações policiais[61]?

39 Por si só, a legislação não garante a resiliência. Embora a Diretiva SRI tenha por finalidade atingir um elevado nível de segurança em toda a UE, centra-se explicitamente em alcançar uma harmonização mínima e não máxima[62]. À medida que o ciberespaço evolui, continuarão a surgir lacunas.

Pontos de reflexão – quadro estratégico

- Quais os passos essenciais necessários para levar os decisores políticos a fazerem a transição para uma cultura mais orientada para o desempenho em matéria de cibersegurança, incluindo a definição da resiliência global?
- Qual a melhor forma de a investigação contribuir para gerar os dados e estatísticas necessários a uma verdadeira avaliação?
- Como se pode adaptar os processos legislativos da UE para que se tornem mais flexíveis e tenham melhor em conta a rapidez da evolução tecnológica e das ameaças?
- De que modo o processo de elaboração de parâmetros (indicadores, metas) do ciclo de políticas da UE pode ser adaptado, ampliado e reproduzido no domínio da cibersegurança no seu todo?
- O que podem as instituições superiores de controlo aprender com a forma como as suas congéneres auditam as políticas e medidas de cibersegurança?
- Que diferenças na transposição e aplicação do quadro jurídico da UE põem em causa uma resposta mais eficaz às lacunas em matéria de cibersegurança e cibercriminalidade, e qual a melhor forma de os Estados-Membros e a UE as superarem?
- Até que ponto os controlos da UE sobre as exportações de bens e serviços cibernéticos são eficazes para evitar violações dos direitos humanos fora da União?

Financiamento e despesas

40 A UE visa tornar-se no ambiente *online* mais seguro do mundo, uma ambição que exige esforços significativos de todas as partes interessadas e em particular uma base financeira sólida e bem gerida.

Desafio 3: adaptar os níveis de investimento aos objetivos

Aumentar o investimento

41 Estima-se que as despesas mundiais totais em cibersegurança sejam de cerca de 0,1% do PIB, um valor que, nos Estados Unidos[63], sobe para cerca de 0,35% (incluindo o setor privado). Em percentagem do PIB, as despesas públicas federais dos EUA são de cerca de 0,1%, o que equivale a cerca de 21 mil milhões de dólares orçamentados em 2019[64].

42 As despesas na UE têm sido comparativamente baixas, fragmentadas e frequentemente não são apoiadas por programas concertados a nível governamental. É difícil obter números, estimando-se contudo que as despesas públicas da UE em matéria de cibersegurança se situem entre um e dois mil milhões de euros por ano[65]. As despesas de alguns Estados-Membros, em percentagem do PIB, são de um décimo das dos EUA ou mesmo inferiores[66]. Para determinarem as lacunas a colmatar, a UE e os seus Estados-Membros precisam de saber o montante global de todos os seus investimentos.

43 É difícil ter uma visão abrangente porque não há dados claros, o que resulta da natureza transversal da cibersegurança e da impossibilidade de, muitas vezes, distinguir as suas despesas das despesas informáticas gerais[67]. O inquérito do Tribunal confirmou a dificuldade em obter estatísticas fiáveis sobre as despesas em ambos os setores público e privado. Três quartos das instituições superiores de controlo declararam que não tinham uma visão geral centralizada das despesas públicas relacionadas com o ciberespaço e nenhum Estado-Membro exigia que as entidades públicas comunicassem as despesas de cibersegurança separadamente nos seus planos financeiros.

44 Aumentar o investimento público e privado nas empresas de cibersegurança da Europa é, em especial, um desafio. Muitas vezes, está disponível capital público para as fases iniciais, mas isso sucede com menos frequência nas fases de crescimento e de

expansão[68]. A UE dispõe de numerosas iniciativas de financiamento que, no entanto, não estão a ser aproveitadas, em grande parte devido à burocracia[69]. Em geral, o desempenho das empresas de cibersegurança europeias é inferior ao das suas congéneres internacionais: sendo em menor número, o nível médio de financiamento que conseguem angariar é significativamente mais baixo[70]. Garantir que se visam e financiam com eficácia as empresas em fase de arranque é, por conseguinte, crucial para atingir os objetivos da política digital da UE.

Amplificar o impacto

45 Colmatar o défice de investimento no ciberespaço deve produzir resultados úteis. Por exemplo, apesar de a UE ter um setor da investigação e inovação forte, os seus resultados não conduzem com frequência suficiente a patentes, à comercialização ou ao aumento de escala de forma a reforçar a resiliência, a competitividade e a autonomia digital[71]. Esta situação é particularmente verdadeira quando comparada com a dos concorrentes da UE a nível mundial. A escassez de resultados devidamente aproveitados resulta de uma série de fatores[72], designadamente:

- a ausência de uma estratégia transnacional coerente capaz de amplificar a abordagem, de modo a responder às necessidades digitais mais vastas da UE em termos de competitividade e maior autonomia;
- a duração do ciclo da cadeia de valor, o que significa que os instrumentos se tornam rapidamente obsoletos;
- a falta de sustentabilidade, pois os projetos normalmente terminam com a dissolução da equipa do projeto e a cessação do apoio, incluindo as atualizações e o *patching* (remendo).

46 A proposta da Comissão de criar uma rede de centros de competências em cibersegurança e um centro de competências de investigação é uma tentativa de superar a fragmentação na área da investigação em cibersegurança e de estimular o investimento a uma escala maior[73]. No total, existem cerca de 665 centros especializados em toda a UE.

Desafio 4: dispor de uma visão geral clara das despesas orçamentais da UE

47 É importante ter uma visão geral a nível central para garantir a transparência e melhorar a coordenação. Sem essa visão, é difícil para os decisores políticos

perceberem até que ponto as despesas correspondem às necessidades de modo a cumprirem os objetivos prioritários.

48 Não existe um orçamento específico para financiar a estratégia de cibersegurança. A nível da UE, as despesas neste domínio provêm antes do orçamento geral da União e do cofinanciamento dos Estados-Membros. A análise do Tribunal revela uma estrutura complexa de pelo menos dez diferentes instrumentos no quadro do orçamento geral da UE, sem que se disponha de uma ideia precisa sobre que fundos vão para que destinos (ver o ***anexo II***).

49 Por isso, ter uma visão geral clara das despesas numa matéria que é transversal a muitos domínios de intervenção é um desafio considerável. Os programas de financiamento são geridos por diferentes serviços da Comissão, cada qual com os seus próprios objetivos, regras e calendários. O cenário complica-se ainda mais ao ter em conta o cofinanciamento dos Estados-Membros, por exemplo no âmbito do Fundo para a Segurança Interna – Polícia[74].

Rastreabilidade das despesas em cibersegurança

50 No período de 2014-2018, a Comissão despendeu mais de 1,4 mil milhões de euros na aplicação da sua Estratégia[75], tendo atribuído a maior parte ao Horizonte 2020[76]. O financiamento deste programa é canalizado maioritariamente através do desafio "Sociedades Seguras" e dos projetos de "Liderança em tecnologias facilitadoras e industriais"[77]. O Tribunal constatou que tinham sido contratados 279 projetos no domínio da cibersegurança até setembro de 2018, com um financiamento total da UE de 786 milhões de euros[78]. A ***figura 5*** ilustra a tipologia dos projetos com base nessa análise.

Figura 5 – Projetos de investigação em cibersegurança contratados no quadro do Horizonte 2020 (em milhões de euros)

Fonte: TCE.

51 Em 2016, foi estabelecida uma parceria público-privada contratual para estimular o desenvolvimento do setor europeu da cibersegurança. A finalidade era canalizar 450 milhões de euros do programa Horizonte 2020 para esta parceria e angariar um montante adicional de 1,8 mil milhões de euros do setor privado até 2020. No período de 18 meses que decorreu até 31 de dezembro de 2017, foram concedidos 67,5 milhões de euros do Horizonte 2020 para a parceria e o setor privado investiu mil milhões de euros[79].

52 A luta contra a cibercriminalidade também é apoiada pelo Fundo para a Segurança Interna – Polícia, na forma de estudos, reuniões de especialistas e atividades de comunicação, num montante de perto de 62 milhões de euros entre 2014 e 2017. No quadro da gestão partilhada, os Estados-Membros podem ainda beneficiar de subvenções para equipamento, formação, investigação e recolha de dados, às quais recorreram 19 Estados-Membros, no montante de 42 milhões de euros.

53 Ao abrigo do Programa de Justiça, gerido pela DG JUST, os fundos de apoio à cooperação judiciária e ao funcionamento dos tratados de assistência jurídica mútua,

com uma incidência específica no intercâmbio eletrónico de dados e informações financeiras, ascenderam a 9 milhões de euros.

54 A Diretiva SRI estabelece explicitamente que as CSIRT devem dispor dos recursos adequados para executar eficazmente as suas atribuições[80]. Entre 2016 e 2018, foram disponibilizados anualmente 13 milhões de euros no âmbito do Mecanismo Interligar a Europa, a que os Estados-Membros podiam recorrer para ajudar a aplicar os requisitos da diretiva. Não foi realizado qualquer estudo para determinar as necessidades financeiras reais para que o grupo de cooperação e a rede de CSIRT tivessem impacto.

55 Parte dos custos operacionais das agências foi especificamente destinada a atividades de cibersegurança e combate à cibercriminalidade. É, todavia, difícil extrair dados exatos das informações disponíveis ao público.

56 A Convenção de Budapeste (ver o ponto ***11***) constituiu a espinha dorsal das despesas externas da UE no domínio da cibersegurança. No período de 2014-2018, a União despendeu cerca de 50 milhões de euros no reforço da cibersegurança além das suas fronteiras. Quase metade desta despesa foi realizada através do Instrumento para a Estabilidade e a Paz, destacando-se um grande projeto – o GLACY+, no montante de 13,5 milhões de euros – que visa reforçar as capacidades a nível mundial para elaborar e aplicar legislação em matéria de cibercriminalidade e intensificar a cooperação internacional[81]. A despesa realizada através de outros instrumentos financeiros da UE foi, em grande medida, orientada para os Balcãs Ocidentais[82] e para os países abrangidos pela política europeia de vizinhança. A título de exemplo, o projeto Cybercrime@EaP com os países da Parceria Oriental visa melhorar a cooperação internacional em matéria de cibercriminalidade e de provas eletrónicas.

Outras despesas em cibersegurança

57 Nem sempre é possível distinguir despesas específicas referentes a cibersegurança nos programas da UE:

- o financiamento do Horizonte 2020 também foi canalizado através da Empresa Comum "Componentes e Sistemas Eletrónicos para uma Liderança Europeia" (ECSEL) para sistemas físicos de cibersegurança. No entanto, o Tribunal não conseguiu determinar as despesas especificamente relacionadas com a cibersegurança nos 27 projetos de um montante total de 437 milhões de euros entre 2015 e 2016;

- no âmbito dos Fundos Europeus Estruturais e de Investimento, está disponível um montante máximo de 400 milhões de euros para despesas em cibersegurança e serviços de confiança, que abrange investimentos em segurança e proteção de dados com a finalidade de melhorar a interoperabilidade e a interconexão da infraestrutura digital, a identificação eletrónica e os serviços de confiança e privacidade.

58 No seu plano operacional de 2018, o Banco Europeu de Investimento anunciou a intenção de aumentar o financiamento nos domínios da tecnologia de dupla utilização, da cibersegurança e da segurança civil até um máximo de 6 mil milhões de euros ao longo de um período de três anos[83].

Perspetivas futuras

59 A componente de cibersegurança da proposta do novo programa Europa Digital[84] para o período de 2021-2027, dotada de 2 mil milhões de euros, destina-se a reforçar o setor da cibersegurança e a proteção societal global na UE, nomeadamente ao contribuir para assegurar a aplicação da Diretiva SRI. A proposta de uma rede de centros de competências em cibersegurança e de um centro de competências de investigação, que visa conduzir a uma abordagem simplificada, deverá constituir o principal mecanismo de execução das despesas da UE ao abrigo do programa Europa Digital.

60 As despesas no domínio da defesa provenientes do orçamento da UE aumentaram recentemente por via do Programa Europeu de Desenvolvimento Industrial no domínio da Defesa, com um montante de 500 milhões de euros a atribuir em 2019 e 2020[85]. Este programa visa melhorar a coordenação e a eficiência das despesas dos Estados-Membros neste domínio mediante incentivos ao desenvolvimento conjunto. O seu objetivo é gerar um total de 13 mil milhões de euros de investimento em capacidades de defesa após 2020 através do Fundo Europeu de Defesa, do qual uma parte abrange a ciberdefesa[86].

Desafio 5: atribuir os recursos adequados às agências da UE

61 Os três principais organismos no cerne da política da UE em matéria de cibersegurança – a ENISA, o EC3 da Europol e a CERT-UE (ver a ***caixa 2***) – enfrentam dificuldades em termos de recursos, numa altura em que as prioridades de políticas são cada vez mais motivadas pela segurança. Os recursos humanos e financeiros de

que as agências da UE dispõem atualmente não lhes permitem corresponder às expectativas[87].

62 Os pedidos de recursos adicionais feitos pelas agências para fazer face à crescente procura não foram integralmente satisfeitos, podendo pôr em causa o cumprimento (atempado) dos objetivos das políticas. A título ilustrativo:

- os parcos recursos foram um fator impeditivo para que a ENISA pudesse concretizar plenamente os seus objetivos em 2017[88]. No pacote de 2017, foram propostos recursos adicionais para corresponder ao seu novo mandato;

- a contratação de analistas e os investimentos em capacidades informáticas no EC3 da Europol não acompanharam o ritmo da procura[89]. Além disso, o grupo de missão "Ação Conjunta contra o Cibercrime" (J-CAT) do EC3 da Europol é constituído por peritos dos Estados-Membros e de países terceiros que prestam apoio a investigações assentes na recolha de informações, mas os custos são, em grande parte, suportados pelos Estados de origem, desencorajando o destacamento de um maior número de peritos. Foi concebido um destacamento temporário numa base casuística com algum financiamento da Europol ou do ciclo político da UE, de modo a permitir a participação de um maior número de países.

63 Algumas limitações existem por culpa das próprias agências. Boa parte do pessoal da CERT-UE e da ENISA é constituído por agentes contratuais, cujos procedimentos de recrutamento são normalmente lentos. Outras limitações, como atrair e conservar talentos, decorrem da incapacidade das agências para competirem com os salários do setor privado ou das fracas expectativas de progressão na carreira. Desta forma, a ENISA subcontratou muito do seu trabalho entre 2014 e 2016[90].

64 A escassez de pessoal e das ferramentas necessárias pode implicar riscos significativos, especialmente no que diz respeito à recolha de informações sobre ameaças. O volume de dados provenientes de fontes abertas e fechadas continua a crescer, existindo o risco de ultrapassar as capacidades dos analistas para examinarem adequadamente as ameaças. Sem a implantação das capacidades e dos instrumentos apropriados que permitam integrar e interligar esses dados, não se poderão obter informações sobre ameaças que possam ser utilizadas, partilhadas e analisadas em toda a UE[91].

Pontos de reflexão — financiamento e despesas

- Como podem a Comissão e os legisladores simplificar as despesas da UE no domínio da cibersegurança e adaptá-las mais explicitamente a objetivos claramente definidos?

- Como poderá ser suprida a insuficiência de recursos das agências da UE de uma forma global e que tenha em conta as necessidades e os objetivos da União?

- Que medidas estão a ser definidas a nível da UE e dos Estados-Membros para reduzir os obstáculos ao acesso das PME a capital de investimento destinado ao aumento da escala das suas atividades?

- Que resultados concretos e sustentáveis estão a ser alcançados pelos fundos do Horizonte 2020 para obter soluções de cibersegurança?

- De que modo estão os exercícios de reforço das capacidades da UE a aumentar essas capacidades além das suas fronteiras para se conformarem aos valores da União?

Construção de uma sociedade ciber-resiliente

65 A governação da cibersegurança envolve a gestão de ameaças e riscos, o reforço das capacidades e da consciencialização e a coordenação e o intercâmbio de informações, assentando numa base de confiança.

Desafio 6: reforçar a governação e as normas

Governação da segurança da informação

66 A governação da segurança da informação implica instituir estruturas e políticas que garantam a confidencialidade, integridade e disponibilidade dos dados. Mais do que uma mera questão técnica, exige uma verdadeira liderança, processos sólidos e estratégias adaptadas aos objetivos da organização[92]. Um seu subconjunto é a governação da cibersegurança, que abrange todos os tipos de ameaças relacionadas com o ciberespaço, designadamente ataques, violações ou incidentes orientados e sofisticados que são difíceis de detetar ou gerir.

67 Os modelos de governação da cibersegurança variam consoante os Estados-Membros e, dentro de cada um, a responsabilidade nesta matéria está frequentemente repartida entre muitas entidades. Estas diferenças podem entravar a cooperação que é necessária para dar resposta a incidentes transfronteiriços em grande escala e para o intercâmbio de informações sobre ameaças a nível nacional e – ainda mais – a nível da UE. O inquérito realizado pelo Tribunal às instituições superiores de controlo revelou que as insuficiências nos mecanismos de governação e na gestão dos riscos por parte das autoridades públicas eram consideradas como os maiores perigos.

68 Embora as consequências para as organizações do setor privado possam ser graves, existem muitas insuficiências na cibergovernação. Perto de nove em cada dez organizações afirmam ter uma função de cibersegurança que não satisfaz inteiramente as suas necessidades[93] e que os responsáveis pela cibersegurança estão muitas vezes a dois ou mais níveis hierárquicos de distância do conselho de administração[94].

69 As diretivas da UE relativas ao direito das sociedades não fixam requisitos específicos sobre a divulgação dos riscos de cibersegurança. Nos Estados Unidos, a *Securities and Exchange Commission* publicou recentemente orientações não vinculativas para ajudar as empresas cotadas a preparar a divulgação dos riscos e incidentes de cibersegurança[95]. O Comité Conjunto das Autoridades Europeias de Supervisão[96] alertou para o aumento dos riscos de cibersegurança e incentivou as instituições financeiras a corrigirem as fragilidades dos sistemas informáticos e a analisarem os riscos inerentes para a segurança da informação, a conectividade e a externalização[97].

70 O reforço da governação da segurança da informação é particularmente difícil nas PME pois, na maior parte das vezes, estas não têm capacidade para instalar sistemas adequados. As PME não dispõem de orientações adequadas para aplicar os requisitos em matéria de segurança da informação e de privacidade e para atenuar os riscos tecnológicos[98]. Por conseguinte, os principais desafios são compreender melhor as suas necessidades e proporcionar os incentivos e o apoio necessários.

71 A falta de um quadro de governação da cibersegurança coerente a nível mundial prejudica a capacidade de a comunidade internacional limitar os ciberataques e dar-lhes resposta. É importante, por conseguinte, construir um consenso sobre esse quadro de governação de modo a que esteja em consonância com os interesses e valores da UE[99]. As tentativas de estabelecer normas internacionais vinculativas para o ciberespaço estão a tornar-se cada vez mais problemáticas, como evidenciado em 2017 pela falta de consenso no âmbito do Grupo de Peritos Governamentais das Nações Unidas sobre o modo de aplicação do direito internacional às respostas dos Estados a incidentes.

72 Além disso, para dar mais substância aos seus planos em matéria de governação do ciberespaço, a UE formalizou seis ciberparcerias, visando estabelecer diálogos regulares sobre as políticas para criar um clima de confiança e áreas comuns de cooperação[100]. Os resultados são variáveis. De um modo geral, a UE ainda não pode ser considerada a nível internacional como um importante interveniente no domínio da cibersegurança, embora tenha reforçado o seu estatuto[101].

Segurança da informação nas instituições da UE

73 Cada instituição da UE tem as suas próprias regras de governação em matéria de segurança da informação, existindo um acordo interinstitucional que prevê assistência neste domínio por parte da Comissão às restantes instituições e organismos. Todos reconheceram a necessidade de reforçar as suas capacidades de cibersegurança e

abordagens de gestão dos riscos de forma coerente. Em 2020, a Comissão, o Conselho e o SEAE devem apresentar um relatório ao Grupo Horizontal das Questões do Ciberespaço sobre a governação em matéria de cibersegurança e os progressos alcançados na sua clarificação e harmonização nas instituições e organismos da UE[102].

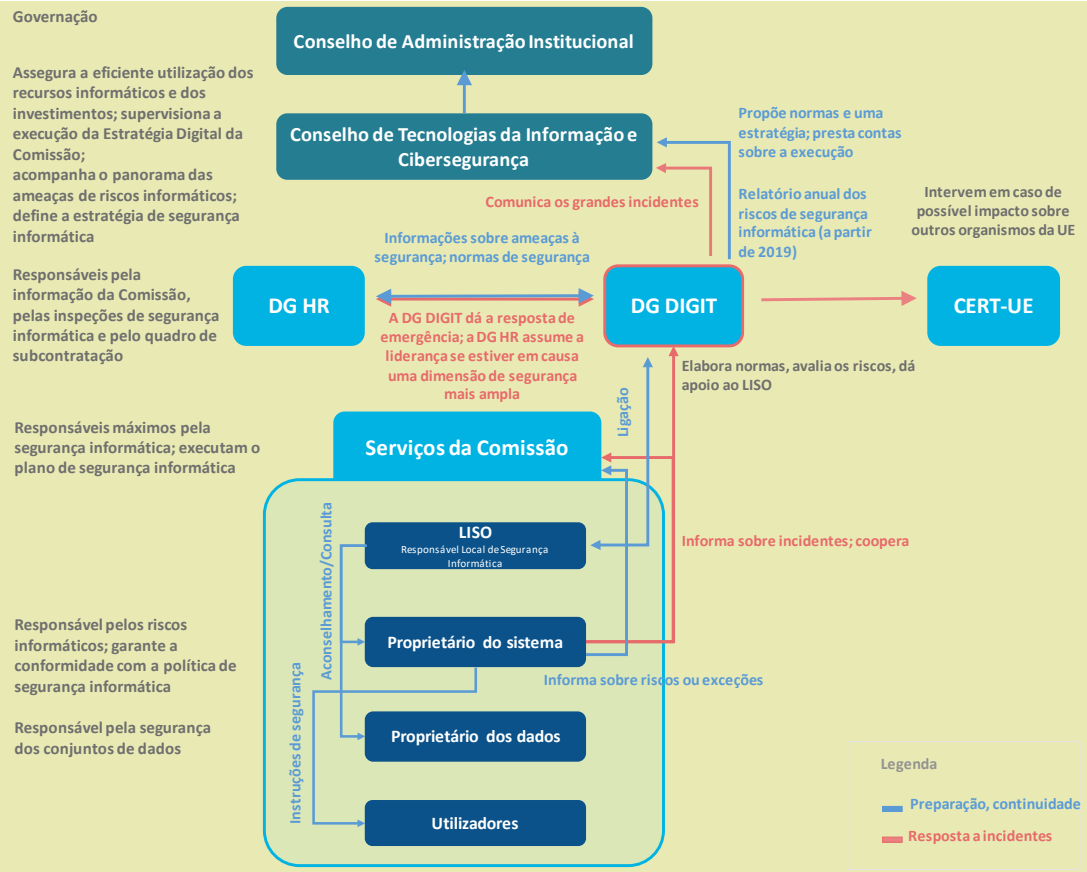
74 Na Comissão, a Direção-Geral da Informática (DG DIGIT) é responsável pela segurança da infraestrutura e serviços de informática (ver a ***caixa 3***). Os principais objetivos de segurança informática da Estratégia Digital da Comissão são: incorporar a segurança informática nos processos de gestão; proporcionar infraestruturas eficazes (em termos de custos) e resiliência; alargar o âmbito da deteção e resposta a incidentes; agregar a governação informática com a de segurança[103]. Nos termos do seu contrato enquanto fornecedor, a Comissão assegura que quase todo o *software* é ativamente mantido e que apenas é utilizado *software* em que existe assistência do fornecedor[104].

75 A importância de proteger as instituições estende-se também às missões e estruturas da Política Comum de Segurança e Defesa (PCSD) da UE em todo o mundo. Uma das prioridades do quadro estratégico de ciberdefesa da UE (na sua atualização de 2018) é aumentar a proteção dos sistemas de comunicação e informação utilizados por entidades da União no âmbito da PCSD. Foi instituído um conselho interno de cibergovernação no SEAE, que se reuniu pela primeira vez em junho de 2017[105].

Caixa 3

Proteção dos sistemas de informação da Comissão

Os cerca de 1 300 sistemas e 50 000 dispositivos da Comissão são constantemente alvo de ciberataques. A responsabilidade pelas tecnologias da informação é descentralizada, como ilustrado na figura seguinte. A segurança informática e da informação baseia-se num plano comum de segurança informática estabelecido pela DG DIGIT. O Conselho de Tecnologias da Informação e Cibersegurança age, na prática, enquanto Diretor da Segurança das Informações da Comissão, sendo o elo de ligação entre a vertente operacional da segurança informática e a gestão de topo da Comissão, representada pelo Conselho de Administração Institucional da Comissão.



Fonte: TCE, com base em decisões da Comissão[106].

A Direção-Geral dos Recursos Humanos e da Segurança tem como principal missão proteger o pessoal, as informações e os bens da Comissão. Também realiza investigações de segurança a incidentes cuja dimensão securitária seja mais vasta do que a informática, contribuindo assim para as suas atividades de contraespionagem e antiterrorismo.

A DG DIGIT é responsável pela segurança informática e alberga a Equipa de Resposta a Emergências Informáticas (CERT-UE). Criada em 2011, a CERT-UE gere um orçamento anual de cerca de 2,5 milhões de euros e tem cerca de 30 efetivos. Dá a resposta de emergência em qualquer incidente de segurança da informação que diga respeito a várias instituições, embora não esteja disponível em permanência, e acolhe uma plataforma de intercâmbio de informações. Em 2018, a CERT-UE assinou um memorando de entendimento não vinculativo com a ENISA, o EC3 e a Agência Europeia de Defesa para reforçar a cooperação e a coordenação, tendo também um acordo técnico com a capacidade de resposta a incidentes informáticos da NATO.

Avaliações das ameaças e dos riscos

76 Avaliações das ameaças e dos riscos contínuas e bem fundamentadas são ferramentas importantes tanto para organizações públicas como privadas. Porém, não existe uma abordagem normalizada para a classificação e o levantamento das

ciberameaças ou para a realização de avaliações dos riscos, fazendo com que o conteúdo dessas avaliações varie consideravelmente e dificultando, assim, uma abordagem coerente a nível da UE em matéria de cibersegurança[107]. Além disso, dependem muitas vezes das mesmas fontes ou mesmo de outras avaliações das ameaças, dando origem a uma câmara de eco que repete os mesmos resultados[108], com o risco de não dedicar suficiente atenção a outras ameaças. Esta situação é ainda agravada pela continuada relutância em partilhar informações e pela não comunicação de todos os incidentes.

77 A célula de fusão contra as ameaças híbridas[109], integrada no SEAE, foi criada com vista a melhorar o conhecimento da situação e apoiar a tomada de decisões através da partilha de análises, necessitando contudo de conhecimentos mais alargados, designadamente em matéria de cibersegurança. Paralelamente, a CERT-UE elabora relatórios e informações para as instituições e organismos da UE sobre ciberameaças a eles dirigidas.

78 A ENISA observou anteriormente que muitos Estados-Membros têm uma compreensão qualitativa das ameaças e que existe a necessidade de maior modelização das ciberameaças[110]. A capacidade de acompanhamento no âmbito da análise estratégica irá reforçar a compreensão global. No entanto, de modo a obter uma visão mais abrangente, as avaliações das ameaças poderiam abranger não só as de natureza tecnológica mas também as de cariz sociopolítico e económico, bem como os elementos condutores das ameaças e as motivações dos intervenientes.

Incentivos

79 Ainda não existem suficientes incentivos legais e económicos para que as organizações comuniquem e partilhem informações sobre incidentes. Por recearem danos à sua reputação, muitas organizações continuam a preferir lidar discretamente com os ciberataques ou pagar aos seus autores, permanecendo por averiguar a eficácia da Diretiva SRI no aumento do número de notificações. A Comissão prevê que as melhorias surjam essencialmente a nível nacional, mas o regulamento sobre a cibersegurança acrescentará uma perspetiva europeia[111].

80 Ao integrarem determinadas normas nos seus procedimentos de contratação, as autoridades públicas exercem uma influência significativa sobre os fornecedores, enquanto compradores de produtos e serviços digitais através de concursos públicos e enquanto financiadores da investigação e de programas (por exemplo, ao exigirem a aplicação de determinadas normas técnicas como o protocolo Internet IPv6, de modo

a contribuir para a luta contra a cibercriminalidade). De momento, contudo, não existe um quadro de contratação conjunto para as infraestruturas de cibersegurança[112], havendo muito que a Comissão pode fazer a este respeito. A proposta relativa ao programa Europa Digital para o próximo quadro financeiro plurianual visa aumentar o investimento do setor público na aquisição de tecnologias de cibersegurança, que até agora foi reduzido.

81 Através das suas competências regulamentares, a Comissão pode garantir que sejam elaboradas e aplicadas de forma generalizada normas adequadas para reforçar a segurança. A Comissão e a Europol colaboram com organismos de governação da Internet como a ICANN (ver o ponto ***38***) e o RIPE-NCC[113], o que é essencial para instituir a arquitetura adequada de combate à cibercriminalidade de modo a auxiliar as autoridades policiais e judiciárias.

Desafio 7: reforçar as competências e a consciencialização

82 A ENISA salientou que os utilizadores desempenham um papel essencial no combate aos ciberataques e que o reforço das competências, da educação e da consciencialização é a chave para construir uma sociedade ciber-resiliente[114]. Qualquer pessoa que, no local de trabalho ou em casa, saiba facilmente detetar os sinais de alerta e esteja munida das técnicas adequadas pode retardar ou impedir ataques.

83 Particularmente preocupante é a crescente assimetria entre os conhecimentos necessários para cometer um cibercrime ou lançar um ciberataque e as competências necessárias para se defender dele. O modelo "criminalidade como serviço" baixou as barreiras de entrada no mercado da cibercriminalidade: pessoas sem conhecimentos técnicos para construir *botnets*, *exploit kits* ou pacotes de *ransomware* podem agora alugá-los.

Formação, competências e reforço das capacidades

84 O mundo enfrenta uma crescente escassez de competências em matéria de cibersegurança, tendo o défice de mão-de-obra aumentado 20% desde 2015[115]. Os canais de recrutamento tradicionais não satisfazem a procura, incluindo para lugares de gestão e funções interdisciplinares[116]. Cerca de 90% da mão-de-obra no domínio da cibersegurança a nível mundial é do sexo masculino e a persistente falta de paridade entre sexos restringe ainda mais a reserva de talentos[117]. Além disso, nas universidades, as disciplinas relacionadas com a cibersegurança estão sub-representadas nos programas não técnicos.

85 É necessária formação e educação a todos os níveis, para os funcionários públicos, os agentes das forças policiais, as autoridades judiciais, as forças armadas e os educadores. Por exemplo, os tribunais têm de conseguir fazer face à rápida evolução das especificidades técnicas da cibercriminalidade e das vítimas[118], não existindo de momento quaisquer normas a nível da UE para a formação e a certificação neste domínio[119]. Nas instituições da UE, é importante dispor da combinação certa de competências. De outra forma, as instituições poderão não conseguir definir apropriadamente o âmbito, encontrar os parceiros adequados e determinar as necessidades de segurança ou não ter capacidade para gerir programas, o que poderá por seu turno prejudicar a eficácia dos programas da UE e a elaboração das suas políticas.

86 Embora os Estados-Membros sejam responsáveis pelas políticas de educação, a nível da UE estão já em curso numerosas ações de formação (ver o ***quadro 2***) e exercícios (ver a ***caixa 4***). A UE pode contribuir para introduzir normas europeias nos programas de ensino em todas as disciplinas pertinentes[120]. No domínio da investigação forense digital, por exemplo, são necessárias normas comuns de formação para abrir a via à admissibilidade de provas nos Estados-Membros. Devido à natureza transfronteiriça da cibercriminalidade, podem estar em causa múltiplas jurisdições, o que exige formação a nível da UE. Apesar disso, a CEPOL, a Agência da UE para a Formação Policial, observou que mais de dois terços dos Estados-Membros não disponibilizam regularmente formação em cibersegurança aos agentes das forças policiais[121]. A UE também pode encontrar formas de criar sinergias em matéria de educação e formação entre as esferas civil e militar[122]. Nestes termos, a ENISA concluiu que, embora existam atualmente vastas oportunidades de formação em setores essenciais, estas não visam suficientemente a resiliência das infraestruturas de importância crítica[123].

Quadro 2 – Exemplos de iniciativas de formação da UE em matéria de cibersegurança

Projetos da Agência Europeia de Defesa, por exemplo o apoio a exercícios do setor privado e o projeto sobre plataformas virtuais de formação cibernética	Rede da Academia Europeia de Segurança e Defesa (que disponibiliza formação civil e militar), incluindo educação em cibersegurança, exercícios de formação e uma plataforma de avaliação	Formação da ENISA, que proporciona programas de formação que o mercado poderá não disponibilizar
Programas de formação da Europol, da CEPOL e do ECTEG[124] – incluindo formações sobre o modelo de governação e o quadro de competências (incluindo a certificação)	Rede de Centros de Competências em Cibersegurança e Centro de Competências de Investigação (proposta)	Medidas sobre a encriptação propostas no 11º relatório intercalar sobre a União da Segurança
Cooperação UE-NATO em matéria de formação e educação em ciberdefesa	Programa Erasmus militar	Rede Europeia de Formação Judiciária

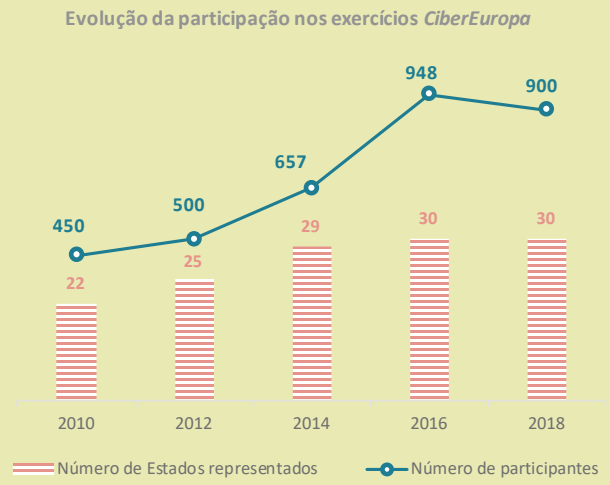
Fonte: TCE.

87 A UE destacou especialistas em combate ao terrorismo e segurança para 17 delegações, visando reforçar a ligação entre a segurança interna e externa da UE[125]. Não obstante as limitações de recursos, dispor de mais conhecimentos em cibersegurança pode ajudar a pôr em prática os projetos adequados e a encontrar as sinergias com outros programas ou fontes de financiamento[126]. Pode também aumentar a visibilidade da cibersegurança no diálogo político, embora esta tenha de competir com muitas outras prioridades, tais como a migração, a criminalidade organizada ou o regresso de combatentes estrangeiros.

Caixa 4

Exercícios

Os exercícios são elementos importantes da educação e formação no domínio do ciberespaço, oferecendo oportunidades privilegiadas para aumentar o grau de preparação ao testar as capacidades, dar respostas a cenários da vida real e criar redes de relações de trabalho. Desde 2010, a sua frequência aumentou consideravelmente.



Fonte: TCE, com base em documentos da ENISA.

Os intervenientes participam no local ou à distância. São realizadas avaliações *a posteriori* para retirar ensinamentos, embora estes possam ainda não estar a interpenetrar-se completamente entre os níveis estratégico/político, operacional e técnico[127].

Os exercícios emblemáticos da UE e da NATO – o exercício bienal CiberEuropa (operacional) e o anual *Locked Shields* (técnico) – reúnem mais de 1 000 participantes de cerca de 30 países. Ambos se centram na proteção e manutenção das infraestruturas de importância crítica em cenários de ataque simulados. Estes exercícios tornaram-se consideravelmente mais profundos e ambos incluem agora elementos relacionados com as políticas mediática, jurídica e financeira, visando melhorar o conhecimento da situação por parte dos profissionais. Os exercícios paralelos e coordenados PACE testam a interação UE-NATO num cenário de crise híbrida.

Estes não são os únicos exercícios internacionais. A ENISA organiza anualmente um desafio de cibersegurança em que as equipas concorrem entre si para resolver desafios em matéria de segurança, por exemplo de segurança da Internet e dos dispositivos móveis, quebra-cabeças de encriptação, engenharia inversa, ética e ciência forense. O primeiro exercício a nível ministerial, o EU CYBRID, teve lugar em setembro de 2017 e incidiu sobre a tomada de decisões estratégicas. Em 2018, foi lançado o exercício *Crossed Swords*, no quadro da NATO, para melhorar os elementos ofensivos do seu exercício *Locked Shields*. A NATO organiza ainda os exercícios *Cyber Coalition*.

Uma das principais dificuldades é assegurar a participação ativa de todos as partes interessadas importantes e a coordenação de todos os exercícios para evitar a duplicação e partilhar a experiência adquirida de forma eficiente.

Consciencialização

88 Os cidadãos são frequentemente o veículo de ataques e da disseminação da desinformação, pois podem ser involuntariamente expostos às vulnerabilidades de *software* ou dispositivos baratos e amplamente distribuídos ou ser vítimas de engenharia social. Por conseguinte, a sensibilização é fundamental para construir uma ciber-resiliência eficaz mas não é, de todo, uma tarefa fácil, pois os não especialistas têm dificuldade em compreender a complexidade da cibersegurança e os riscos associados.

89 São exemplos de campanhas de sensibilização o Dia por uma Internet Mais Segura e o Mês Europeu da Consciencialização para a Cibersegurança, ao qual já aderiram sete países terceiros[128]. A campanha da Europol *Say No!* (Diz Não!) pretende reduzir o risco de as crianças serem vítimas de extorsão e coação sexual na Internet, algo que é importante porque, de momento, poucas vítimas denunciam estes crimes à polícia[129]. A Comissão reconhece que a estratégia de cibersegurança foi apenas parcialmente eficaz na sensibilização dos cidadãos e das empresas[130], devido à envergadura da tarefa, à escassez de recursos, ao desigual empenho dos Estados-Membros e à falta de provas científicas sobre a melhor forma de aumentar e medir o nível de consciencialização.

90 O desafio para a Comissão e as agências competentes é garantir que as medidas de sensibilização são bem orientadas e publicitadas, são inclusivas e adaptadas à natureza das ameaças, evitam efeitos não intencionais como a "fadiga da segurança"[131] e desenvolvem métodos e métricas de avaliação da sua eficácia. Estes critérios devem aplicar-se em igual medida no interior das próprias instituições da UE, onde é necessário melhorar a cultura de consciencialização[132].

Desafio 8: melhorar o intercâmbio de informações e a coordenação

91 A cibersegurança exige a cooperação entre os setores público e privado, principalmente em termos do intercâmbio de informações e da partilha de boas práticas. A confiança é indispensável a todos os níveis para criar o ambiente adequado para a partilha de informações sensíveis além das fronteiras. Uma fraca coordenação conduz à fragmentação, à duplicação de esforços e à dispersão das competências. Uma coordenação eficaz pode resultar em sucessos tangíveis, como o encerramento de mercados da Internet oculta[133]. Apesar dos progressos alcançados nos últimos anos, os níveis de confiança continuam a ser insuficientes[134] a nível da UE e em alguns Estados-Membros[135].

Coordenação entre as instituições da UE e com os Estados-Membros

92 Um dos objetivos da estratégia de cibersegurança e das estruturas de cooperação introduzidas pela Diretiva SRI foi reforçar a confiança entre as partes interessadas. Apesar de, na avaliação da estratégia, se ter reconhecido que tinham sido criadas as bases de uma cooperação estratégica e operacional a nível da UE[136], a coordenação é, em geral, insuficiente[137]. O desafio consiste em assegurar que o intercâmbio de informações é não apenas pertinente, mas que também permite obter uma visão de conjunto. A este respeito, chegar a um entendimento comum sobre a terminologia aceite é um fator importante (ver a ***caixa 5***).

93 Na avaliação da ENISA salientou-se, contudo, que a abordagem da UE à cibersegurança não estava suficientemente coordenada, levando à falta de sinergias entre as atividades desta agência e as de outras partes interessadas. Os mecanismos de cooperação ainda estão relativamente pouco desenvolvidos[138], uma questão que o Regulamento sobre a cibersegurança visa corrigir ao reforçar o papel de coordenação da ENISA. O desejo de reforçar a cooperação foi a lógica subjacente ao memorando de entendimento assinado em 2018 entre a ENISA, a AED, o EC3 da Europol e a CERT-UE[139]. Uma prioridade da Comissão para os próximos anos será assegurar a adequada harmonização entre as iniciativas das políticas, as necessidades e os programas de investimento, de modo a superar a fragmentação e criar sinergias[140].

94 As funções de coordenação estão incorporadas em vários organismos institucionais. O Grupo de Trabalho sobre a União da Segurança foi criado para desempenhar um papel central na coordenação das diferentes Direções-Gerais da

Comissão com vista a apoiar os planos da União da Segurança[141]. O subgrupo de trabalho sobre cibersegurança é presidido pela DG CNECT.

95 No Conselho, a cibersegurança está a cargo do Grupo Horizontal das Questões do Ciberespaço, que coordena as questões estratégicas e horizontais nesta matéria e contribui para a preparação de exercícios e avaliação dos seus resultados. Este grupo colabora de perto com o Comité Político e de Segurança, que tem um papel decisório central no respeitante a todas as medidas diplomáticas no âmbito do ciberespaço (ver a ***caixa 6*** no capítulo seguinte). Uma vez que a cibersegurança é um tema de natureza transversal, a coordenação de todos os interesses pertinentes não é simples: pelo menos 24 grupos de trabalho e instâncias preparatórias lidaram recentemente com questões nessa matéria[142].

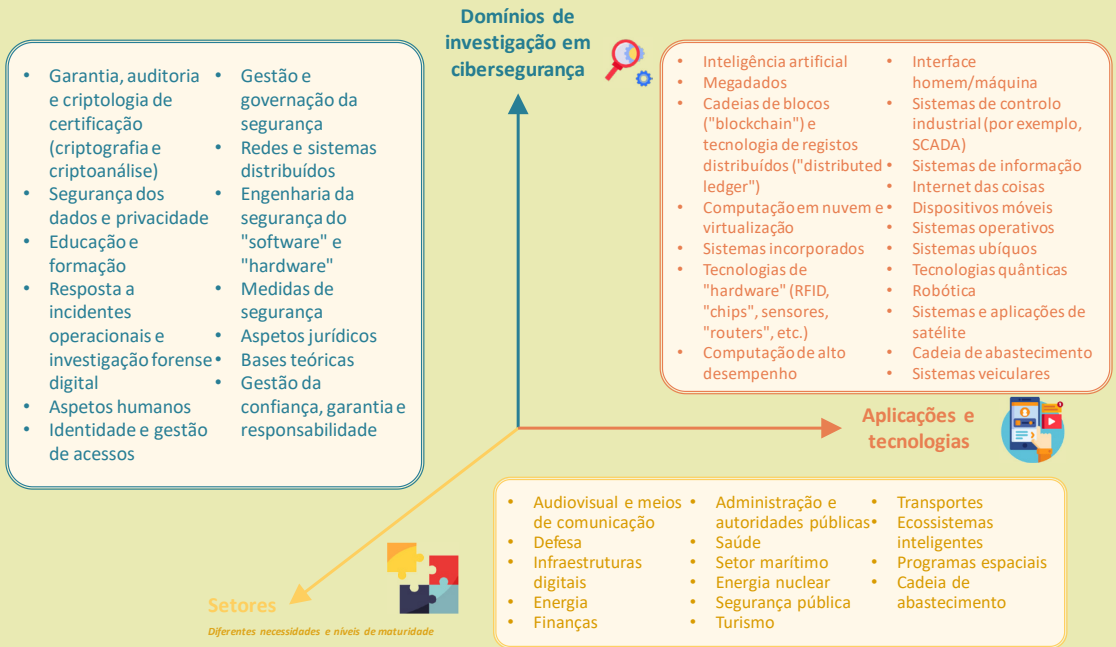
96 As duas mais recentes propostas legislativas sobre o reforço da ENISA (2017) e a criação de uma rede de centros de competências em cibersegurança e de um centro de competências de investigação (2018) destinam-se especificamente a corrigir a fragmentação e a duplicação de esforços. A rede e o centro surgiram devido à necessidade de colmatar a lacuna que não foi preenchida pelas estruturas de cooperação da Diretiva SRI, pois não foram concebidas para apoiar o desenvolvimento de soluções de ponta.

Caixa 5

Tentativa de falar a mesma ciberlíngua: *coerência tecnológica*

A clareza terminológica melhora o conhecimento da situação e a coordenação[143], além de ajudar a determinar com precisão o que constitui uma ameaça e um risco.

O Centro Comum de Investigação (JRC) da Comissão elaborou recentemente uma versão revista da taxonomia de investigação a partir de diferentes normas internacionais[144], com a finalidade de se tornar um ponto de referência para utilização como índice remissivo por entidades de investigação em toda a Europa.



Fonte: TCE, adaptado a partir de informações da Comissão Europeia.

Até há pouco tempo, as instituições e organismos da UE não dispunham de definições comuns, uma realidade que está a mudar. No âmbito do seu plano de ação, o grupo de cooperação elaborou uma taxonomia de incidentes que visa facilitar a eficiência da colaboração transfronteiriça.

Cooperação e intercâmbio de informações com o setor privado

97 A cooperação entre as autoridades públicas e o setor privado é essencial para reforçar os níveis globais de cibersegurança. Não obstante, na sua avaliação de 2017 sobre a estratégia de cibersegurança, a Comissão concluiu que o intercâmbio de informações entre as partes interessadas privadas e entre os setores público e privado ainda não era o melhor, devido à ausência de mecanismos de comunicação de confiança e de incentivos ao intercâmbio de informações[145], impedindo a realização dos objetivos estratégicos. A Comissão observou também a ausência de um mecanismo de cooperação eficiente para os Estados-Membros trabalharem em conjunto no reforço estratégico de capacidades industriais duradouras com economias de escala[146].

98 Os centros de partilha e análise de informações são organismos criados para disponibilizar plataformas e recursos que facilitem o intercâmbio de informações entre os setores público e privado e para recolher informações sobre ciberameaças. Destinam-se a reforçar a confiança, através da partilha de experiências, conhecimentos e análises, especialmente sobre causas profundas, incidentes e ameaças. Já existem centros de partilha nacionais e setoriais em muitos Estados-Membros, mas o seu número a nível europeu é ainda relativamente reduzido[147]. Estes centros têm associados, no entanto, vários desafios (condicionalismos de recursos, dificuldades em avaliar o seu êxito, criação das estruturas adequadas ao envolvimento dos setores público e privado, envolvimento das autoridades policiais) que terão de ser ultrapassados antes de poderem contribuir para a execução da Diretiva SRI e para a construção de capacidades de segurança à escala europeia[148].

99 Uma cooperação estreita com o setor privado é particularmente importante para combater a cibercriminalidade complexa, mas a sua eficiência é desigual entre os Estados-Membros e depende do nível de confiança[149]. Apesar disso, o EC3 da Europol criou uma série de grupos consultivos com operadores do setor privado, instituições e organismos da UE e outras organizações internacionais, visando melhorar a colaboração através da criação de redes, da partilha de informações estratégicas e da cooperação. Estes grupos trabalham em planos harmonizados com os objetivos do ciclo político da UE[150]. A utilização criminosa da encriptação é outra área plena de desafios que exigem maior cooperação com o setor privado. O EC3 da Europol está atualmente a examinar diferentes opções para acolher destacamentos – de curto prazo e específicos para cada caso – de peritos do setor privado e do meio académico junto do grupo de missão da Europol "Ação Conjunta contra o Cibercrime" (ver o ponto ***62***).

100 A falta de mecanismos de cooperação eficientes afeta as comunidades civis e de defesa, tanto públicas como privadas. Os domínios que colocam um desafio comum incluem a criptografia, sistemas seguros incorporados, a deteção de *malware*, técnicas de simulação, a proteção de redes e de sistemas de comunicação e as tecnologias de autenticação. A promoção da cooperação entre os civis e os militares e o apoio à investigação e à tecnologia (em especial através de incentivos às PME) são duas das prioridades do quadro estratégico de ciberdefesa da UE (na sua versão atualizada de 2018).

Pontos de reflexão — Reforçar a resiliência

- Como obter um equilíbrio adequado a nível da UE entre a necessidade de dar importância à política de cibersegurança e de assegurar uma coordenação eficiente entre os vários intervenientes e a dispersão das responsabilidades?
- Qual o grau de preparação das instituições e organismos da UE para o próximo grande ataque que lhes for lançado diretamente?
- Como tornar os organismos da UE com responsabilidades na cibersegurança mais atrativos para os talentos?
- Que medidas adicionais são necessárias para assegurar as capacidades adequadas em todas as instituições e organismos da UE, de modo a disporem de um quadro coerente de avaliação dos riscos e ameaças?
- De que forma estão as autoridades europeias de supervisão (a Autoridade Bancária Europeia, a Autoridade Europeia dos Valores Mobiliários e dos Mercados e a Autoridade Europeia dos Seguros e Pensões Complementares de Reforma) a responder às vulnerabilidades de cibersegurança inerentes ao setor financeiro, e que lições podem ser retiradas para outros setores?
- Dado o défice global de competências especializadas, como utilizar da melhor forma a assistência técnica que a UE concede às autoridades públicas para a obter o máximo impacto global no reforço da ciber-resiliência?
- Como podem a UE e os Estados-Membros assegurar uma participação significativa nos debates internacionais que permita moldar a governação e as normas do ciberespaço e promover os valores da UE?
- Que medidas de sensibilização a nível da UE e dos Estados-Membros (incluindo os esforços de prevenção) estão a fazer realmente a diferença, e o que pode a UE fazer para aumentar a sua escala?
- Qual poderá ser o papel da UE na contribuição para a paridade entre sexos no domínio da cibersegurança?
- De que forma poderão a UE e os Estados-Membros melhorar as sinergias entre as comunidades civis e de defesa, em consonância com o quadro estratégico de ciberdefesa (na sua versão atualizada de 2018)?

Resposta eficaz a ciberincidentes

101 Conceber uma resposta eficaz aos ciberataques é fundamental para os deter o mais cedo possível. É particularmente importante que os setores de importância crítica, os Estados-Membros e as instituições da UE sejam capazes de reagir de forma rápida e coordenada, sendo a deteção precoce essencial para esse fim.

Desafio 9: aumentar a eficácia na deteção e resposta

Deteção e notificação

102 Embora os instrumentos de deteção comuns ajudem a frustrar diariamente a grande maioria dos ataques[151], os sistemas digitais tornaram-se de tal modo complexos que é impossível impedi-los todos. A sua sofisticação faz com que iludam frequentemente a deteção por períodos prolongados, levando os peritos a afirmar que a tónica deve ser colocada na deteção e defesa rápidas[152]. No entanto, alguns instrumentos de deteção – tais como a automatização, a aprendizagem automática e a análise comportamental, que procuram reduzir os riscos e analisar e aprender com o comportamento do sistema – sofrem de baixas taxas de aplicação por parte das empresas[153]. Esta situação deve-se, em parte, à geração de falsos positivos, em que atividades inócuas são erradamente tomadas por maliciosas.

103 Quando uma violação é detetada e analisada, é necessário um processo rápido de notificação e comunicação de informações, para que outras entidades públicas e privadas possam tomar medidas preventivas e para que as autoridades competentes possam dar apoio aos afetados. Muitas organizações têm relutância em admitir e comunicar ciberincidentes[154]. O envolvimento precoce das autoridades policiais na resposta inicial a suspeitas de cibercrimes e a partilha proativa de informações com as CSIRT é igualmente essencial.

104 A anterior falta de requisitos comuns a nível da UE sobre a notificação de incidentes conduzia ao risco de atrasos na comunicação de violações e a obstáculos na resposta, uma situação que a introdução da Diretiva SRI pretendia resolver (ver o ponto ***20***). Na sequência dos ataques do WannaCry, em 2017, a Comissão concluiu que o sistema da rede de CSIRT "ainda não estava plenamente operacional"[155]. Dado que a diretiva está em processo de aplicação, ainda não é possível perceber se as orientações elaboradas pelo grupo de cooperação serão eficazes para superar a relutância em comunicar os incidentes[156].

105 Ao abrigo dos regulamentos da UE em vigor, os operadores de serviços essenciais em determinados setores têm múltiplas obrigações de notificação (incluindo aos consumidores), o que pode prejudicar a eficiência do processo. A título ilustrativo, os operadores dos setores financeiro e bancário estão sujeitos a diferentes critérios de notificação, normas, limites e prazos nos termos estabelecidos pelo RGPD, pela Diretiva SRI, pela Diretiva relativa aos serviços de pagamento, pelo BCE/MUS, pelo TARGET 2 e pelo Regulamento eIDAS[157]. É importante, por conseguinte, simplificar estas obrigações, pois esta heterogeneidade, além de constituir um encargo administrativo desnecessário, pode conduzir a uma comunicação fragmentada de informações.

Resposta coordenada

106 A instituição de um quadro de cooperação europeia para crises de cibersegurança está ainda em curso. O "roteiro" nesta matéria[158] (ver o ponto ***18***) foi criado, por isso, com a finalidade de introduzir o ponto de vista da cibersegurança no Mecanismo Integrado de Resposta Política a Situações de Crise, melhorar o conhecimento da situação e garantir uma melhor integração com outros mecanismos da UE para a gestão de crises[159], envolvendo as instituições e organismos da UE e os Estados-Membros. Integrar todos estes mecanismos de resposta a situações de crise sem criar atritos é um desafio[160]. A atual ausência de uma rede de comunicações seguras comum às instituições da UE é também uma lacuna considerável[161].

107 A capacidade de resposta da UE a nível político e operacional aos ciberataques em caso de incidentes transfronteiriços em grande escala foi considerada como reduzida, em parte por a cibersegurança ainda não estar integrada nos mecanismos vigentes a nível da UE para a coordenação da resposta a crises[162]. A Diretiva SRI não corrigiu esta situação.

108 A recente proposta de reforma da ENISA, que previa conferir-lhe um maior papel operacional na resposta a incidentes de cibersegurança em grande escala, não foi apoiada pelos Estados-Membros, que preferiram que o papel da agência apoiasse e complementasse as suas próprias ações operacionais[163]. Existem já muitas CERT/CSIRT a nível dos Estados-Membros mas as suas capacidades variam consideravelmente, o que constitui um obstáculo à eficácia da cooperação transfronteiriça necessária para a respostas a incidentes em grande escala[164].

109 O Tribunal tentou fazer um levantamento dos diferentes papéis atribuídos aos diversos intervenientes mencionados no roteiro, tendo constatado a existência de lacunas que será necessário colmatar à medida que a aplicação avançar. Uma das áreas inicialmente negligenciadas foi garantir a aplicação da lei, pese embora a entrada em vigor, em dezembro de 2018, do protocolo de resposta de emergência dos serviços policiais da UE[165]. Será essencial assegurar que o roteiro é prático e que todos os intervenientes sabem qual o seu papel, o que necessitará de testes alargados nos próximos anos.

110 A eficácia da resposta implica mais do que a contenção dos danos, sendo também fulcral a atribuição de responsabilidades pelos ataques. Detetar e identificar os autores, sobretudo num ataque híbrido, pode ser muito difícil, devido à crescente utilização abusiva de ferramentas de anonimização, criptomoedas e encriptação. Esta questão é conhecida como o problema da atribuição, cuja solução não é apenas um desafio técnico, mas também do foro da justiça penal. As diferenças jurídicas e processuais entre países podem dificultar as investigações criminais e a instauração de ações penais contra os suspeitos. A resolução do problema da atribuição exigirá um intercâmbio operacional de informações mais formalizado, mediante procedimentos mais claros junto da Europol ou da Rede Judiciária Europeia da Eurojust em matéria de cibercriminalidade, por exemplo.

111 A nível político, o conjunto de instrumentos de ciberdiplomacia (ver a ***caixa 6***) foi elaborado com a finalidade de dar apoio à resolução de litígios internacionais sobre o ciberespaço por meios pacíficos. A criação de equipas de resposta rápida no domínio da cibersegurança e a iniciativa para a assistência mútua em matéria de cibersegurança são dois projetos que promovem o reforço da partilha de informações e que estão a ser desenvolvidos no quadro da CEP[166].

Caixa 6

Conjunto de instrumentos de ciberdiplomacia

A resposta diplomática conjunta da UE às ciberatividades maliciosas[167], designada por "conjunto de instrumentos de ciberdiplomacia", nasceu das conclusões de 2015 do Conselho sobre a ciberdiplomacia[168]. A ciberdiplomacia destina-se a desenvolver e aplicar uma abordagem comum e abrangente ao ciberespaço com base nos valores da UE, no Estado de direito, no reforço das capacidades e em parcerias, na promoção do modelo multilateral de governação da Internet e na atenuação das ameaças de cibersegurança e estabilidade acrescida nas relações internacionais.

O conjunto de instrumentos permite que a UE e os seus Estados-Membros apresentem uma resposta diplomática conjunta perante ciberatividades maliciosas. Para o efeito, fazem pleno uso de medidas no âmbito da Política Externa e de Segurança Comum, que podem ser preventivas (por exemplo, sensibilização, reforço das capacidades), cooperativas, de estabilidade ou restritivas (por exemplo, proibições de viagem, embargos de armas, congelamento de fundos), ou ainda de apoio à resposta dos Estados-Membros[169]. A premissa é a de que uma maior cooperação para atenuar as ameaças e o envio de sinais claros das consequências prováveis de uma resposta conjunta poderão dissuadir comportamentos (potencialmente) agressivos.

A resposta conjunta da UE às ciberatividades maliciosas deverá ser proporcional ao alcance, dimensão, duração, intensidade, complexidade, sofisticação e impacto da ciberatividade.

Para o êxito do conjunto de instrumentos, são fundamentais uma boa interligação com o roteiro e o Mecanismo Integrado de Resposta Política a Situações de Crise (ver o ponto ***106***), a obtenção de um bom conhecimento da situação através do rápido e permanente intercâmbio de informações (nomeadamente sobre dados relativos à atribuição)[170] e, por último, uma cooperação eficaz. Igualmente fulcral para o sucesso da sua aplicação será uma comunicação eficaz e coordenada. Até à data, o conjunto de instrumentos foi utilizado duas vezes: para iniciar um diálogo com os Estados Unidos na sequência do ataque *WannaCry*[171] e para elaborar conclusões do Conselho em condenação do uso malicioso de tecnologias da informação e comunicação[172]. A operacionalização do conjunto está em curso, permanecendo por aferir o seu grau de eficácia no cumprimento dos objetivos.

Desafio 10: proteger as infraestruturas e funções societais de importância crítica

Proteger as infraestruturas

112 Grande parte das infraestruturas de importância crítica da UE é operada através de sistemas de controlo industrial[173], muitos dos quais foram concebidos como sistemas autónomos, com reduzida conectividade ao mundo exterior. À medida que as suas componentes foram ganhando ligações à Internet, estes sistemas tornaram-se mais vulneráveis a interferências externas. A manutenção e o *patching* (remendo) dos sistemas existentes poderá já não ser viável, mas a sua modernização não é um processo rápido nem barato. Os esforços envidados para melhorar a segurança das

infraestruturas de importância crítica devem, por conseguinte, incluir a modernização dos sistemas de controlo industrial.

113 À medida que a indústria se continua a digitalizar (processo vulgarmente conhecido por "Indústria 4.0" ou "quarta revolução industrial"), o impacto de um incidente em grande escala num setor industrial poderá ter repercussões noutros. A ENISA sublinhou a importância do levantamento das dependências mútuas dos setores de importância crítica[174], o que é crucial para compreender o potencial alastramento de um incidente e constitui a base de uma resposta bem coordenada.

114 A Diretiva SRI visa aumentar o grau de preparação nos principais setores responsáveis pelas infraestruturas de importância crítica. No entanto, nem todos foram abrangidos (ver o ***quadro 1***)[175], o que reduz a eficácia da estratégia[176]. A este respeito, é particularmente importante proteger a integridade democrática das eleições contra a desinformação e as interferências nas infraestruturas eleitorais (ver a ***caixa 7***). Além da revisão da legislação vigente, um dos desafios fundamentais consistirá, por isso, em estudar formas de incentivar estes setores a darem respostas eficazes a incidentes em grande escala.

115 As vulnerabilidades das infraestruturas de importância crítica não estão confinadas às fronteiras da Europa. Um desafio importante para a Comissão é incentivar os países candidatos a aplicarem as mesmas normas que os Estados-Membros, por exemplo em domínios como a legislação relativa ao ciberespaço ou a proteção das infraestruturas de importância crítica.

Caixa 7

Proteger as funções societais de importância crítica: *combater a interferência em eleições*

Em maio de 2019, cerca de 400 milhões de eleitores irão às urnas nas eleições para o Parlamento Europeu, as primeiras após a entrada em vigor do RGPD. As eleições realizam-se na sequência dos escândalos em torno da utilização indevida de dados pessoais para a microssegmentação com fins políticos e de campanhas coordenadas de desinformação (notícias falsas) sem precedentes. A Comissão alertou para a probabilidade de interferências semelhantes nestas eleições[177], o que exigirá uma estratégia que abranja todos os governos e toda a sociedade.

Infraestruturas eleitorais

A organização de eleições é um processo complexo, devendo os Estados-Membros assegurar a sua proteção e integridade. A interferência nas eleições e nas infraestruturas eleitorais pode ter por objetivo influenciar as preferências dos

eleitores, a afluência às urnas ou o processo eleitoral em si, incluindo a própria votação e o apuramento e comunicação dos votos. Nas eleições para o Parlamento Europeu, proteger o chamado "quilómetro final" (a comunicação dos resultados das capitais nacionais a Bruxelas) é um desafio de importância particularmente crítica, pois não existe nem foi testada uma abordagem de segurança comum para o efeito[178].

O recente pacote da Comissão sobre as eleições previu medidas para reforçar a cibersegurança eleitoral, tais como a designação de pontos de contacto nacionais para coordenar e trocar informações no período pré-eleitoral. A partilha de boas práticas e da experiência adquirida reveste-se de especial importância[179].

Os sistemas eleitorais não são considerados parte integrante das infraestruturas de importância crítica[180] nem estão abrangidos pela Diretiva SRI. Não obstante, o grupo de cooperação elaborou orientações práticas sobre a segurança da tecnologia utilizada nas eleições para dar assistência às autoridades públicas, e os pontos de contacto nacionais deverão reunir-se no início de 2019[181]. Os Estados-Membros foram igualmente encorajados a realizar avaliações dos riscos das ciberameaças aos seus processos eleitorais.

Desinformação

A desinformação é um elemento cada vez mais importante dos ataques híbridos, que associa ciberataques e pirataria de redes. Estes ataques podem ser utilizados para dividir as sociedades, criar suspeitas e minar a confiança nos processos democráticos ou noutras questões (por exemplo, contra as vacinas ou as alterações climáticas). A desinformação tem crescido em escala, rapidez e abrangência e constitui uma verdadeira ameaça de segurança para a União.

A UE tomou uma série de medidas para combater esta atividade. Em 2015, foi criado no SEAE o grupo de trabalho de comunicação estratégica para o Leste "*East StratCom*", com a finalidade de combater as campanhas de desinformação provenientes da Rússia[182]. Os especialistas louvaram o seu trabalho na promoção das políticas da UE, no apoio aos meios de comunicação social independentes nos países da Vizinhança e na previsão, rastreamento e combate da desinformação[183]. No entanto, os recursos do grupo de trabalho são reduzidos em relação à dimensão e à complexidade das campanhas de desinformação[184], sendo necessárias uma interação mais sistemática com as estruturas da UE existentes e uma maior cooperação em matéria de comunicação estratégica[185]. Em dezembro de 2018, o Conselho Europeu aprovou um novo plano de ação[186].

Mais recentemente, na sequência da sua comunicação de abril de 2018 sobre o combate à desinformação na Internet[187], a Comissão elaborou um código de boas práticas, voluntário e de autorregulação[188], baseado nos instrumentos de política em vigor, ao qual aderiram as plataformas *online* e as empresas de publicidade[189]. Algumas das medidas são a ajuda para reforçar a fiabilidade dos conteúdos e o apoio aos esforços para aumentar a literacia quanto a notícias e à comunicação social, além do estabelecimento de uma rede europeia independente de verificadores de factos.

A Comissão afirmou que, se o código de boas práticas não for respeitado, poderão seguir-se medidas de regulação adicionais. Aferir a eficácia das medidas será crucial, em especial determinar como medir as melhorias em termos de confiança, transparência e prestação de contas.

Outro desafio consistirá em encontrar formas de melhorar a deteção, análise e exposição da desinformação[190], sendo ainda necessário proceder à análise e ao acompanhamento ativo e estratégico das fontes de dados abertas[191]. As tentativas de conseguir compreender melhor o ambiente das ameaças deve também abranger tendências emergentes como os "*deepfakes*" ("falsificações profundas", vídeos falsos realizados com recurso à inteligência artificial e à aprendizagem automática), assim como as ferramentas necessárias à sua deteção.

Reforçar a autonomia

116 A UE é um importador líquido de produtos e serviços de cibersegurança, o que aumenta o risco de dependência tecnológica e de vulnerabilidade em relação aos operadores de países terceiros[192]. Em especial, esta realidade ameaça a segurança das infraestruturas de importância crítica da UE, uma situação reforçada pelas complexas cadeias de abastecimento globais. O risco é ainda agravado nos casos em que operadores de países terceiros adquirem empresas europeias de cibersegurança. Os Estados-Membros são responsáveis pela análise dos investimentos diretos estrangeiros, não existindo de momento qualquer mecanismo na matéria à escala europeia[193].

117 O aumento da autonomia estratégica é um objetivo consagrado na Estratégia Global da UE e na Comunicação de 2017 "*Resiliência, dissuasão e defesa*"[194]. Superar a multiplicidade de desafios apresentados no presente relatório contribuirá para reforçar essa desejada autonomia, algo que nenhuma medida, por si só, conseguirá alcançar.

Pontos de reflexão – Resposta eficaz

- De que forma a Diretiva SRI melhorou a notificação de incidentes de cibersegurança em setores de importância crítica e além deles?
- Em que medida estão as instituições da UE a internalizar a coordenação da resposta a crises em caso de grandes incidentes de cibersegurança?
- Como pode a ciberdiplomacia desempenhar um papel de maior destaque nas ações externas da UE?
- As atuais estruturas e ações da UE destinadas a combater a desinformação são proporcionais à escala e complexidade do problema?

Observações finais

118 Nos últimos anos, a UE e os seus Estados-Membros têm dado mais prioridade à cibersegurança de modo a melhorar a ciber-resiliência geral. Porém, alcançar um maior nível de cibersegurança na União continua a ser um trabalho hercúleo. No presente documento informativo, o Tribunal procurou destacar alguns dos principais desafios à ambição da UE de se tornar no ambiente digital mais seguro do mundo.

119 A análise do Tribunal demonstra que é necessária uma transição para uma cultura de desempenho com práticas de avaliação integradas, de forma a garantir uma verdadeira **prestação de contas e avaliação**. **Subsistem algumas lacunas legais, e os Estados-Membros não transpõem a legislação vigente da mesma forma**, o que pode dificultar a concretização de todo o seu potencial. Outro desafio apontado diz respeito à **adaptação dos níveis de investimento aos objetivos estratégicos**, o que requer um aumento dos níveis de investimento e do seu impacto e se torna mais exigente quando a UE e os Estados-Membros não dispõem de uma **visão geral clara das despesas da UE** no domínio da cibersegurança. Além disso, foram comunicadas **restrições quanto à atribuição dos recursos adequados às agências da UE com responsabilidades na cibersegurança**, designadamente dificuldades em atrair e reter talentos.

120 Os estudos disponíveis concluem que **é possível melhorar a governação da cibersegurança** de modo a impulsionar a capacidade de resposta da comunidade internacional a ciberataques e incidentes e que, ao mesmo tempo, é impossível evitar todos os ataques. Por conseguinte, a **rapidez de deteção e resposta** e a **proteção das infraestruturas e funções societais de importância crítica**, em conjunto com a melhoria do **intercâmbio de informações e da coordenação** entre os setores público e privado, são alguns dos principais desafios a superar. Por último, a crescente escassez de competências em matéria de cibersegurança significa que o **reforço das competências e da consciencialização** em todos os setores e níveis da sociedade é também um desafio fundamental.

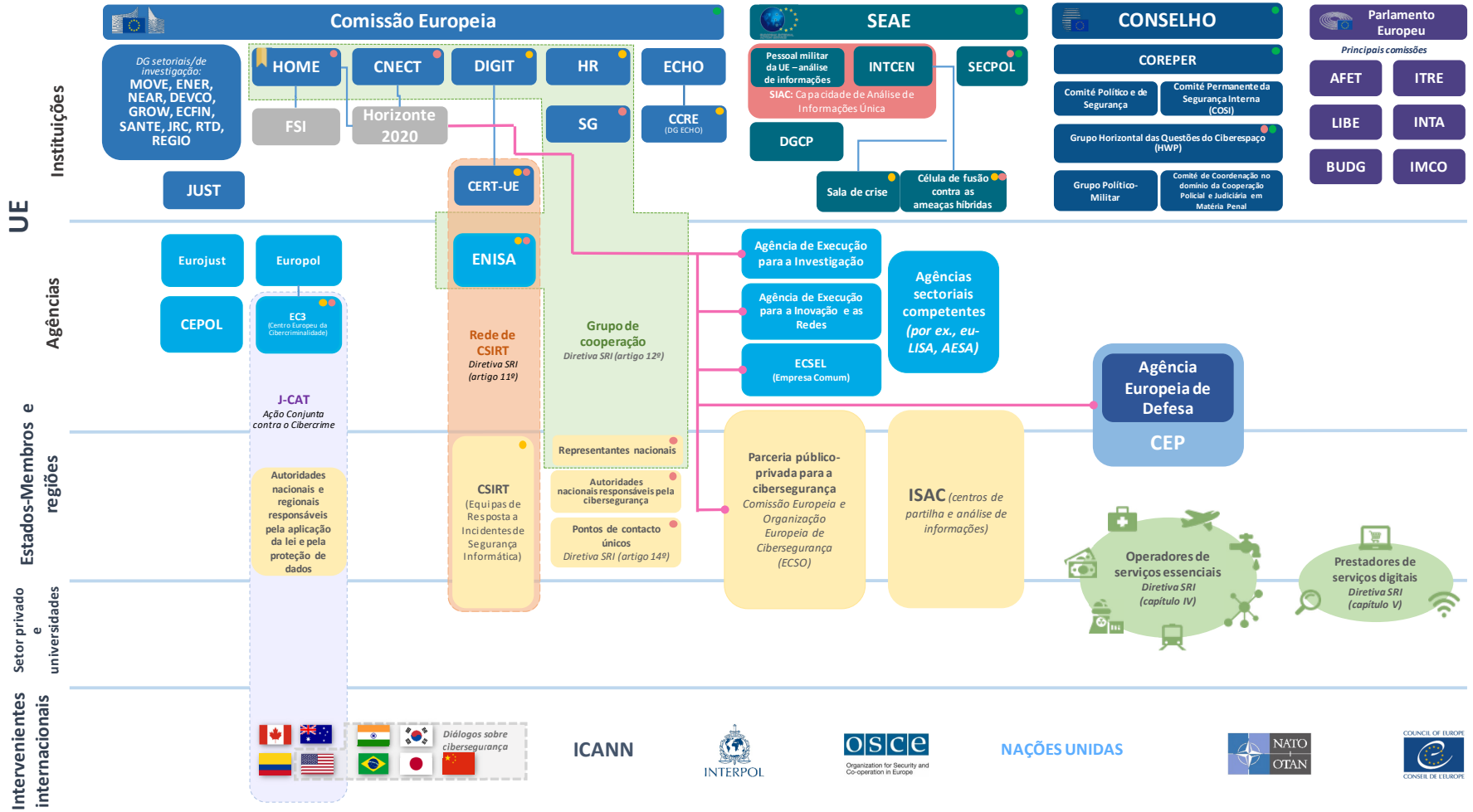
121 Estes desafios que as ciberameaças colocam à UE e ao mundo requerem o empenho contínuo e a adesão firme e permanente aos valores da UE.

O presente documento informativo foi adotado pela Câmara III na sua reunião de 14 de fevereiro de 2019.

Pelo Tribunal de Contas

Klaus-Heiner Lehne
Presidente

Anexo I — Um panorama complexo e multifacetado com muitos intervenientes



Níveis de cooperação previstos no ***roteiro*** de 2017 da UE para grandes incidentes de cibersegurança, de modo a conseguir uma resposta coordenada; consciencialização partilhada da situação e comunicação com o público

- **Técnico** — Gestão do incidente durante uma crise; acompanhamento e vigilância do incidente, incluindo a avaliação contínua da ameaça e dos riscos
- **Operacional** — Preparação das decisões a tomar a nível das políticas; coordenação da gestão das crises de cibersegurança; avaliação das consequências e impacto a nível da UE
- **Política** — Gestão estratégica e política dos aspetos da crise relacionados e não relacionados com o ciberespaço, incluindo medidas ao abrigo do quadro para uma resposta diplomática conjunta às ciberatividades maliciosas ("conjunto de instrumentos de ciberdiplomacia")

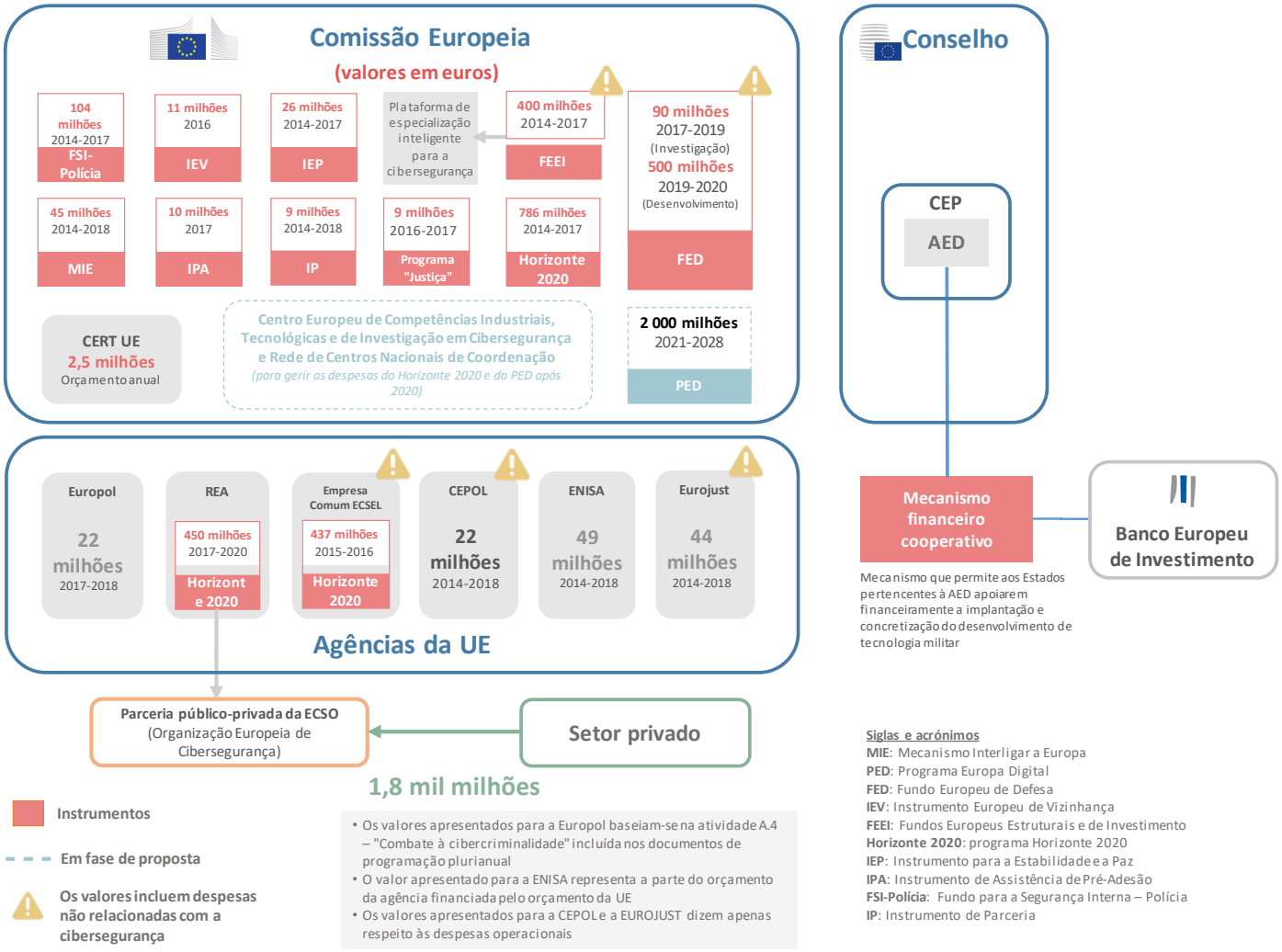
Principais fluxos de despesa do programa Horizonte 2020

A DG HOME alberga o Secretariado do Grupo de Trabalho sobre a União da Segurança

Nota: o acordo interinstitucional da CERT-UE abrange 11 instituições e organismos e 37 agências da UE.

Fonte: TCE.

Anexo II — Despesas da UE no domínio da cibersegurança desde 2014



Fonte: TCE, com base em documentos da Comissão Europeia e das agências da UE.

Anexo III — Relatórios das instituições superiores de controlo dos Estados-Membros da UE

Tipo	Título (com hiperligação)	Ano	Estado-Membro
Auditorias de conformidade	Nota de avaliação do controlo interno	2014	FR
	Relatório de certificação das contas do Regime Geral de Segurança Social (defesa e negócios estrangeiros)	2016	FR
	Certificação das contas do Estado	2016	FR
	Garantir a segurança e preservação das bases de dados nacionais estónias de importância crítica	Finalizado em 2018 / ainda não publicado	EE
	Eficácia dos controlos internos na proteção dos dados pessoais constantes das bases de dados nacionais	2008	EE
Auditorias de resultados/de otimização dos recursos	Relatório sobre a atenuação dos ciberataques	2013	DK
	RiR 2014:23 Segurança da informação na administração pública civil	2014	SE
	Relatório sobre o tratamento pelo Governo de dados confidenciais sobre pessoas e empresas	2014	DK
	Programa Nacional de Cibersegurança	2014	UK
	Relatório à Comissão Orçamental do Parlamento Federal alemão, nos termos do artigo 88º, nº 2, do código orçamental federal (BHO) – consolidação das tecnologias de informação, Governo Federal	2015	DE
	Relatório sobre o acesso aos sistemas informáticos que apoiam a prestação de serviços essenciais à sociedade dinamarquesa	2015	DK
	Autoridade pública de planeamento da *Plaine de France*	2015	FR
	"Ambiente de cibersegurança na Lituânia" Versão em lituano Resumo traduzido para inglês	2015	LT
	Desempenho das tarefas de cibersegurança pelos organismos públicos na Polónia (em polaco)	2015	PL
	RiR 2015:21 Cibercriminalidade – as forças policiais e os procuradores podem ser mais eficientes	2015	SE
	Défice de competências digitais no Governo (inquérito)	2015	UK
	Relatório ao Parlamento Federal: Finanças federais – cobrança do imposto sucessório	2016	BE
	Relatório sobre a gestão da segurança informática dos sistemas externalizados a fornecedores externos	2016	DK
	Relatório de auditoria sobre os empréstimos concedidos pelo Instituto Oficial de Crédito – 2016	2016	ES
	Dirigir a Rede de Segurança do Governo	2016	FI
	Garantir a segurança dos sistemas informáticos utilizados para tarefas públicas	2016	PL

Tipo	Título (com hiperligação)	Ano	Estado-Membro
	Prevenção e combate da ciberintimidação entre crianças e jovens	2016	PL
	Trabalho em matéria de segurança da informação em nove organismos – Nova auditoria à segurança da informação no Estado RiR 2016:8	2016	SE
	Proteger a informação em todo o Governo	2016	UK
	Relatório sobre a proteção dos sistemas informáticos e dos dados relativos à saúde em três regiões dinamarquesas	2017	DK
	Nota sobre os resultados da auditoria paralela internacional "Eficácia dos controlos internos na proteção dos dados pessoais constantes das bases de dados nacionais"	2017	EE
	Disposições de cibersegurança	2017	FI
	Dirigir a fiabilidade operacional dos serviços eletrónicos	2017	FI
	Rede de Câmaras Agrícolas (síntese)	2017	FR
	Câmara de Comércio e Indústria do departamento de Vaucluse (pela Câmara Regional de Auditoria da região da Provença-Alpes-Côte d'Azur)	2017	FR
	Garantir a segurança e preservação das bases de dados nacionais estónias de importância crítica	Finalizado em 2018 / ainda não publicado	EE
	"Desenvolvimento das infraestruturas das comunicações eletrónicas do Estado" Versão em lituano Resumo traduzido para inglês	2017	LT
	Auditoria às tecnologias da informação: a cibersegurança em todas as entidades públicas	2017	MT
	Sistema nacional de registos: segurança, desempenho e facilidade de utilização	2017	PL
	O incidente *WannaCry*	2017	UK
	Fraude *online*	2017	UK
	Relatório sobre a proteção contra ataques de *ransomware*	2018	DK
	Hospital de Arpajon (pela Câmara Regional de Île-de-France)	2018	FR
	"Gestão dos recursos de informação de importância crítica do Estado"	2018	LT
	"Crimes eletrónicos"	2019	LT
	Segurança da informação na Polónia	2019	PL
Outros	Base de dados dos organismos públicos	n.a.	BE
	Questionário sobre a política de segurança e análise dos riscos (em curso)	n.a.	BE

Siglas e acrónimos

AED: Agência Europeia de Defesa

CEP: Cooperação Estruturada Permanente

CERT-UE: equipa de resposta a emergências informáticas

CSIRT: equipa de resposta a incidentes de segurança informática

DDoS: ataque distribuído de negação de serviço

DG CNECT: Direção-Geral das Redes de Comunicação, Conteúdos e Tecnologias

DG DIGIT Direção-Geral da Informática

DG HOME: Direção-Geral da Migração e dos Assuntos Internos

DG JUST: Direção-Geral da Saúde e dos Consumidores

Diretiva SRI: Diretiva relativa à segurança das redes e da informação

EC3: Centro Europeu da Cibercriminalidade da Europol

ECSEL: Componentes e Sistemas Eletrónicos para uma Liderança Europeia

ECSO: Organização Europeia de Cibersegurança

ENISA: Agência Europeia para a Segurança das Redes e da Informação

FEEI: Fundos Europeus Estruturais e de Investimento

JRC: Centro Comum de Investigação

LISO: Responsável Local de Segurança Informática

PCSD: Política Comum de Segurança e Defesa

PME: Pequenas e Médias Empresas

RGPD Regulamento Geral sobre a Proteção de Dados

SEAE: Serviço Europeu para a Ação Externa

TCE: Tribunal de Contas Europeu

UE: União Europeia

Glossário

"Hacktivistas": indivíduos ou grupos que obtêm acesso não autorizado a sistemas ou redes informáticos com vista a utilizá-los para fins sociais ou políticos.

***Adware* (*software* de publicidade não solicitada):** *software* malicioso que apresenta faixas publicitárias ou janelas instantâneas (*pop-ups*) que incluem código destinado a rastrear o comportamento das vítimas na Internet.

Ameaça híbrida: manifestação de intenções hostis por parte de adversários através de uma combinação de técnicas de guerra convencionais e não convencionais (ou seja, métodos militares, políticos, económicos e tecnológicos) destinadas a atingirem pela força os seus objetivos.

Ataque distribuído de negação de serviço (DDoS): ciberataque que impede o acesso dos utilizadores legítimos a um serviço ou recurso *online* através do envio em massa de mais pedidos do que esse serviço ou recurso consegue tratar.

***Botnet*:** rede de computadores infetados por *software* malicioso e controlados à distância, sem o conhecimento dos utilizadores, com a finalidade de enviar mensagens eletrónicas não solicitadas, roubar informações ou lançar ciberataques coordenados.

Ciberataque: tentativa de prejudicar ou destruir a confidencialidade, integridade e disponibilidade de dados ou de um sistema informático através do ciberespaço.

Cibercriminalidade: diferentes atividades criminosas que envolvem computadores e sistemas informáticos como instrumentos ou alvos principais, entre as quais se encontram crimes tradicionais (por exemplo, fraude, falsificação e roubo de identidade), crimes relacionados com conteúdos (por exemplo, distribuição *online* de pornografia infantil ou incitamento ao ódio racial) e crimes específicos dos computadores e sistemas informáticos (por exemplo, ataques contra sistemas informáticos, ataques de negação de serviço e *malware*).

Ciberdefesa: subdivisão da cibersegurança que visa defender o ciberespaço através de meios militares e outras formas adequadas a fim de alcançar objetivos estratégico-militares.

Ciberespaço: ambiente global intangível em que se realiza a comunicação *online* entre pessoas, *software* e serviços através de redes informáticas e dispositivos tecnológicos.

Ciberincidente: evento que, direta ou indiretamente, provoca danos ou ameaça a resiliência e segurança de um sistema informático e dos dados por ele tratados, guardados ou transmitidos.

Ciber-resiliência: capacidade de prevenir ciberataques e ciberincidentes, de se preparar para eles, de lhes resistir e de recuperar deles.

Cibersegurança: todas as garantias e medidas tomadas para defender os sistemas e dados informáticos de acessos não autorizados e de ataques e danos, de forma a assegurar a sua disponibilidade, confidencialidade e integridade.

Clonagem: roubo de dados de cartões de crédito ou débito introduzidos *online*.

Computação em nuvem: disponibilização de recursos informáticos a pedido – como armazenamento e capacidade de computação ou de partilha de dados – através da Internet, mediante o acolhimento em servidores distantes.

Confidencialidade: proteção das informações, dados ou recursos contra o acesso ou divulgação não autorizados.

Conteúdos digitais: quaisquer dados – tais como texto, som, imagens ou vídeo – guardados em formato digital.

Crime dependente do ciberespaço: crime que só pode ser cometido através de dispositivos informáticos.

Crime possibilitado pelo ciberespaço: crime tradicional que é cometido em maior escala graças à utilização de sistemas informáticos.

Criptomoeda: ativo digital que é emitido e trocado através de técnicas de encriptação, sem intermédio de um banco central. É aceite como meio de pagamento entre os membros de uma comunidade virtual.

Dados de acesso: informações sobre a atividade de início e fim de sessão de um utilizador ao aceder a um serviço, por exemplo a hora, a data e o endereço IP.

Dados pessoais: informações relativas a uma pessoa identificável.

Desinformação: informação comprovadamente falsa ou enganosa que é criada, apresentada e divulgada para obter vantagens económicas ou para enganar deliberadamente o público, e que é suscetível de causar um prejuízo público.

Disponibilidade: garantia de acesso e utilização das informações de forma oportuna e fiável.

Ecossistema cibernético: comunidade complexa de dispositivos, dados, redes, pessoas, processos e organizações que interagem entre si e o ambiente de processos e tecnologias que influencia e apoia essas interações.

Encriptação: transformação de informações legíveis em código ilegível para as proteger. Para ler as informações, o utilizador tem de ter acesso a uma chave ou senha secretas.

Engenharia social: no domínio da segurança da informação, manipulação psicológica para induzir as pessoas a realizarem uma ação ou divulgarem informações confidenciais.

***Exploit kit*:** tipo de conjunto de ferramentas utilizado pelos cibercriminosos para atacar os pontos vulneráveis de redes e sistemas informáticos de forma a que possam distribuir *malware* ou levar a cabo outras atividades mal-intencionadas.

Gestão das vulnerabilidades: parte integrante da segurança dos computadores e das redes, visando atenuar de forma proativa ou prevenir a exploração de vulnerabilidades de *software* e do sistema através da sua identificação, classificação e reparação.

Infraestruturas de importância crítica: recursos, serviços e instalações físicos cuja perturbação ou destruição teria um forte impacto no funcionamento da economia e da sociedade.

Infraestruturas eleitorais: inclui sistemas informáticos e bases de dados das campanhas eleitorais, informações sensíveis sobre os candidatos, o recenseamento dos eleitores e sistemas de gestão.

Integridade: proteção contra a alteração ou destruição das informações de forma imprópria e garantia da sua autenticidade.

Internet das coisas: rede de objetos de uso quotidiano equipados com eletrónica, *software* e sensores que lhes permitem comunicar e trocar dados através da Internet.

***Malware* (*software* malicioso):** programa informático destinado a provocar danos num computador, servidor ou rede.

***Malware* de apagamento:** categoria de *malware* destinada a apagar o disco rígido do computador que infeta.

Modelo "criminalidade como serviço": modelo de negócio criminoso que impulsiona a economia digital clandestina, disponibilizando uma vasta gama de serviços comerciais e ferramentas que permitem que cibercriminosos iniciantes e sem competências cometam cibercrimes.

***Patching* (remendo):** introdução de um conjunto de alterações num *software* para o atualizar, reparar ou melhorar, incluindo corrigir vulnerabilidades em termos de segurança.

***Phishing*:** prática de enviar mensagens eletrónicas que aparentemente provêm de uma fonte fidedigna para enganar os destinatários e levá-los a clicar em ligações maliciosas ou a partilhar informações pessoais.

***Ransomware* (*software* de sequestro):** *software* malicioso que impede que as vítimas acedam a um sistema informático ou torna os ficheiros ilegíveis, geralmente através de encriptação. Em geral, o autor do ataque faz então chantagem com a vítima, recusando-se a repor o acesso até que seja pago um resgate.

Segurança das informações: conjunto de processos e ferramentas que protegem dados físicos e digitais contra o acesso, utilização, divulgação, perturbação, alteração, registo ou destruição não autorizados.

Segurança das redes: subdivisão da cibersegurança que protege os dados enviados através de dispositivos da mesma rede com o fim de garantir que as informações não sejam intercetadas ou alteradas.

Serviços de confiança: serviços que reforçam a validade jurídica de uma operação eletrónica como, por exemplo, assinaturas eletrónicas, selos, aposição de data e hora, entrega registada e autenticação de sítios Internet.

Sistema legado: aplicação, linguagem de programação ou sistema informático obsoletos ou desatualizados mas ainda em uso e para os quais poderão já não estar disponíveis atualizações e apoio do fornecedor, incluindo apoio em matéria de segurança.

Vetorização de texto: processo de conversão de palavras, frases ou documentos completos em vetores numéricos para possam ser utilizados por algoritmos de aprendizagem automática.

[1] Na proposta de legislação da UE sobre a cibersegurança, esta é definida como todas as atividades necessárias para proteger de ciberameaças as redes e os sistemas de informação, os seus utilizadores e as pessoas afetadas. Este diploma deverá ser aprovado pelo Parlamento Europeu e pelo Conselho no início de 2019.

[2] Europol, *Internet Organised Crime Threat Assessment 2017* (Avaliação da ameaça da criminalidade organizada na Internet - 2017).

[3] Organização Europeia de Cibersegurança (ECSO), *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership* (Proposta do setor de cibersegurança europeu para uma parceria público-privada contratualizada), junho de 2016.

[4] Parlamento Europeu, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses* (A cibersegurança na União Europeia e além dela: análise das ameaças e das respostas das políticas), estudo realizado para a Comissão LIBE, setembro de 2015.

[5] ENISA, *ENISA Threat Landscape Report 2017* (Análise panorâmica das ameaças pela ENISA - 2017), 18 de janeiro de 2018.

[6] Europol, *Internet Organised Crime Threat Assessment 2018* (Avaliação da ameaça da criminalidade organizada na Internet - 2018).

[7] Europol, *ibid.*, 2018.

[8] *European Centre for International Political Economy*, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?* (Roubar o trovão: iremos permitir que a ciberespionagem trave a Europa na corrida mundial pela competitividade industrial?), documento ocasional n.º 2/18, fevereiro de 2018.

[9] Comissão Europeia, Discurso sobre o Estado da União em 2017, proferido pelo Presidente da Comissão Europeia.

[10] Europol, *World's Biggest Marketplace selling internet paralysing DDoS attacks taken down* (Retirado o maior mercado mundial de venda de ataques DDoS para paralisar a Internet), comunicado de imprensa, 25 de abril de 2018.

[11] Europol, *Internet Organised Crime Threat Assessment 2017* (Avaliação da ameaça da criminalidade organizada na Internet - 2017).

[12] Ficha informativa da Comissão Europeia sobre a cibersegurança, setembro de 2017.

[13] Os custos poderiam incluir: perda de receitas; custos de reparação de sistemas danificados; responsabilidades potenciais por informações ou recursos roubados; incentivos à retenção de clientes; subida dos prémios de seguro; aumento dos custos de proteção (novos sistemas, funcionários, formação); potencial regularização de custos de conformidade ou litigância.

[14] NTT Security, *Risk: Value 2018 Report* (Relatório risco-valor 2018).

[15] O *ransomware* WannaCry tirou proveito das vulnerabilidades de um protocolo do Microsoft Windows que permitia tomar o controlo à distância de qualquer computador. Após a descoberta da vulnerabilidade, a Microsoft distribuiu um *patch* (remendo), mas centenas de milhares de computadores ainda não tinham sido atualizados e muitos deles foram posteriormente infetados. Fonte: A. Greenberg, *Hold North Korea Accountable For Wannacry—and the NSA, too* (Responsabilizem a Coreia do Norte pelo WannaCry, e a NSA também), WIRED, 19 de dezembro de 2017.

[16] Comissão Europeia, *Europeans' attitudes towards cybersecurity* (Comportamentos dos europeus face à cibersegurança), Eurobarómetro Especial 464a, setembro de 2017. Espera-se a publicação de um inquérito de seguimento no início de 2019.

[17] A Convenção de Budapeste é um guia internacional vinculativo para os países que elaboram legislação contra a cibercriminalidade, estabelecendo um quadro para a cooperação internacional entre os Estados que dela fazem parte. Atualmente, a UE é representada pela Comissão, pelo Conselho da União Europeia, pela Europol, pela ENISA e pela Eurojust.

[18] Comissão Europeia, *Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido*, JOIN(2013) 1 final, de 7 de fevereiro de 2013.

[19] Comissão Europeia, *Agenda Europeia para a Segurança*, COM(2015) 185 final, de 28 de abril de 2015.

[20] Comissão Europeia, *Estratégia para o Mercado Único Digital na Europa*, COM(2015) 192 final, de 6 de maio de 2015.

[21] SEAE, *Visão partilhada, ação comum: uma Europa mais forte). Estratégia Global para a Política Externa e de Segurança da União Europeia*, junho de 2016.

[22] Centro de Estudos de Política Europeia (CEPE), *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force* (Reforçar as capacidades de ciberdefesa da UE – Relatório de um grupo de trabalho do CEPE), novembro de 2018.

[23] O *software* malicioso por trás do ataque de *ransomware* WannaCry, cuja autoria foi atribuída à Coreia do Norte pelos Estados Unidos, o Reino Unido e a Austrália, foi inicialmente desenvolvido e guardado pela Agência de Segurança Nacional (NSA) dos Estados Unidos para explorar as vulnerabilidades do Windows. Fonte: A. Greenberg, *ibid*., WIRED, 19 de dezembro de 2017. Na sequência dos ataques, a Microsoft condenou a prática de os governos guardarem em reserva as vulnerabilidades detetadas em *software* e reiterou o seu apelo à necessidade de uma Convenção de Genebra Digital.

[24] Além de terra, mar, ar e espaço.

[25] Quadro Estratégico da UE para a Ciberdefesa (atualização de 2018), documento nº 14413/18, 19 de novembro de 2018.

[26] Comissão Europeia/Serviço Europeu para a Ação Externa, *Quadro comum em matéria de luta contra as ameaças híbridas: uma resposta da União Europeia*, JOIN(2016) 18 final, de 6 de abril de 2016.

[27] Declarações Conjuntas dos Presidentes do Conselho Europeu e da Comissão Europeia e do Secretário-Geral da Organização do Tratado do Atlântico Norte, 8 de julho de 2016 e 10 de julho de 2018.

[28] Comissão Europeia/Serviço Europeu para a Ação Externa, *Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE*, JOIN(2017) 450 final, de 13 de setembro de 2017.

[29] 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 (JO L 194 de 19.7.2016, p. 1).

[30] 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.

[31] Estas equipas estão integradas em estruturas de cooperação criadas pela diretiva, a Rede de CSIRT (uma rede composta pelas CSIRT designadas pelos Estados-Membros da UE e pela CERT-UE, cujo secretariado é assegurado pela ENISA) e o Grupo de Cooperação (que apoia e articula a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros e cujo secretariado se situa na Comissão).

[32] 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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

[33] Comissão Europeia, *Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à ENISA, a "Agência da União Europeia para a Cibersegurança", e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 ("Regulamento Cibersegurança")*, COM(2017) 477 final, de 13 de setembro de 2017.

[34] Comissão Europeia, *Proposta de Regulamento do Parlamento Europeu e do Conselho relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal*, COM(2018) 225 final, de 17 de abril de 2018.

[35] Comissão Europeia, *Proposta de Diretiva do Parlamento Europeu e do Conselho que estabelece normas harmonizadas aplicáveis à designação de representantes legais para efeitos de recolha de provas em processo penal*, COM(2018) 226 final, de 17 de abril de 2018.

[36] Comissão Europeia, *Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação*, COM(2018) 630 final, de 12 de setembro de 2018.

[37] H. Carrapiço e A. Barrinha, *The EU as a Coherent (Cyber)Security Actor?* (A UE enquanto interveniente coerente na (ciber)segurança? *Journal of Common Market Studies*, vol. 55, n.º 6, 2017.

[38] Comissão Europeia, *ibid*., SWD(2017) 295 final, de 13 de setembro de 2017.

[39] Serviço de Estudos do Parlamento Europeu, *Transatlantic cyber-insecurity and cybercrime – Economic impact and future prospects* (Ciber-insegurança e cibercriminalidade a nível transatlântico – Impacto económico e evolução futura), PE 603.948, dezembro de 2017.

[40] ENISA, *An evaluation framework for Cyber Security Strategies* (Quadro de avaliação das estratégias de cibersegurança), 27 de novembro de 2014.

[41] Uma exceção é o artigo 14º ("Acompanhamento e estatísticas") da 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.

[42] Comité Económico e Social Europeu, *Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks* (Cibersegurança: garantir a consciencialização e resiliência do setor privado na Europa face à escalada dos riscos cibernéticos), março de 2018. Grupo de trabalho Centro de Estudos de Política Europeia (CEPE)-Comissão Europeia contra o Racismo e a Intolerância (CERI), *Cybersecurity in Finance: Getting the policy mix right!* (Cibersegurança das finanças: acertar na combinação de políticas), junho de 2018.

[43] Das 28 instituições superiores de controlo nacionais, 24 responderam ao inquérito.

[44] Ou seja, baseado em princípios e tão neutro em termos de tecnologia quanto possível.

[45] Mecanismo de Aconselhamento Científico da Comissão Europeia, *Scientific Opinion 2/2017* (Opinião científica nº 2/2017), 24 de março de 2017.

[46] L. Rebuffi, *EU Digital Autonomy: A possible approach* (Autonomia digital da UE: uma abordagem possível), *Digma Zeitschrift für Datenrecht und Informationssicherheit*, setembro de 2018. *European Centre for International Political Economy*, *ibid*., *Occasional Paper n.º 2/18* (Documento ocasional nº 2/18), fevereiro de 2018.

[47] Comissão Europeia, *Proposta de diretiva do Parlamento Europeu e do Conselho sobre certos aspetos relativos aos contratos de fornecimento de conteúdos digitais*, COM(2015) 634 final, de 9 de dezembro de 2015.

[48] Comissão Europeia, *Proposta de diretiva do Parlamento Europeu e do Conselho relativa a certos aspetos que dizem respeito a contratos de vendas em linha de bens e outras vendas à distância de bens*, COM(2015) 635 final, de 9 de dezembro de 2015.

[49] Conselho neerlandês de cibersegurança, *European Foresight Cyber Security Meeting 2016: Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care* (Simpósio de antevisão da cibersegurança a nível europeu, 2016: Recomendações do meio académico público-privado à Comissão Europeia sobre a Internet das coisas e a harmonização dos deveres de diligência), 2016.

[50] Centro de Estudos de Política Europeia (CEPE), *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges – Report of a CEPS Task Force* (Divulgação de vulnerabilidades de *software* na Europa: tecnologia, políticas e desafios jurídicos – Relatório do grupo de trabalho do CEPE), junho de 2018.

[51] Comissão Europeia, *Tirar o maior partido da SIR – Para uma execução efetiva da Diretiva (UE) 2016/1148 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União*, COM(2017) 476 final/2, de 4 de outubro de 2017.

[52] Europol, *ibid*., 2017.

[53] Conselho da União Europeia, *Relatório final da sétima ronda de avaliações mútuas sobre "Implementação e aplicação prática das políticas europeias de prevenção e combate à cibercriminalidade"*, 12711/1/17 REV 1, 9 de outubro de 2017.

[54] Comissão Europeia, *Impact assessment accompanying the document "Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment"* (Avaliação de impacto que acompanha o documento "Proposta de Diretiva relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário"), SWD/2017/0298 final, de 13 de setembro de 2017. Em dezembro de 2018 foi alcançado um consenso político sobre a nova legislação, prevendo-se que seja aprovada no início de 2019.

[55] Europol, *ibid*., 2017.

[56] C-362/14: Maximillian Schrems/*Data Protection Commissioner* (Irlanda), 6 de outubro de 2015.

[57] Europol/Eurojust, *Common challenges in combating cybercrime* (Desafios comuns no combate à cibercriminalidade), 7021/17, 13 de março de 2017.

[58] Comissão Europeia, *Assessment of the EU 2013 Cybersecurity Strategy* (Avaliação da Estratégia de 2013 da UE para a Cibersegurança), SWD(2017) 295 final, de 13 de setembro de 2017.

[59] Serviço de Estudos do Parlamento Europeu, *Briefing: EU Legislation in Progress – Review of dual-use export controls* (Legislação da UE em curso – Revisão dos controlos das exportações de produtos de dupla utilização), *PE589.832*.

[60] Resolução do Parlamento Europeu, *Direitos humanos e tecnologia: o impacto da intrusão e dos sistemas de vigilância nos direitos humanos em países terceiros*, 2014/2232(INI), 8 de setembro de 2015. Os bens e serviços de dupla utilização, em que se incluem o *software* e a tecnologia, podem ter aplicações civis e militares.

[61] As informações acessíveis ao público estão armazenadas na base de dados WHOIS, gerida pela ICANN (Sociedade Internet para os Nomes e Números Atribuídos), que mantém o Sistema de Nomes de Domínio. A utilização abusiva dos nomes de domínio facilita a cibercriminalidade.

[62] Artigo 3.º da Diretiva SRI, *ibid*.

[63] Atlantic Council, *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures* (Nexo entre os riscos: seremos dominados pelos riscos cibernéticos? Benefícios e custos económicos de futuros cibernéticos alternativos), 10 de setembro de 2015.

[64] Casa Branca, *Cybersecurity spending fiscal year 2019* (Despesas em cibersegurança, exercício orçamental de 2019).

[65] Comissão Europeia, *Commission Staff Working Document: Impact Assessment accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027'* (Documento de trabalho dos serviços da Comissão: avaliação de impacto que acompanha o documento "Proposta de Regulamento do Parlamento Europeu e do Conselho que cria o programa Europa Digital para o período de 2021-2027"), SWD(2018) 305 final, de 6 de junho de 2018.

[66] *The Hague Centre for Strategic Studies*, *Dutch investments in ICT and cybersecurity: putting it in perspective* (Investimentos dos Países Baixos nas tecnologias da informação e em cibersegurança: contextualização), dezembro de 2016.

[67] Comissão Europeia, *ibid*., COM(2018) 630 final, de 12 de setembro de 2018.

[68] Unidade da Prospetiva Científica do Serviço de Estudos do Parlamento Europeu, *Achieving a sovereign and trustworthy ICT industry in the EU* (Concretizar um setor de tecnologias da informação soberano e fiável na UE), dezembro de 2017.

[69] *European Digital SME Alliance*, *Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem* (Documento de posição sobre a estratégia de cibersegurança europeia: promover o ecossistema das PME), 31 de julho de 2017.

[70] Unidade da Prospetiva Científica do Serviço de Estudos do Parlamento Europeu, *ibid*., dezembro de 2017.

[71] *Ibid*.

[72] Comissão Europeia, *Impact assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centre* (Avaliação de impacto que acompanha a Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação), SWD(2018) 403 final (parte 1/4), de 12 de setembro de 2018.

[73] Comissão Europeia, *ibid*., COM(2018) 630 final, de 12 de setembro de 2018.

[74] Relatório Especial nº 13/2018 do TCE: "Combate à radicalização que leva ao terrorismo".

[75] Os valores referidos nesta secção provêm de documentos da Comissão acessíveis ao público, salvo o montante de 42 milhões de euros mencionado no ponto ***51***, que foi facultado diretamente pela Comissão.

[76] O Horizonte 2020 é o programa de investigação e inovação da UE. Dotado de 80 mil milhões de euros, apoia a União da Inovação, que visa garantir a competitividade global da UE.

[77] Desafio societal 7 do Horizonte 2020 – "Sociedades seguras e inovadoras: proteger a liberdade e a segurança da Europa e dos seus cidadãos".

[78] O Tribunal analisou os projetos do Horizonte 2020 a partir do conjunto de dados CORDIS. Foi realizada a vetorização de texto da descrição de cada projeto com a taxonomia de cibersegurança do JRC (ver a ***caixa 5*** no próximo capítulo), de modo a detetar projetos passíveis de estarem relacionados com a cibersegurança. Os resultados foram em seguida verificados manualmente e analisados.

[79] Organização Europeia de Cibersegurança, *ECS cPPP Progress Monitoring Report 2016-2017* (Relatório de acompanhamento dos progressos da parceria público-privada contratualizada sobre a cibersegurança), 29 de outubro de 2018.

[80] Artigo 9.º, nº 2, da Diretiva SRI, *ibid*.

[81] O GLACY+ (Ação Global sobre a Cibercriminalidade+) é um projeto conjunto com o Conselho da Europa, apoiando doze países em África, na Ásia-Pacífico e na América Latina e Caraíbas que, por seu turno, podem servir de plataformas para partilhar a sua experiência nas suas regiões.

[82] O Centro Europeu de Estratégia Política, um centro de reflexão da Comissão, alertou para o risco de vir a emergir um "ângulo morto digital" se o fosso entre a UE e os seus vizinhos dos Balcãs Ocidentais continuar a crescer. Países como a China e a Rússia estão a investir montantes significativos na região, comportando o risco de marginalizar a UE enquanto interveniente no domínio da cibersegurança nesse espaço. Fonte: Centro Europeu de Estratégia Política, *Engaging with the Western Balkans: an investment in Europe's security* (Interagir com os Balcãs Ocidentais: um investimento na segurança da Europa), 17 de maio de 2018.

[83] Banco Europeu de Investimento, *The EIB Group Operating Framework and Operational Plan 2018* (Quadro de funcionamento e plano operacional do Grupo BEI), 12 de dezembro de 2017. À data da elaboração do presente relatório, não estavam disponíveis mais informações.

[84] Comissão Europeia, *Proposta de Regulamento do Parlamento Europeu e do Conselho que cria o programa Europa Digital para o período de 2021-2027*, COM(2018) 434 final, de 6 de junho de 2018.

[85] Comissão Europeia, *Regulamento (UE) 2018/1092 do Parlamento Europeu e do Conselho, de 18 de julho de 2018, que estabelece o Programa Europeu de Desenvolvimento Industrial no domínio da Defesa destinado a apoiar a competitividade e a capacidade inovadora da indústria de defesa da União* (JO L 200 de 7.8.2018, p. 30). Em 2017, foi ainda iniciada uma ação preparatória sobre investigação no domínio da defesa, dotada de um total de 90 milhões de euros no período de 2017-2019 e financiada pelo Horizonte 2020, não sendo claro se inclui despesas relacionadas com a cibersegurança.

[86] O TCE prevê publicar em 2019 um documento informativo dedicado à defesa na UE.

[87] O pessoal do EC3 da Europol, da ENISA, do SEAE, da Agência Europeia de Defesa e da CERT-UE é, em conjunto, constituído por 159 pessoas. Este número não inclui o pessoal a trabalhar na área da cibersegurança na Comissão Europeia e nos Estados-Membros. Fonte: Centro de Estudos de Política Europeia, *ibid*., novembro de 2018.

[88] *ENISA evaluation* (Avaliação da ENISA), 2017.

[89] No seu plano plurianual de 2018-2020, a Europol solicitou um aumento do pessoal de 70 agentes temporários por ano, mas apenas foi aprovado um aumento de 26 para 2018. Na proposta do próximo plano plurianual, para 2019-2021, a Europol assumiu um aumento modesto, admitindo que um maior pedido de recursos não teria resposta positiva. Fonte: Consulta sobre a proposta de programa de trabalho plurianual para 2019-2021, apresentada ao grupo de controlo parlamentar conjunto, A 000834, 1 de fevereiro de 2018.

[90] *ENISA evaluation* (Avaliação da ENISA), 2017. Entre 2014 e 2016, cerca de 80 % do orçamento operacional da ENISA foi utilizado para a encomenda de estudos.

[91] ENISA, *Exploring the opportunities and limitations of current Threat Intelligence Platforms* (Exploração das oportunidades e limitações das atuais plataformas de informações sobre ameaças), dezembro de 2017.

[92] ISACA (anteriormente conhecida como *Information Systems Audit and Control Association*), *Information Security Governance: Guidance for Boards of Directors and Executive Management* (Governação da segurança da informação: orientações para conselhos de administração e gestores executivos), 2.ª ed., 2006.

[93] EY, *Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017* (Recuperar a cibersegurança: preparação contra ciberataques. 20º inquérito global sobre a segurança da informação – 2017), p. 16.

[94] McKinsey (J. Choi, J. Kaplan, C. Krishnamurthy and H. Lung), *Hit or myth? Understanding the true costs and impact of cybersecurity programs* (Realidade ou mito? Compreender os verdadeiros custos e o impacto dos programas de cibersegurança), julho de 2017.

[95] *Securities and Exchange Commission*, *Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures* (Declaração e orientação interpretativa sobre a comunicação de informações de cibersegurança das empresas cotadas), 21 de fevereiro de 2018.

[96] Fórum de cooperação entre a Autoridade Bancária Europeia, a Autoridade Europeia dos Valores Mobiliários e dos Mercados e a Autoridade Europeia dos Seguros e Pensões Complementares de Reforma.

[97] Autoridade Europeia dos Valores Mobiliários e dos Mercados, *Joint Committee report on risks and vulnerabilities in the EU financial system* (Relatório do Comité Conjunto sobre riscos e vulnerabilidades no sistema financeiro da UE), abril de 2018.

[98] ENISA, *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs* (Normas de segurança da informação e de privacidade para as PME: recomendações para melhorar a aplicação de normas de segurança da informação e de privacidade nas PME), dezembro de 2015.

[99] Em referência aos Estados-Membros da UE, o Mecanismo de Aconselhamento Científico da Comissão registou o nível substancial e inédito de acordo sobre princípios e valores fundamentais, bem como o interesse estratégico comum que poderá constituir o cerne da governação eficaz da UE em matéria de cibersegurança. Fonte: *Scientific Opinion 2/2017* (Opinião científica nº 2/2017), 24 de março de 2017.

[100] Com os Estados Unidos, a China, o Japão, a Coreia do Sul, a Índia e o Brasil.

[101] Academia Europeia de Segurança e Defesa (T. Renard e A. Barrinha), *Handbook on cyber security, chapter 3.4 The EU as a partner in cyber diplomacy and defence* (Manual de cibersegurança, capítulo 3.4 – A UE como parceira na ciberdiplomacia e na defesa), 23 de novembro de 2018.

[102] Conselho da União Europeia, *Plano de ação para aplicação das Conclusões do Conselho sobre a comunicação conjunta ao Parlamento Europeu e ao Conselho intitulada"Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE"*, 15748/17, de 12 de dezembro de 2017.

[103] Comissão Europeia, *European Commission Digital Strategy: A digitally transformed, user-focused and data-driven Commission* (Estratégia Digital da Comissão Europeia: uma Comissão digitalmente transformada, centrada no utilizador e baseada em dados), C (2018) 7118 final, 21 de novembro de 2018.

[104] Resposta da Comissária Mariya Gabriel a pergunta parlamentar escrita (E-004294-17), 28 de junho de 2017.

[105] Conselho da União Europeia, *Annual Report on the Implementation of the Cyber Defence Policy Framework* (Relatório anual sobre a aplicação do quadro estratégico de ciberdefesa), 15870/17, 19 de dezembro de 2017.

[106] As Decisões 2015/443, 2015/444 e 2017/46 regulam a segurança dos sistemas de comunicação e informação da Comissão. A Decisão C(2018) 7706 da Comissão, de 21 de novembro de 2018, cria um Conselho de Tecnologias da Informação e Cibersegurança, que reúne os anteriores Conselho Informático e Conselho Diretivo da Segurança dos Sistemas de Informação.

[107] Comité Económico e Social Europeu, *ibid*., março de 2018.

[108] Parlamento Europeu, *ibid*., setembro de 2015.

[109] A célula de fusão contra as ameaças híbridas foi criada em 2016 no âmbito do Centro de Situação e de Informações do SEAE, recebendo e analisando informações confidenciais e de fontes abertas de diferentes partes interessadas sobre ameaças híbridas.

[110] ENISA, *National-level Risk Assessments: An Analysis Report* (Avaliações de risco a nível nacional: relatório de análise), novembro de 2013.

[111] Comissão Europeia, *Impact assessment on the EU Cybersecurity Agency and Cybersecurity Act* (Avaliação de impacto sobre o Regulamento relativo à Agência da União Europeia para a Cibersegurança e à Cibersegurança), SWD(2017) 500 final (parte 1/6), de 13 de setembro de 2018.

[112] Comissão Europeia, *ibid*., SWD(2018) 403 final, de 12 de setembro de 2018.

[113] *Résaux IP Européens - Network Coordination Centre*, o registo regional da Internet para a Europa, que supervisiona a atribuição e o registo dos recursos de números Internet.

[114] ENISA, *EISAS Large-Scale Pilot Collaborative Awareness Raising for EU Citizens & SMEs* (Projeto-piloto de grande escala da SEPIA – colaboração para a sensibilização dos cidadãos e PME da UE, novembro de 2012.

[115] *Centre for Cyber Safety and Education*, em parceria com *Booz Allen Hamilton*, *Alta Associates* e *Frost & Sullivan*, *2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk* (Estudo de 2017 sobre os profissionais de segurança da informação a nível mundial – Avaliação comparativa da capacidade dos profissionais e da resposta aos riscos de cibersegurança).

[116] Comité Económico e Social Europeu, *ibid*., março de 2018.

[117] *House of Lords-House of Commons Joint Committee on the National Security Strategy – Cyber Security Skills and the UK's Critical National Infrastructure, Second Report of Session 2017–19* (Comissão conjunta da Câmara dos Lordes e da Câmara dos Comuns sobre a estratégia nacional de segurança – Competências de cibersegurança e infraestruturas de importância crítica do Reino Unido, segundo relatório da sessão 2017-19), 16 de julho de 2018.

[118] Europol/Eurojust, *Common challenges in combating cybercrime* (Desafios comuns no combate à cibercriminalidade), 7021/17, 13 de março de 2017.

[119] Europol/Eurojust, *ibid*., 7021/17, 13 de março de 2017.

[120] Comissão Europeia, *ibid*., SWD(2018) 403 final, de 12 de setembro de 2018.

[121] CEPOL, *Decision of the Management Board 33/2018/MB on the CEPOL Single Programming Document 2020-2022* (Decisão do Conselho de Administração 33/2018/MB sobre o documento único de programação da CEPOL para o período de 2020-2022), 20 de novembro de 2018.

[122] Por exemplo, através da cooperação entre o SEAE, os Estados-Membros, as agências e organismos como a CEPOL, o ECTEG ou a AESD.

[123] ENISA, *Stock-taking of information security training needs in critical sectors* (Levantamento das necessidades de formação em segurança da informação em setores de importância crítica), dezembro de 2017.

[124] Grupo Europeu de Ensino e Formação sobre Cibercriminalidade.

[125] Comissão Europeia, Décimo terceiro relatório para a criação de uma União da Segurança genuína e eficaz, COM(2018) 46 final, de 24 de janeiro de 2018.

[126] Com base em observações do Relatório Especial nº 14/2018, *ibid*.

[127] Resolução do Parlamento Europeu, de 13 de junho de 2018, sobre ciberdefesa (2018/2004(INI)). Conselho da União Europeia, *ibid*., 15870/17, 19 de dezembro de 2017.

[128] Suíça, Macedónia do Norte, Ucrânia, Bósnia-Herzegovina, Kosovo (esta designação não prejudica as posições relativas ao estatuto e está em conformidade com a Resolução 1244/99 do CSNU e com o parecer do TIJ sobre a declaração de independência do Kosovo), Turquia e Estados Unidos.

[129] Europol, *Internet Organised Crime Threat Assessment 2018* (Avaliação da ameaça da criminalidade organizada na Internet - 2018).

[130] Comissão Europeia, *ibid*., SWD(2017) 295 final, de 13 de setembro de 2017.

[131] B. Stanton, M. F. Theofanos, S. S. Prettyman e S. Furman, *Security Fatigue* (Fadiga da segurança), *IT Professional*, vol. 18, nº 5, 2016, pp. 26-32. Ver igualmente NIST.

[132] Comissão Europeia/Serviço Europeu para a Ação Externa, *Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas*, JOIN(2018) 16 final, de 13 de junho de 2018.

[133] Por exemplo, o encerramento do AlphaBay e do Hansa em operações conjuntas lideradas pelo FBI e pela polícia nacional dos Países Baixos com o apoio da Europol. Estes eram dois dos maiores mercados para o comércio de bens ilícitos, como drogas, armas de fogo e instrumentos de cibercriminalidade, por exemplo *malware*. Fonte: Europol, *Crime on the Dark Web: Law Enforcement coordination is the only cure* (Criminalidade na Internet oculta: coordenar a aplicação da lei é a única solução), Comunicado de Imprensa, 29 de maio de 2018.

[134] Comissão Europeia, *ibid*., SWD(2018) 403 final, de 12 de setembro de 2018.

[135] Conselho da União Europeia, *ibid*., 12711/1/17 REV 1, de 9 de outubro de 2017.

[136] Comissão Europeia, *ibid*., SWD(2017) 295 final, de 13 de setembro de 2017.

[137] Comissão Europeia/Serviço Europeu para a Ação Externa, *ibid*., JOIN(2018) 16, de 13 de junho de 2018.

[138] Comissão Europeia, SWD(2017) 500 final, de 13 de setembro de 2017.

[139] *Memorandum of Understanding – ENISA, EDA, Europol EC3, and CERT-EU* (Memorando de entendimento entre a ENISA, a AED, o EC3 da Europol e a CERT-UE), 23 de maio de 2018.

[140] Comissão Europeia, concurso *Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap* (Criação e operação de um projeto-piloto de uma rede de competências de cibersegurança para desenvolver e aplicar um roteiro comum de investigação e inovação em cibersegurança), 27 de outubro de 2017.

[141] Jean-Claude Juncker, *Mission letter for the Commissioner for the Security Union* (Carta de missão ao comissário responsável pela União da Segurança), 2 de agosto de 2016. A defesa está fora do âmbito de competências do grupo de trabalho.

[142] Conselho da União Europeia, *EU cybersecurity roadmap* (Roteiro de cibersegurança da UE), documento 8901/17, de 11 de maio de 2017.

[143] *Friends of Europe*, *Debating Security Plus: Crowdsourcing solutions to the world's security issues* (*Debating Security Plus*: soluções de financiamento colaborativo para as questões de segurança mundial), 5.ª ed., novembro de 2017.

[144] Relatórios Técnicos do JRC, *European Cybersecurity Centres of Expertise Map: Definitions and Taxonomy (Mapa dos centros especializados europeus de cibersegurança: definições e taxonomia). Impact assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres* (Avaliação de impacto que acompanha a Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação), SWD(2018) 403 final, de 12 de setembro de 2018.

[145] Comissão Europeia, *ibid*., SWD(2017) 295 final, de 13 de setembro de 2017.

[146] Comissão Europeia, *ibid*., SWD(2018) 403 final, de 12 de setembro de 2018.

[147] Por exemplo, os centros de partilha e análise de informações dos institutos financeiros europeus incluem representantes do setor financeiro, das CERT nacionais, dos organismos responsáveis pela aplicação da lei, da ENISA, da Europol, do Banco Central Europeu, do Conselho Europeu de Pagamentos e da Comissão Europeia.

[148] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models* (Modelos cooperativos de centros de partilha e análise de informações - ISAC), 14 de fevereiro de 2018.

[149] Conselho da União Europeia, *ibid*., documento 12711/1/17 REV 1, de 9 de outubro de 2017.

[150] https://www.europol.europa.eu/empact.

[151] Um estudo de 2018 realizado pela Accenture em 15 países constatou que 87 % dos ciberataques dirigidos eram impedidos: *2018 State of Cyber Resilience* (Estado da ciber-resiliência em 2018), 10 de abril de 2018.

[152] P. Timmers, *Cybersecurity is Forcing a Rethink of Strategic Autonomy* (A cibersegurança está a obrigar a repensar a autonomia estratégica), blogue de política da Universidade de Oxford, 14 de setembro de 2018.

[153] Caroline Preece, *Three reasons why cyber threat detection is still ineffective* (Três razões pelas quais a deteção das ciberameaças continua a ser ineficaz), *IT Pro*, 14 de julho de 2017.

[154] Comité Económico e Social Europeu, *ibid.*, março de 2018.

[155] Comissão Europeia, *Oitavo relatório para a criação de uma União da Segurança genuína e eficaz*, COM(2017) 354 final, de 29 de junho de 2017.

[156] Ver as várias publicações do grupo de cooperação SRI.

[157] Diretiva relativa aos serviços de pagamento 2; BCE/MUS: Banco Central Europeu/Mecanismo Único de Supervisão; TARGET 2: Transferências Automáticas Transeuropeias de Liquidações pelos Valores Brutos em Tempo Real (2ª geração); Regulamento (UE) nº 910/2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno. Fonte: Grupo de trabalho Centro de Estudos de Política Europeia (CEPE)-Comissão Europeia contra o Racismo e a Intolerância (CERI), *ibid*., junho de 2018.

[158] Comissão Europeia, *Recomendação sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala*, C(2017) 6100 final, de 13 de setembro de 2017.

[159] Comissão Europeia, *ibid*., SWD(2017) 295 final, de 13 de setembro de 2017. Existem vários mecanismos de gestão de crise, designadamente o Mecanismo Integrado de Resposta Política a Situações de Crise, o Argus (o mecanismo de resposta da Comissão a situações de crise), o mecanismo de resposta do SEAE a situações de crise, o Mecanismo de Proteção Civil da União e o protocolo de resposta de emergência dos serviços policiais da UE.

[160] Além disso, poderão também ser invocados o artigo 42.º, n.º 7, do Tratado da União Europeia (cláusula de assistência mútua) ou o artigo 222.º do Tratado sobre o Funcionamento da União Europeia (cláusula de solidariedade).

[161] Comissão Europeia/Serviço Europeu para a Ação Externa, *ibid*., JOIN(2018) 16, de 13 de junho de 2018. Em dezembro de 2018, a comunicação social noticiou que a rede de comunicações diplomáticas do SEAE (COREU) tinha sido alegadamente pirateada (fonte: New York Times, *Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran* (Telegramas europeus pirateados revelam grandes ansiedades sobre Trump, a Rússia e o Irão), 18 de dezembro de 2018). A questão está atualmente sob investigação.

[162] Também é necessário desenvolver a cooperação sobre os alertas precoces e a assistência mútua. Ver *Conclusões do Conselho sobre a resposta coordenada da UE a incidentes e crises de cibersegurança de grande escala*, documento 10085/18, de 26 de junho de 2018.

[163] Serviço de Estudos do Parlamento Europeu, *Briefing EU Legislation in Progress: ENISA and a new cybersecurity act* (*Briefing* sobre a legislação da UE em curso: a ENISA e um novo regulamento sobre a cibersegurança), PE 614.643, setembro de 2018.

[164] Comité Económico e Social Europeu, *ibid*., março de 2018.

[165] Conselho da União Europeia, *EU Law Enforcement Emergency Response Protocol (LE ERP) for Major Cross-Border Cyber-Attacks* (Protocolo de resposta de emergência dos serviços policiais da UE para ataques informáticos transfronteiriços de grande escala), documento 14893/18, de dezembro de 2018.

[166] Equipas de resposta rápida a ciberataques e assistência mútua no domínio da cibersegurança; plataforma de partilha de informações relativas às ciberameaças e à resposta a incidentes informáticos. Fonte: Conselho da União Europeia, *Permanent Structured Cooperation (PESCO) updated list of PESCO projects – Overview* (Cooperação Estruturada Permanente (CEP) – Lista atualizada de projetos da CEP – Visão global), de 19 de novembro de 2018.

[167] Conselho da União Europeia, Conclusões sobre o quadro para uma resposta diplomática conjunta da UE às ciberatividades maliciosas, documento 9916/17, de 7 de junho de 2017.

[168] Conselho da União Europeia, *Conclusões do Conselho sobre a ciberdiplomacia*, documento 6122/55, de 11 de fevereiro de 2015.

[169] Conselho da União Europeia, *Draft implementing guidelines for the Framework on a Joint Diplomatic Response to Malicious Cyber Activities* (Projeto de orientações de execução do quadro para uma resposta diplomática conjunta às ciberatividades maliciosas), documento 13007/17.

[170] A atribuição da responsabilidade por um incidente continua a ser uma decisão política soberana dos Estados-Membros, e nem todas as medidas do conjunto de instrumentos exigem essa atribuição.

[171] O conjunto de instrumentos não conduziu à ação conjunta; os Estados-Membros acolheram individualmente a posição dos Estados Unidos.

[172] Conselho da União Europeia, *Conclusões sobre ciberatividades maliciosas*, documento 7925/18, de 16 de abril de 2018.

[173] Sistemas informáticos utilizados para o controlo de processos em diversos setores, tais como serviços de utilidade pública, fabrico de produtos químicos e industriais, transformação de produtos alimentares, sistemas e plataformas de transporte e serviços logísticos.

[174] ENISA, *ibid*., dezembro de 2017.

[175] Por exemplo, as administrações públicas, as indústrias química e nuclear, a produção industrial, a transformação de produtos alimentares, o turismo, a logística e a proteção civil.

[176] Comissão Europeia, *ibid*., SWD(2017) 295 final, de 13 de setembro de 2017.

[177] Discurso da Comissária Věra Jourová na sessão plenária do Parlamento Europeu sobre *Reforçar a resiliência da UE contra a influência de intervenientes externos na próxima campanha eleitoral do PE*, 14 de novembro de 2018.

[178] *Carnegie Endowment for International Peace*, E. Brattberg e T. Maurer, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks* (A interferência russa nas eleições: a luta da Europa contra as notícias falsas e os ataques informáticos), 23 de maio de 2018.

[179] Centro Europeu de Estratégia Política, L. Past, *Cybersecurity of Election Technology: Inevitable Attacks and Variety of Responses* (A cibersegurança da tecnologia nas eleições: ataques inevitáveis e a diversidade das respostas), em: "*Election Interference in the Digital Age – Building Resilience to Cyber-Enabled Threats: A collection of think pieces of 35 leading practitioners and experts*" (A interferência eleitoral na era digital – reforçar a resiliência a ameaças possibilitadas pelo ciberespaço: recolha de artigos de reflexão de 35 eminentes profissionais e peritos), 2018.

[180] Segundo a Diretiva 2008/114/CE do Conselho relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção.

[181] Comissão Europeia, Recomendação sobre as redes de cooperação eleitoral, a transparência em linha, a proteção contra os incidentes de cibersegurança e as campanhas de desinformação no âmbito das eleições para o Parlamento Europeu, documento C(2018) 5949, de 12 de setembro de 2018.

[182] Conclusões do Conselho Europeu, documento EUCO 11/15, de 20 de março de 2015. Desde esta data, foram acrescentados dois novos grupos de trabalho, um para os Balcãs Ocidentais e outro para a Vizinhança do Sul.

[183] Um relatório do *Atlantic Council* defendia que a UE deveria exigir que todos os Estados-Membros enviassem peritos para o grupo de trabalho. Ver: D. Fried e A. Polyakova, *Democratic Defense Against Disinformation* (Defesa democrática contra a desinformação), 5 de março de 2018.

[184] Inicialmente desprovida de orçamento próprio, foi-lhe atribuído em 2018 um montante de 1,1 milhões de euros pelo Parlamento Europeu para uma ação preparatória "*StratCom Plus*".

[185] *Carnegie Endowment for International Peace*, E. Brattberg e T. Maurer, *ibid*., 23 de maio de 2018.

[186] Comissão Europeia, Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, *Plano de Ação contra a Desinformação*, JOIN(2018) 36 final. O plano incide na melhoria das capacidades das instituições da UE para detetar, analisar e expor a desinformação; no reforço de respostas coordenadas e conjuntas; na mobilização do setor privado; na sensibilização e na melhoria da resiliência societal.

[187] Comissão Europeia, *Combater a desinformação em linha: uma estratégia europeia*, COM(2018) 236 final, de 26 de abril de 2018.

[188] Não confundir com o código de conduta para lutar contra o discurso ilegal de incitação ao ódio *online*.

[189] JRC, *The digital transformation of news media and the rise of disinformation and fake news* (A transformação digital dos meios de comunicação social e o aumento da desinformação e das notícias falsas), relatórios técnicos do JRC, documento de trabalho do JRC sobre a economia digital 2018-02, abril de 2018.

[190] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News")* (Reforçar a segurança das redes e da informação e proteger contra a desinformação *online* (notícias falsas), abril de 2018

[191] Centro Europeu de Estratégia Política, C. Frutos López, *A Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats* (A responsabilidade de apoiar a organização de eleições na antecipação e luta contra as ciberameaças), *ibid*., 2018.

[192] Comissão Europeia, *ibid*., SWD(2018) 403 final, de 12 de setembro de 2018.

[193] A proposta de regulamento (COM(2017) 487 final, de 13 de setembro de 2017) relativa à análise dos investimentos diretos estrangeiros, apresentada em setembro de 2017, está atualmente em tramitação no processo legislativo. A proposta cobre especificamente as

tecnologias de importância crítica, entre as quais a inteligência artificial, a cibersegurança e as aplicações de dupla utilização.

[194] Comissão Europeia/Serviço Europeu para a Ação Externa, *ibid*., JOIN(2017) 450 final, de 13 de setembro de 2017.

Equipa do TCE

O presente documento informativo, intitulado *Desafios à eficácia da política de cibersegurança da UE*, foi adotado pela Câmara de Auditoria III, responsável pela auditoria às despesas das ações externas, segurança e justiça, presidida pelo Membro do TCE Bettina Jakobsen. A tarefa foi realizada sob a responsabilidade do Membro do TCE Baudilio Tomé Muguruza, com a colaboração de Daniel Costa de Magalhães, chefe de gabinete, e Ignacio García de Parada, assessor de gabinete; Alejandro Ballester-Gallardo, responsável principal; Michiel Sweerts, responsável de tarefa; Simon Dennett, Aurelia Petliza, Mirko Iaconisi, Michele Scardone e Sílvia Monteiro da Cunha, auditores, bem como de Johannes Bolkart, estagiário. Hannah Critoph prestou assistência linguística.

Da esquerda para a direita: Ignacio García de Parada, Sílvia Monteiro da Cunha, Michele Scardone, Michiel Sweerts, Mirko Iaconisi, Baudilio Tomé Muguruza, Simon Dennett, Hannah Critoph e Daniel Costa de Magalhães.

TRIBUNAL DE CONTAS EUROPEU

Serviço das Publicações

TRIBUNAL DE CONTAS EUROPEU
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tel. +352 4398-1

Informações: eca.europa.eu/pt/Pages/ContactForm.aspx
Sítio Internet: eca.europa.eu
Twitter: @EUAuditors