COMISSÃO
EUROPEIA

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

Bruxelas, 16.12.2020
JOIN(2020) 18 final

COMUNICAÇÃO CONJUNTA AO PARLAMENTO EUROPEU E AO CONSELHO

Estratégia de cibersegurança da UE para a década digital

COMUNICAÇÃO CONJUNTA AO PARLAMENTO EUROPEU E AO CONSELHO

Estratégia de cibersegurança da UE para a década digital

I. INTRODUÇÃO: UMA TRANSFORMAÇÃO DIGITAL CIBERSEGURA NUM CENÁRIO DE AMEAÇAS COMPLEXO

A cibersegurança é parte integrante da segurança dos europeus. Quer se trate de dispositivos conectados, redes elétricas, bancos, aeronaves, administrações públicas ou hospitais, as pessoas têm direito a utilizá-los ou frequentá-los com a garantia de que estarão protegidas contra ciberameaças. Mais do que nunca, a economia, a democracia e a sociedade na UE estão dependentes de ferramentas e ligações digitais seguras e fiáveis. A cibersegurança afigura-se, portanto, essencial para construir uma Europa resiliente, ecológica e digital.

Os transportes, a energia, a saúde, as telecomunicações, o sistema financeiro, a segurança, os processos democráticos, o espaço e a defesa são domínios que dependem em larga medida de redes e de sistemas de informação cada vez mais interligados. As interdependências transetoriais são muito fortes, dado que as redes e os sistemas de informação dependem, por sua vez, de um fornecimento de eletricidade estável para poderem funcionar. O número de dispositivos conectados já supera a população do planeta, prevendo-se que atinja 25 mil milhões até 2025[1]: um quarto destes dispositivos estará na Europa. A pandemia de COVID-19 veio acelerar a digitalização dos modelos de trabalho, tendo 40 % dos trabalhadores da UE passado para o regime de teletrabalho, com prováveis efeitos permanentes na vida quotidiana[2]. Esta mudança aumenta as vulnerabilidades perante ciberataques[3]. Em muitos casos, os objetos conectados são entregues ao consumidor com vulnerabilidades conhecidas, ampliando assim a superfície de ataque das ciberatividades maliciosas[4]. O panorama industrial da UE é cada vez mais digitalizado e conectado, mas tal significa igualmente que os ciberataques podem ter um impacto maior do que nunca nas indústrias e nos ecossistemas.

---

[1] Estimativa da associação empresarial do setor das telecomunicações GSMA: https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf. A International Data Corporation prevê um número de 42,6 mil milhões de máquinas, sensores e câmaras conectados: https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] Num inquérito realizado em junho de 2020, 47 % dos dirigentes de empresas afirmaram que tencionavam dar aos seus funcionários a possibilidade de trabalhar à distância a tempo inteiro mesmo depois de ser possível voltar ao local de trabalho; 82 % tencionavam permitir o trabalho à distância pelo menos durante uma parte do tempo: https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time.

[3] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf.

[4] Um dos *software* maliciosos mais prejudiciais até à data, conhecido como Mirai, criou redes zômbis em mais de 600 000 dispositivos que provocaram perturbações em numerosos sítios Web na Europa e nos Estados Unidos.

O cenário de ameaças é constituído por tensões geopolíticas relativamente à Internet mundial e aberta e relativamente ao controlo das tecnologias em toda a cadeia de abastecimento[5]. Estas tensões refletem-se no número crescente de Estados-nação que têm levantado fronteiras digitais. As restrições da Internet e no seio da mesma ameaçam o ciberespaço mundial e aberto, bem como o Estado de direito, os direitos fundamentais, a liberdade e a democracia — os valores fundamentais da UE. O ciberespaço é cada vez mais explorado para fins políticos e ideológicos, e a crescente polarização à escala internacional está a dificultar um multilateralismo eficaz. As ameaças híbridas combinam campanhas de desinformação com ciberataques a infraestruturas, processos económicos e instituições democráticas, tendo capacidade para causar danos materiais, conseguir acesso ilegal a dados pessoais, furtar segredos industriais ou de Estado, gerar desconfiança e enfraquecer a coesão social. Estas atividades põem em causa a segurança e a estabilidade no plano internacional e os benefícios que o ciberespaço proporciona ao desenvolvimento económico, social e político.

Os ataques direcionados contra infraestruturas críticas representam um risco significativo a nível mundial[6]. A Internet tem uma arquitetura descentralizada, sem nenhuma estrutura central e com uma governação multilateral. Tem logrado manter aumentos exponenciais nos volumes de tráfego, isto apesar de ser constantemente alvo de tentativas de perturbação maliciosas[7]. Ao mesmo tempo, observa-se uma crescente dependência das principais funções da Internet global e aberta, mais concretamente o Sistema de Nomes de Domínio (DNS), e dos serviços essenciais da Internet nos domínios das comunicações e alojamento, aplicações e dados. Estes serviços estão cada vez mais concentrados nas mãos de um pequeno número de empresas privadas[8], deixando a economia e sociedade europeias vulneráveis perante acontecimentos disruptivos no plano geopolítico ou técnico que afetam a essência da Internet ou uma ou mais das referidas empresas. A maior utilização da Internet e a alteração dos hábitos decorrentes da pandemia tornaram ainda mais patente a fragilidade das cadeias de abastecimento que dependem destas infraestruturas digitais.

As preocupações de segurança são um grande desincentivo à utilização dos serviços em linha[9]**.** Cerca de dois quintos dos utilizadores na UE já tiveram problemas relacionados com a segurança e três quintos sentem-se incapazes de se protegerem contra a

[5] Nomeadamente as tecnologias de componentes eletrónicos, de análise de dados, de computação em nuvem, de redes mais rápidas e inteligentes com sistemas 5G e superiores, de cifragem e de inteligência artificial (IA) e novos paradigmas de computação e de tratamento de dados de confiança, tais como as cadeias de blocos, as tecnologias da nuvem para a periferia («cloud-to-edge») e a computação quântica.

[6] Fórum Económico Mundial, *Global Risks Report 2020*.

[7] A pandemia resultou num aumento de 60 % do tráfego na Internet, segundo a Organização de Cooperação e de Desenvolvimento Económicos: https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/. O Organismo dos Reguladores Europeus das Comunicações Eletrónicas e a Comissão publicam regularmente relatórios sobre o estado da capacidade de Internet durante as medidas de confinamento associadas ao coronavírus. Segundo um relatório da ENISA, durante o terceiro trimestre de 2019, registou-se um aumento de 241 % no número de ataques distribuídos de negação de serviço em relação ao terceiro trimestre de 2018. A intensidade deste tipo de ataque tem vindo a crescer, tendo o maior ataque de sempre ocorrido em fevereiro de 2020, com um pico de tráfego que atingiu 2,3 terabits por segundo. Na «interrupção da CenturyLink» de agosto de 2020, um problema de encaminhamento no fornecedor de serviços de Internet norte-americano provocou uma queda de 3,5 % do tráfego mundial na Internet: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service.

[8] Internet Society, *The Global Internet Report: Consolidation in the Internet Economy*: https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/.

[9] https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG.

cibercriminalidade[10]. Um terço recebeu, nos últimos três anos, mensagens de correio eletrónico fraudulentas ou chamadas telefónicas a solicitar dados pessoais, mas 83 % nunca denunciaram um cibercrime. Uma em cada oito empresas já foi afetada por ciberataques[11]. Mais de metade dos computadores pessoais (PC) de empresas e particulares que sofrem uma infeção com programas maliciosos voltam a ser infetados no mesmo ano[12]. Todos os anos, perdem-se centenas de milhões de registos devido a violações de dados; o custo médio por empresa de uma violação de dados ascendeu a mais de 3,5 milhões de EUR em 2018[13]. Em muitos casos, não é possível isolar os efeitos de um ciberataque, que podem desencadear reações em cadeia na economia e na sociedade, afetando milhões de pessoas[14].

A investigação de quase todos os tipos de crime tem uma vertente digital. Em 2019, apurou-se que o número de incidentes triplicou em termos homólogos. Estima-se que existam 700 milhões de novas amostras de programas maliciosos — o meio mais frequente de efetuar um ciberataque[15]. As estimativas apontam para que, em 2020, o custo anual da cibercriminalidade para a economia mundial seja de 5,5 biliões de EUR, o dobro em relação a 2015[16]. Este valor representa a maior transferência de riqueza económica da história, superando o tráfico de droga mundial. Relativamente a um incidente de grande escala, nomeadamente o ataque com o programa de sequestro WannaCry em 2017, estima-se que o custo para a economia mundial tenha sido superior a 6,5 mil milhões de EUR[17].

Os serviços digitais e o setor financeiro estão entre os alvos mais frequentes dos ciberataques, a par do setor público e da indústria transformadora. Ainda assim, a prontidão e sensibilização das empresas e dos particulares para as questões digitais mantêm-se em níveis baixos[18], verificando-se um grande défice de qualificações de cibersegurança na mão de obra[19]. Em 2019, registaram-se perto de 450 incidentes de cibersegurança que afetaram infraestruturas críticas europeias em domínios como o sistema financeiro e a energia[20]. As organizações e os profissionais de saúde foram atingidos de forma particularmente grave durante a pandemia. Com a ligação cada vez mais indissociável entre a tecnologia e o mundo físico, os ciberataques põem em risco a vida e o bem-estar dos

[10] *2020 Digital Economy and Society Index*; https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG.
[11] Eurostat, comunicado de imprensa, «ICT security measures taken by vast majority of enterprises in the EU», 6/2020, 13 de janeiro de 2020. Fórum Económico Mundial, «Cyberattacks on critical infrastructure have become the new normal across sectors such as energy, healthcare and transportation», *Global Risks Report 2020*.
[12] Fonte: Comparitech.
[13] Ponemon Institute, *Annual Cost of a Data Breach Report*, 2020, com base numa análise quantitativa de 524 violações recentes em 17 geografias e 17 setores: https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf.
[14] JRC, *Cybersecurity – Our digital anchor*: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor.
[15] Fonte: AV-TEST, https://www.av-test.org/en/statistics/malware/.
[16] JRC, *Cybersecurity – Our Digital Anchor*.
[17] Fonte: Cyence.
[18] As empresas continuam a demonstrar um nível reduzido de sensibilização para os furtos informáticos de segredos comerciais, especialmente as PME. PwC, *The scale and impact of industrial espionage and theft of trade secrets through cyber: Dissemination report on measures to tackle and prevent cyber-theft of trade secrets*, 2018.
[19] Ver ENISA, *Threat Landscape 2020*. Ver também Verizon, *Data Breach Investigations Report 2020*: https://enterprise.verizon.com/resources/reports/dbir/.
[20] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f.

mais vulneráveis[21]. Considera-se que mais de dois quintos das empresas, principalmente PME, são «principiantes» no domínio da cibersegurança, estimando-se que as empresas europeias estão menos bem preparadas do que as suas congéneres da Ásia e da América[22]. Calcula-se que continuem por preencher cerca de 291 000 vagas de profissionais da cibersegurança na Europa. A contratação e a formação de peritos em cibersegurança são processos lentos, dando azo a um acréscimo dos riscos de cibersegurança para as organizações[23].

A UE carece de um conhecimento situacional coletivo das ciberameaças. Tal deve-se ao facto de as autoridades nacionais não recolherem e partilharem de forma sistemática informações — por exemplo, os dados disponíveis no setor privado — que poderiam ajudar a avaliar o estado da cibersegurança na UE. Apenas uma fração dos incidentes é comunicada pelos Estados-Membros e a partilha de informações não é sistemática nem exaustiva[24]; os ciberataques podem ser apenas uma faceta de ataques maliciosos concertados contra as sociedades europeias. Atualmente, a assistência operacional mútua dos Estados-Membros é reduzida, não existindo nenhum mecanismo operacional entre os Estados-Membros e as instituições, agências e organismos da UE para a eventualidade de ciberincidentes ou cibercrises transfronteiras de grande escala[25].

Melhorar a cibersegurança é, por conseguinte, fundamental para que os cidadãos confiem, utilizem e tirem proveito da inovação, conectividade e automatização, bem como para proteger os direitos e as liberdades fundamentais, incluindo os direitos à vida privada e à proteção dos dados de caráter pessoal, e a liberdade de expressão e de informação. A cibersegurança é indispensável para a conectividade à rede e para a Internet aberta e mundial que deve apoiar a transformação da economia e da sociedade na década de 2020. Contribui para melhores e mais empregos, locais de trabalho mais flexíveis, transportes e agricultura mais eficientes e sustentáveis e um acesso mais fácil e equitativo aos serviços de saúde. A cibersegurança é igualmente essencial com vista à transição para energia mais limpa, no quadro do Pacto Ecológico Europeu[26], por meio de redes transfronteiras e contadores inteligentes e evitando a duplicação desnecessária do armazenamento de dados. Por último, é crucial para a segurança e a estabilidade no plano internacional e para o desenvolvimento das economias, das democracias e das sociedades à escala mundial. Os governos, as empresas e os particulares terão, portanto, de utilizar as ferramentas digitais de forma responsável e tendo consciência das questões de segurança. A sensibilização e a «higiene» no domínio da cibersegurança devem apoiar a transformação digital das atividades quotidianas.

A nova estratégia de cibersegurança da UE para a década digital é parte integrante da estratégia intitulada «Construir o futuro digital da Europa»[27], do plano de recuperação da

[21] Têm sido utilizados programas de sequestro para visar hospitais e registos de saúde, por exemplo, na Roménia (junho de 2020), em Düsseldorf (setembro de 2020) e em Vastaamo (outubro de 2020).
[22] PwC, *The Global State of Information Security 2018*; ESI ThoughLlab, *The Cybersecurity Imperative*, 2019.
[23] ENISA, *Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database*, dezembro de 2019.
[24] Nos termos do artigo 10.º, n.º 3, da Diretiva Segurança das Redes e da Informação [Diretiva (UE) 2016/1148], os Estados-Membros devem apresentar um relatório de síntese anual ao grupo de cooperação sobre as notificações recebidas.
[25] Estão instituídos procedimentos operacionais normalizados para uma assistência mútua entre os membros da rede de CSIRT.
[26] Pacto Ecológico Europeu [COM(2019) 640 final].
[27] Construir o futuro digital da Europa [COM(2020) 67 final].

Europa da Comissão[28], da Estratégia da UE para a União da Segurança 2020-2025[29], da Estratégia Global para a Política Externa e de Segurança da UE[30] e da Nova Agenda Estratégica do Conselho Europeu para 2019-2024[31]. A estratégia define a abordagem que a UE vai seguir para proteger os seus cidadãos, empresas e instituições contra as ciberameaças, aumentar a cooperação internacional e assegurar a liderança na proteção de uma Internet aberta e mundial.

II. PENSAR À ESCALA MUNDIAL, AGIR DE FORMA EUROPEIA

A presente estratégia visa assegurar uma Internet mundial e aberta com barreiras de segurança firmes, com vista a enfrentar os riscos que se colocam à segurança e aos direitos e liberdades fundamentais das pessoas na Europa. Dando sequência aos progressos alcançados no âmbito das estratégias anteriores, a estratégia contém propostas concretas relativas ao estabelecimento de **três instrumentos principais — instrumentos de regulamentação, de investimento e de política —** para intervir em **três domínios de ação da UE: 1) resiliência, soberania tecnológica e liderança; 2) criação de capacidade operacional para prevenir, dissuadir e responder; e 3) promoção de um ciberespaço mundial e aberto.** A UE está empenhada em apoiar esta estratégia mediante um **nível de investimento sem precedentes na transição digital da UE ao longo dos próximos sete anos** — que poderá atingir o quádruplo dos níveis anteriores —, no âmbito de novas políticas tecnológicas e industriais e da agenda de recuperação[32].

A cibersegurança deve ser integrada em todos estes investimentos no domínio digital, particularmente em tecnologias fulcrais, como a inteligência artificial (IA), a cifragem e a computação quântica, recorrendo a incentivos, obrigações e parâmetros de referência. Esta medida pode estimular o crescimento da indústria europeia da cibersegurança e conferir o grau de certeza necessário para facilitar a eliminação gradual dos sistemas herdados. O Fundo Europeu de Defesa (FED) apoiará soluções europeias de ciberdefesa, no âmbito de uma base tecnológica e industrial de defesa europeia. A cibersegurança faz parte dos instrumentos de financiamento externo destinados a apoiar os parceiros da UE, mais concretamente o Instrumento de Vizinhança, de Cooperação para o Desenvolvimento e de Cooperação Internacional. Prevenir a utilização abusiva das tecnologias, proteger as infraestruturas críticas e garantir a integridade das cadeias de abastecimento permite igualmente à UE respeitar as normas, regras e princípios das Nações Unidas sobre o comportamento responsável dos Estados[33].

---

[28] A Hora da Europa: Reparar os Danos e Preparar o Futuro para a Próxima Geração [COM(2020) 456 final].
[29] Estratégia da UE para a União da Segurança 2020-2025 [COM(2020) 605 final].
[30] https://eeas.europa.eu/topics/eu-global-strategy_en.
[31] https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/#.
[32] Os investimentos em toda a cadeia de abastecimento das tecnologias digitais, que representarão contribuições para a transição digital ou soluções para os desafios dela decorrentes, deverão ascender a pelo menos 20 % (o equivalente a 134,5 mil milhões de EUR) dos 672,5 mil milhões de EUR do Mecanismo de Recuperação e Resiliência, em subvenções e empréstimos. O financiamento da UE previsto no quadro financeiro plurianual para 2021-2027 para a cibersegurança no âmbito do programa Europa Digital e para a investigação no domínio da cibersegurança ao abrigo do programa Horizonte Europa (com uma tónica especial no apoio às PME) poderá atingir um montante total de 2 000 milhões de EUR, a somar aos investimentos dos Estados-Membros e da indústria.
[33] https://undocs.org/A/70/174.

1 RESILIÊNCIA, SOBERANIA TECNOLÓGICA E LIDERANÇA

As infraestruturas críticas e os serviços essenciais da UE estão cada vez mais interdependentes e digitalizados. Tudo o que está ligado à Internet na UE, quer se trate de veículos automatizados, sistemas de controlo industrial ou eletrodomésticos, e o conjunto das cadeias de abastecimento que os disponibilizam têm de ser seguros desde a conceção, resilientes a ciberincidentes e prontamente corrigidos quando são detetadas vulnerabilidades. Trata-se de um aspeto fundamental para que os setores público e privado da UE tenham a possibilidade de escolha entre as infraestruturas e os serviços mais seguros. A próxima década será uma oportunidade para a UE assumir a dianteira no desenvolvimento de tecnologias seguras em toda a cadeia de abastecimento. A fim de assegurar a resiliência e capacidades industriais e tecnológicas mais sólidas na cibersegurança, devem ser mobilizados todos os instrumentos necessários de regulamentação, de investimento e de política. A cibersegurança desde a fase de conceção para processos, operações e dispositivos industriais pode atenuar os riscos, proporcionar uma redução dos custos, tanto para as empresas, como para a sociedade em geral, e aumentar, deste modo, a resiliência.

1.1 Infraestruturas resilientes e serviços críticos

As **regras da UE relativas à segurança das redes e da informação (SRI)** são centrais no mercado único da cibersegurança. A Comissão propõe reformar estas regras no âmbito de uma Diretiva SRI revista, com o intuito de incrementar o nível de **ciber-resiliência de todos os setores, quer públicos quer privados, que desempenham uma função importante para a economia e a sociedade[34].** Esta revisão é necessária para diminuir as incoerências no conjunto do mercado único, mediante um alinhamento dos requisitos relativos ao âmbito de aplicação, à segurança e à comunicação de incidentes, da supervisão e aplicação ao nível nacional e das atribuições das autoridades competentes.

Uma Diretiva SRI revista servirá de base a regras mais específicas que são igualmente necessárias para setores estrategicamente importantes, nomeadamente a energia, os transportes e a saúde. A fim de assegurar uma abordagem coerente, conforme anunciado na Estratégia para a União da Segurança 2020-2025, a proposta de diretiva revista é apresentada juntamente com uma revisão da legislação em matéria de resiliência das infraestruturas críticas[35]. As tecnologias energéticas que incorporam componentes digitais e a segurança das respetivas cadeias de abastecimento são importantes para a continuidade dos serviços essenciais e para o controlo estratégico de infraestruturas energéticas críticas. Por conseguinte, a Comissão proporá medidas a serem adotadas até ao final de 2022, incluindo um «código de rede» destinado a estabelecer regras aplicáveis à cibersegurança nos fluxos transfronteiriços de eletricidade. O setor financeiro deve igualmente reforçar a resiliência operacional digital e assegurar uma capacidade para enfrentar todos os tipos de perturbações e ameaças relacionadas com as tecnologias da informação e comunicação (TIC), tal como proposto pela Comissão[36]. No que respeita aos transportes, a Comissão aditou disposições sobre cibersegurança[37] à legislação da UE em matéria de segurança da aviação e prosseguirá os seus esforços com vista a aumentar a ciber-resiliência em todos os modos de transporte. O

[34] [*inserir referência à proposta de Diretiva SRI*].
[35] [inserir referência à *proposta* de diretiva relativa à resiliência das entidades críticas].
[36] Proposta de regulamento relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 e (UE) n.º 909/2014 [COM(2020) 595 final).
[37] Regulamento de Execução (UE) 2019/1583 da Comissão.

reforço da ciber-resiliência dos **processos democráticos e das instituições** é um elemento nuclear do Plano de Ação para a Democracia Europeia no que respeita à garantia e à promoção de eleições livres, do discurso democrático e da pluralidade dos meios de comunicação social[38]. Por último, relativamente à segurança das infraestruturas e dos serviços no âmbito do futuro Programa Espacial, a Comissão continuará a aprofundar a estratégia de cibersegurança do Galileo para a próxima geração de serviços do sistema mundial de navegação por satélite, bem como outras componentes do Programa Espacial[39].

1.2 Construir um ciberescudo europeu

Atendendo à disseminação da conectividade e à sofisticação cada vez maior dos ciberataques, os centros de partilha e análise de informações (ISAC) desempenham uma importante função, incluindo ao nível setorial, ao permitirem o intercâmbio entre vários intervenientes de informações sobre ciberameaças[40]. Acresce que as redes e os sistemas informáticos requerem um acompanhamento e uma análise em permanência, por forma a detetar intrusões e anomalias em tempo real. Por conseguinte, muitas empresas privadas, organizações públicas e autoridades nacionais criaram equipas de resposta a incidentes de segurança informática (CSIRT) e centros de operações de segurança.

Estes centros de operações de segurança têm um papel essencial na recolha de registos[41] e no isolamento de ocorrências suspeitas nas redes de comunicação que monitorizam. Para o efeito, recorrem à identificação de sinais e padrões e à extração de conhecimento sobre ameaças a partir das grandes quantidades de dados que é necessário avaliar. Têm contribuído para a deteção das atividades de ficheiros executáveis maliciosos e, por outro lado, ajudado a conter os ciberataques. O trabalho pedido a estes centros é muito exigente e caracteriza-se por um ritmo acelerado, motivo pelo qual a IA e, mais concretamente, as técnicas de aprendizagem automática podem prestar um apoio inestimável aos profissionais[42].

A Comissão propõe desenvolver uma **rede de centros de operações de segurança em toda a UE[43]**, bem como apoiar a melhoria dos centros existentes e o estabelecimento de novos centros. Além disso, prestará assistência à formação e ao desenvolvimento das qualificações do pessoal com funções nesses centros. A Comissão poderá afetar, com base numa análise das necessidades levada a cabo com as partes interessadas e apoiada pela Agência da UE para a Cibersegurança (ENISA), mais de 300 milhões de EUR ao apoio à cooperação entre entidades públicas e privadas e transfronteiras na criação de redes nacionais e setoriais, que

[38] Comunicação sobre o Plano de Ação para a Democracia Europeia [COM(2020) 790]. Ao abrigo deste plano e da Rede Europeia de Cooperação para as Eleições, as redes eleitorais dos Estados-Membros apoiarão o destacamento de equipas conjuntas de peritos a fim de combater as ameaças — incluindo ciberameaças — aos processos eleitorais: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en.

[39] Incluem-se a nova iniciativa relativa às comunicações governamentais por satélite (GOVSATCOM) e os detritos espaciais (SST).

[40] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.

[41] De um modo que permita às autoridades policiais e judiciárias utilizá-los como meios de prova.

[42] Fonte: Ponemon Institute Research, *Improving the Effectiveness of the SOC*, 2019; quanto a estudos sobre a utilização da IA nos centros de operações de segurança, ver, por exemplo: Khraisat, A., Gondal, I., Vamplew, P., *et al.*, «Survey of intrusion detection systems: techniques, datasets and challenges», *Cybersecurity*, 2, 20, 2019.

[43] Serão desenvolvidos mecanismos mais detalhados relativos à governação, aos princípios de funcionamento e ao financiamento destes centros, bem como à forma como complementarão as estruturas existentes, tais como os polos de inovação digital.

envolva igualmente as PME, assentando em mecanismos de governação, de partilha de dados e de segurança adequados.

Os Estados-Membros são encorajados a coinvestir neste projeto. Os centros poderão, assim, ser capazes de partilhar e correlacionar de forma mais eficiente os sinais detetados e de gerar informações de elevada qualidade sobre ciberameaças, a partilhar com os ISAC e as autoridades nacionais, permitindo, deste modo, um conhecimento situacional mais completo. A finalidade seria ligar, de forma faseada, o máximo de centros possível em toda a UE, no sentido de gerar um conhecimento coletivo e de partilhar boas práticas. Será concedido apoio a estes centros, a fim de melhorar a deteção de incidentes, a análise e os tempos de resposta através de IA de ponta e de funções de aprendizagem automática, que será complementado por infraestruturas de supercomputação desenvolvidas na UE pela Empresa Comum para a Computação Europeia de Alto Desempenho[44].

Mediante a colaboração e cooperação contínuas, esta rede alertará, em tempo útil, as autoridades e todas as partes interessadas, incluindo a ciberunidade conjunta (ver secção 2.1), para incidentes de cibersegurança. **Funcionará como verdadeiro escudo de cibersegurança para a UE**, proporcionando um agregado consistente de torres de vigilância capazes de detetar ameaças potenciais antes de estas poderem causar danos em grande escala.

1.3 Uma infraestrutura de comunicação ultrassegura

O sistema de comunicações governamentais por satélite da União Europeia[45], uma componente do Programa Espacial, proporcionará capacidades de comunicação espacial seguras e económicas a missões e operações críticas no plano da segurança geridas pela UE e pelos seus Estados-Membros, incluindo os intervenientes no domínio da segurança nacional e as instituições, organismos e agências da UE.

Os Estados-Membros comprometeram-se a trabalhar em conjunto com a Comissão no desenvolvimento de uma infraestrutura de comunicação quântica (QCI) segura para a Europa[46]. Com a QCI, as entidades públicas terão ao seu dispor uma forma completamente nova de transmitir informação confidencial por meio de um método de cifragem ultrasseguro, destinado a servir de escudo contra ciberataques, e desenhado com tecnologia europeia. A QCI terá duas componentes principais: as redes terrestres de comunicação por fibra existentes, que interligam sítios estratégicos à escala nacional e transfronteiras; e satélites espaciais ligados que abrangem todo o território da UE, incluindo os territórios ultramarinos[47]. Esta iniciativa, tendente a desenvolver e implementar métodos de cifragem

[44] https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking.
[45] O GOVSATCOM é uma componente do Programa Espacial da União.
[46] A Declaração EuroQCI foi assinada pela maioria dos Estados-Membros, devendo o desenvolvimento e implantação de infraestruturas decorrer no período de 2021-2027 com o financiamento dos programas Horizonte Europa e Europa Digital, bem como da Agência Espacial Europeia, ao abrigo dos mecanismos de governação aplicáveis: https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network.
[47] O desenvolvimento de uma componente espacial é necessário para alcançar ligações ponto a ponto de grande distância (> 1000 km) que as infraestruturas terrestres não conseguem assegurar. Explorando as propriedades da mecânica quântica, a QCI permitirá às partes, num primeiro momento, partilhar chaves secretas aleatórias de forma segura, que deverão ser utilizadas para encriptar e desencriptar mensagens. Além disso, abrangerá a implantação de uma infraestrutura de teste e conformidade, com o intuito de avaliar a conformidade com a QCI dos dispositivos e sistemas europeus de comunicação quântica, bem como a sua certificação e validação antes da respetiva integração na QCI. Será concebida para apoiar aplicações adicionais à medida que estas atingirem o

mais seguros, assim como delinear novas formas de proteger ativos de comunicação e dados críticos, pode contribuir para manter em segurança informações sensíveis e infraestruturas críticas.

Neste contexto, seguindo uma abordagem prospetiva, a Comissão analisará a possível implantação de um sistema multiorbital de conectividade seguro. Tendo por base o GOVSATCOM e a QCI, poderá integrar tecnologias de ponta (tecnologias quânticas, 5G, IA, computação periférica) conformes com o mais rigoroso quadro de cibersegurança, a fim de apoiar serviços seguros desde a conceção, tais como uma conectividade fiável, segura e com uma boa relação custo-eficácia e comunicações encriptadas para atividades governamentais críticas.

1.4 Segurança da próxima geração de redes móveis de banda larga

Os cidadãos e as empresas da UE que utilizem aplicações avançadas e inovadoras baseadas nas **redes 5G e de gerações futuras** devem poder contar com os mais elevados padrões de segurança. Os Estados-Membros, em colaboração com a Comissão e com o apoio da ENISA, definiram, no conjunto de instrumentos da UE para as redes 5G[48], de janeiro de 2020, uma abordagem global, objetiva e assente no risco em matéria de cibersegurança das redes 5G, que assenta numa avaliação de possíveis planos de atenuação e na identificação das medidas mais eficazes. Além disso, a UE tem vindo a consolidar as suas capacidades no domínio das redes 5G e não só, a fim de evitar dependências e de promover uma cadeia de abastecimento sustentável e diversificada.

Em dezembro de 2020, a Comissão publicou um relatório sobre os impactos da recomendação de 26 de março de 2019 sobre a cibersegurança das redes 5G[49]. O relatório demonstrou que foram realizados progressos significativos desde a aprovação do conjunto de instrumentos e que a maioria dos Estados-Membros está no caminho certo para concluir uma parte considerável da aplicação do conjunto de instrumentos no futuro próximo, não obstante algumas variações e as lacunas subsistentes que já tinham sido assinaladas no relatório intercalar publicado em julho de 2020[50].

Em outubro de 2020, o Conselho Europeu exortou a UE e os Estados-Membros «a fazerem pleno uso do conjunto de instrumentos para a cibersegurança das redes 5G» e «a aplicarem as restrições necessárias aos fornecedores de alto risco no que respeita a ativos essenciais definidos como críticos e sensíveis nas avaliações coordenadas dos riscos ao nível da UE»[51].

Prospetivamente, a UE e os seus Estados-Membros devem assegurar que os riscos identificados tenham sido atenuados de forma satisfatória e coordenada, atendendo principalmente ao objetivo de minimizar a exposição a fornecedores de alto risco e de evitar depender dos mesmos aos níveis nacional e da União, e que eventuais novos desenvolvimentos ou riscos significativos sejam tidos em conta. Os Estados-Membros são

---

nível de maturidade tecnológica necessário. O atual projeto-piloto OpenQKD (https://openqkd.eu/) é um precursor desta infraestrutura de teste e conformidade.

[48]Comunicação da Comissão intitulada «Implantação segura de redes 5G na UE – Aplicação do conjunto de instrumentos da UE» [COM(2020) 50].

[49]Relatório de 15 de dezembro de 2020 sobre os impactos da Recomendação (UE) 2019/534 da Comissão, de 26 de março de 2019, sobre a cibersegurança das redes 5G.

[50]Relatório do grupo de cooperação SRI sobre a aplicação do conjunto de instrumentos, de 24 de julho de 2020.

[51]EUCO 13/20, reunião extraordinária do Conselho Europeu (1 e 2 de outubro de 2020) — Conclusões.

convidados a fazerem pleno uso do conjunto de instrumentos no âmbito dos seus investimentos nas capacidades digitais e na conectividade.

Com base no relatório sobre os impactos da recomendação de 2019, a Comissão insta os Estados-Membros a acelerarem os seus esforços no sentido de concluir a aplicação das principais medidas do conjunto de instrumentos até ao segundo trimestre de 2021. Adicionalmente, exorta os Estados-Membros a prosseguirem o acompanhamento conjunto dos progressos realizados e a garantirem uma maior harmonização das abordagens. No plano da UE, serão visados três objetivos principais para apoiar este processo: garantir uma maior convergência das abordagens de atenuação dos riscos em toda a UE, apoiar continuamente o intercâmbio de conhecimentos e o reforço de capacidades, bem como promover a resiliência das cadeias de abastecimento e outros objetivos estratégicos da UE no domínio da segurança. O apêndice da presente comunicação especifica medidas concretas relacionadas com estes objetivos principais.

A Comissão continuará a colaborar estreitamente com os Estados-Membros para realizar estes objetivos e medidas, com o apoio da ENISA (ver apêndice).

Paralelamente, a abordagem da UE no conjunto de instrumentos para as redes 5G suscitou interesse em países terceiros que estão atualmente a elaborar as suas abordagens para tornar as respetivas redes de comunicação seguras. Os serviços da Comissão, a par do Serviço Europeu para a Ação Externa e da rede de delegações da UE, estão disponíveis para fornecer informações suplementares acerca da sua abordagem abrangente, objetiva e assente no risco a entidades de todo o mundo, caso lhes sejam solicitadas.

1.5 Uma Internet de Coisas Seguras

Qualquer objeto conectado tem vulnerabilidades que podem ser exploradas, com ramificações potencialmente generalizadas. As regras do mercado interno preveem salvaguardas contra produtos e serviços inseguros. A Comissão está a trabalhar com vista a assegurar **soluções de segurança e uma certificação transparentes, no âmbito do Regulamento Cibersegurança**, e a incentivar produtos e serviços seguros sem pôr em causa o desempenho[52]. No primeiro trimestre de 2021, a Comissão adotará o primeiro programa de trabalho evolutivo da União (a atualizar pelo menos de três em três anos), a fim de permitir que a indústria, as autoridades nacionais e os organismos de normalização se preparem com antecedência para os futuros sistemas europeus de certificação da cibersegurança[53]. Com a proliferação da Internet das coisas, impõe-se um reforço das normas aplicáveis, quer para garantir a resiliência geral, quer para fomentar a cibersegurança.

A Comissão equacionará uma abordagem abrangente, incluindo possíveis **novas regras horizontais para melhorar a cibersegurança de todos os produtos conectados e serviços**

[52] Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (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). O Regulamento Cibersegurança promove a certificação das TIC ao nível da UE, com um enquadramento europeu para a certificação da cibersegurança aplicável à criação de sistemas europeus de certificação da cibersegurança voluntários, com o objetivo de assegurar um nível adequado de cibersegurança para os produtos, os serviços e os processos de TIC na União e de reduzir a fragmentação do mercado interno no que toca aos sistemas de certificação da cibersegurança na União. Por outro lado, as empresas de «notação» da cibersegurança estão geralmente sediadas fora da UE, com uma transparência e supervisão limitadas: https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings.

[53] Nos termos do artigo 47.º, n.º 5, do Regulamento Cibersegurança.

conexos colocados no mercado interno[54]. Estas regras podem incluir um **novo dever de diligência para os fabricantes de dispositivos conectados**, que teriam a responsabilidade de eliminar as vulnerabilidades dos programas informáticos, nomeadamente a disponibilização contínua de atualizações de segurança e dos programas, e de assegurar, no fim de vida, a supressão dos dados pessoais e outros dados sensíveis. Estas regras podem reforçar a iniciativa «direito à reparação de *software* obsoleto» apresentada no Plano de Ação para a Economia Circular e complementar as medidas que abordam tipos específicos de produtos, tais como requisitos obrigatórios a propor para o acesso ao mercado de certos produtos sem fios (mediante a adoção de um ato delegado ao abrigo da Diretiva Equipamentos de Rádio[55]) e o objetivo de aplicar regras de cibersegurança para os veículos a motor para todos os novos tipos de veículos a partir de julho de 2022[56]. Além disso, poderão complementar a proposta de revisão das regras gerais de segurança dos produtos, que não se referem diretamente aos aspetos de cibersegurança[57].

1.6 Maior segurança mundial da Internet

Um conjunto de protocolos centrais e de infraestruturas de apoio assegura a funcionalidade e integridade da Internet à escala mundial[58]. Este conjunto inclui o DNS e o seu sistema hierárquico e delegado de zonas, iniciando-se, no topo da hierarquia, com a zona de raiz e os treze servidores de raiz DNS[59], dos quais depende a rede World Wide Web. A Comissão tenciona elaborar **um plano de contingência, apoiado por financiamento da UE, para dar resposta a cenários extremos que afetem a integridade e a disponibilidade do sistema de raiz DNS mundial.** Trabalhará em conjunto com a ENISA, os Estados-Membros, os dois operadores de servidores de raiz DNS da UE[60] e a comunidade multilateral no sentido de avaliar o papel destes operadores para assegurar que a Internet permanece acessível mundialmente em todas as circunstâncias.

Para que um cliente aceda a um recurso sob um nome de domínio específico na Internet, o seu pedido (por norma, de Localizador Uniforme de Recursos, ou URL) deve ser traduzido ou «resolvido» num endereço IP, através de uma referência aos servidores de nome DNS. Contudo, na UE, as pessoas e as organizações estão cada vez mais dependentes de um pequeno número de resolvedores de DNS públicos geridos por entidades não localizadas na

[54] Conclusões do Conselho sobre o apelo a medidas horizontais relativas à cibersegurança dos dispositivos conectados; 13629/20, 2 de dezembro de 2020.
[55] Diretiva 2014/53/UE.
[56] Segue o regulamento da ONU adotado em junho de 2020; http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf.
[57] Revisão das atuais regras gerais de segurança dos produtos (Diretiva 2001/95/CE); também estão previstas regras adaptadas no tocante à responsabilidade dos produtores no ambiente digital, no âmbito do quadro regulamentar da UE em matéria de responsabilidade.
[58] «O núcleo público da internet aberta, ou seja, os seus principais protocolos e infraestruturas, que são um bem público mundial, assegura a principal funcionalidade da internet no seu conjunto e serve de base ao seu funcionamento normal. A ENISA deverá apoiar a segurança do núcleo público da internet aberta e a estabilidade do seu funcionamento, incluindo, entre outros, os protocolos essenciais (nomeadamente, DNS, BGP e IPv6), o funcionamento do sistema de nomes de domínio (tal como o funcionamento de todos os domínios de topo) e o funcionamento da zona de raiz»; considerando 23 do Regulamento Cibersegurança.
[59] https://www.iana.org/domains/root/servers.
[60] Os servidores «i.root», geridos pela Netnod, na Suécia, e os servidores «k.root», geridos pela RIPE NCC, nos Países Baixos.

UE. Esta concentração da resolução de DNS nas mãos de um pequeno número de empresas[61] torna o próprio processo de resolução vulnerável em caso de acontecimentos significativos que afetem um grande fornecedor, dificultando a tarefa das autoridades da UE na resposta a possíveis ciberataques maliciosos e grandes incidentes geopolíticos ou técnicos[62].

Com vista a reduzir os problemas de segurança relacionados com a concentração do mercado, a Comissão promoverá a adoção de uma estratégia de diversificação da resolução de DNS junto das partes interessadas, incluindo as empresas, os fornecedores de serviços Internet e os fornecedores de navegadores da UE. A Comissão pretende igualmente contribuir para tornar a conectividade à Internet segura, apoiando o desenvolvimento de um **serviço público europeu de resolução de DNS**. Esta iniciativa, «DNS4EU», oferecerá um serviço europeu alternativo para aceder à Internet mundial. O DNS4EU será transparente e compatível com as mais recentes normas e regras de segurança, proteção de dados e privacidade desde a conceção e por predefinição, e fará parte da Aliança Industrial Europeia para os Dados e a Nuvem[63].

A Comissão vai igualmente, em articulação com os Estados-Membros e a indústria, **acelerar a adoção de padrões de Internet essenciais, incluindo o IPv6[64], padrões de segurança da Internet bem implantados e boas práticas de DNS, encaminhamento e segurança do correio eletrónico[65]**, não excluindo medidas regulamentares como uma cláusula de caducidade europeia para o Ipv4, a fim de orientar o mercado caso os progressos na sua adoção sejam insuficientes. A UE deve promover (por exemplo, no âmbito da Estratégia UE-África[66]) a aplicação destes novos padrões nos países parceiros, como forma de apoiar o desenvolvimento da Internet mundial e aberta e de contrariar os modelos da Internet fechados e baseados no controlo. Por último, a Comissão aferirá a necessidade de um mecanismo de monitorização e recolha mais sistemáticas de dados agregados no tráfego da Internet e de aconselhamento sobre potenciais perturbações[67].

1.7 Uma presença mais forte na cadeia de abastecimento de tecnologia

Com o apoio financeiro que prevê conceder para a transformação digital cibersegura ao longo do quadro financeiro plurianual para 2021-2027, a UE tem a oportunidade única de reunir os seus ativos para impulsionar a sua Estratégia Industrial[68] e o seu papel de liderança nas

[61] *Consolidation in the DNS resolver market – how much, how fast how dangerous? Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services*.

[62] Também há provas que demonstram que os dados DNS podem ser utilizados para fins de definição de perfis, com repercussões nos direitos à vida privada e à proteção de dados.

[63] Declaração conjunta: *Building the next generation cloud for businesses and the public sector in the EU;* https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe.

[64] A implantação do IPv6 está agora mais adiantada, com a redução drástica da oferta de endereços IPv4 e o aumento do seu custo. Todavia, a implantação do IPv6 não é uniforme no território da UE.

[65] Estes padrões incluem o DNSSEC, HTTPS, DNS sobre HTTPS (DoH), DNS sobre TLS (DoT), SPF, DKIM, /DMARC, STARTTLS, DANE e normas e boas práticas de encaminhamento, por exemplo as normas de acordo mútuo para a segurança do encaminhamento (MANRS).

[66] Comunicação Conjunta intitulada «Rumo a uma estratégia abrangente para África», de 9 de março de 2020 [JOIN(2020) 4 final].

[67] Um «observatório da Internet» desta natureza poderia enquadrar-se no âmbito de atividades do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança; 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].

[68] Comunicação da Comissão intitulada «Uma nova estratégia industrial para a Europa» [COM(2020) 102 final].

tecnologias digitais e na cibersegurança em toda a cadeia de abastecimento digital (incluindo nas tecnologias de dados e de computação em nuvem, nas tecnologias de processadores de próxima geração, na conectividade ultrassegura e nas redes 6G), em consonância com os seus valores e prioridades. A intervenção do setor público deve ter por base os instrumentos definidos no quadro regulamentar da UE em matéria de contratos públicos e os projetos importantes de interesse europeu comum. Num contexto mais amplo, também pode mobilizar investimento privado por meio de parcerias público-privadas (incluindo um aproveitamento da experiência adquirida com a parceria público-privada contratual para a cibersegurança e a sua execução pela Organização Europeia para Cibersegurança), capital de risco para apoio às PME ou alianças e estratégias industriais no domínio das capacidades tecnológicas.

Será também dada especial atenção ao instrumento de assistência técnica[69] e à melhor utilização das mais recentes ferramentas de cibersegurança pelas PME — principalmente às que não são abrangidas pela Diretiva SRI revista —, nomeadamente através de atividades específicas no quadro dos polos de inovação digital no programa Europa Digital. O objetivo é mobilizar um montante de investimento semelhante por parte dos Estados-Membros, ao qual a indústria deverá corresponder no âmbito de uma parceria coadministrada com os Estados-Membros no **Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e na Rede de Centros Nacionais de Coordenação (CCCN) propostos**. Com os contributos das comunidades industriais e académicas, os CCCN devem ter um papel determinante no desenvolvimento da soberania tecnológica da UE relativamente à cibersegurança, no reforço da capacidade para proteger infraestruturas sensíveis, como as redes 5G, e na redução da dependência de outras regiões do globo para as tecnologias mais cruciais.

A Comissão pretende apoiar, possivelmente com os CCCN, o desenvolvimento de um programa de mestrado dedicado à cibersegurança e contribuir para um roteiro europeu comum de investigação e inovação sobre cibersegurança para o período pós-2020. Os investimentos através dos CCCN podem igualmente potenciar a cooperação em investigação e desenvolvimento a cargo das redes de centros de excelência em cibersegurança, que congregam as melhores equipas de investigação da Europa e a indústria, para delinear e pôr em prática agendas comuns de investigação, em consonância com o roteiro da Organização Europeia para Cibersegurança[70]. A Comissão continuará a inspirar-se no trabalho de investigação realizado pela ENISA e pela Europol, bem como a apoiar, no âmbito do Horizonte Europa, inovadores individuais da Internet que desenvolvam tecnologias de reforço da privacidade e de comunicação segura com base em *software* e equipamento informático de código aberto, à semelhança dos projetos no quadro da iniciativa Internet da próxima geração.

1.8 Uma mão de obra da UE ciberqualificada

Os esforços da UE no sentido de melhorar as qualificações da mão de obra, de desenvolver, atrair e manter os melhores profissionais no domínio da cibersegurança e investir em investigação e inovação de craveira mundial representam uma componente importante da proteção contra as ciberameaças em geral. Este domínio oferece um grande potencial. Por isso, deve ser prestada atenção particular à necessidade de desenvolver, atrair e manter talentos mais diversificados. O Plano de Ação para a Educação Digital revisto incluirá a sensibilização das pessoas para a cibersegurança, principalmente das crianças e jovens, assim

[69] https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=COM:2020:0409:FIN.
[70] https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies.

como das organizações, mormente as PME[71]. Incentivará igualmente a participação das mulheres no ensino da ciência, tecnologia, engenharia e matemática («CTEM») e na melhoria e requalificação das competências digitais do emprego em TIC. Além disso, a Comissão procederá, em conjunto com o Instituto da Propriedade Intelectual da UE na Europol, a ENISA, os Estados-Membros e o setor privado, ao desenvolvimento de ferramentas e orientações de sensibilização para aumentar a resiliência das empresas da UE perante os **furtos de propriedade intelectual possibilitados pelo ciberespaço**[72].

A educação — incluindo o ensino e formação profissionais (EFP) —, a sensibilização e os exercícios devem igualmente contribuir para um reforço das qualificações em cibersegurança e ciberdefesa ao nível da UE. Para o efeito, os intervenientes relevantes na UE, tais como a ENISA, a Agência Europeia de Defesa (AED) e a Academia Europeia de Segurança e Defesa (AESD)[73], devem procurar criar sinergias entre as respetivas atividades.

Iniciativas estratégicas

A UE deve assegurar o seguinte:

- Adoção de uma Diretiva SRI revista;
- Medidas regulamentares tendentes a uma Internet de coisas seguras;
- Através do investimento dos CCCN em cibersegurança (nomeadamente o programa Europa Digital, o Horizonte Europa e o mecanismo de recuperação), a mobilização de até 4,5 mil milhões de EUR em investimentos públicos e privados no período de 2021-2027;
- Uma rede da UE de centros de operações de segurança possibilitados pela IA e uma infraestrutura de comunicação ultrassegura que potencie as tecnologias quânticas;
- Adoção generalizada de tecnologias de cibersegurança através de um apoio específico às PME, no âmbito dos polos de inovação digital;
- Desenvolvimento de um serviço de resolução de DNS da UE, como alternativa segura e aberta para o acesso dos cidadãos, empresas e administrações públicas da UE à Internet; e
- Conclusão da aplicação do conjunto de instrumentos 5G até ao segundo trimestre de 2021 (ver apêndice).

2 CRIAÇÃO DE CAPACIDADE OPERACIONAL PARA PREVENIR, DISSUADIR E RESPONDER

Quer sejam involuntários ou resultado de uma ação deliberada de criminosos, de intervenientes estatais ou de outros intervenientes não estatais, os ciberincidentes podem provocar enormes danos. A sua escala e complexidade, geralmente relacionadas com a exploração de serviços, equipamento informático e *software* de terceiros para inviabilizar um

[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en.
[72] https://ec.europa.eu/commission/presscorner/detail/pt/IP_20_2187.
[73] Através da plataforma de educação, formação, avaliação e exercício em matéria de cibersegurança e ciberdefesa (ETEE).

alvo bem definido, tornam o cenário de ameaças coletivo da UE difícil de combater sem um quadro sistemático e completo de partilha de informações e cooperação, no âmbito de uma resposta comum. A UE visa, **através da aplicação plena dos instrumentos regulamentares, da mobilização e da cooperação**, apoiar os Estados-Membros na defesa dos seus cidadãos, bem como dos seus interesses económicos e de segurança nacional, no pleno respeito dos direitos e liberdades fundamentais e do Estado de direito. Diversas comunidades, constituídas por redes, pelas instituições, organismos e agências da UE e ainda pelas autoridades dos Estados-Membros, são responsáveis por prevenir, desincentivar, dissuadir e responder às ciberameaças, fazendo uso dos respetivos instrumentos e iniciativas[74]. Estas comunidades incluem: i) as autoridades de SRI, como as CSIRT, e a resposta a catástrofes; ii) as autoridades policiais e judiciais; iii) a ciberdiplomacia; e iv) a ciberdefesa.

2.1 Uma Ciberunidade Conjunta

Uma Ciberunidade Conjunta pode funcionar como plataforma virtual e física de cooperação para as diferentes comunidades de cibersegurança na UE, com ênfase na coordenação operacional e técnica contra os principais ciberincidentes e ciberameaças transfronteiras.

A Ciberunidade Conjunta pode constituir um passo importante para a conclusão do **quadro europeu de gestão de crises de cibersegurança**. Tal como referido nas orientações políticas da presidente da Comissão[75], a Ciberunidade deve permitir aos Estados-Membros e às instituições, organismos e agências da UE aproveitar plenamente as estruturas, recursos e capacidades existentes e promover uma mentalidade de «**necessidade de partilhar**». Assim, pode constituir um meio para consolidar os progressos realizados até à data na recomendação de 2017 sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala («plano de ação»)[76]. Pode igualmente fornecer uma oportunidade para aprofundar a cooperação relativamente à arquitetura do plano de ação e para aproveitar os progressos alcançados, especialmente, no âmbito do grupo de cooperação SRI e da rede CyCLONe.

Esta abordagem poderia suprir **duas lacunas principais** que têm aumentado atualmente as vulnerabilidades e criado ineficiências na resposta dada às ameaças e incidentes transfronteiras que afetam a União. Em primeiro lugar, as **comunidades** de cibersegurança civis, diplomáticas, policiais e de defesa ainda não têm um espaço comum para pôr em prática uma cooperação estruturada e facilitar a cooperação operacional e técnica. Em segundo lugar, as partes interessadas na cibersegurança ainda não foram capazes de explorar todo o **potencial** da cooperação operacional e da assistência mútua no âmbito das redes e comunidades existentes. Tal é ilustrado pela ausência de uma plataforma que permita a

[74]Incluindo o apoio da Agência da União Europeia para a Cibersegurança (ENISA) à cooperação operacional e à gestão de crises; a rede de CSIRT; a Rede de Organizações de Coordenação de Cibercrises (CyCLONe, que se tornará «EU-CyCLONe», tal como proposto ao abrigo da Diretiva SRI revista); o grupo de cooperação SRI; a iniciativa «rescEU»; O Centro Europeu da Cibercriminalidade, o Grupo de Ação Conjunto contra a Cibercriminalidade da Europol e o protocolo relativo à resposta de emergência dos serviços repressivos; o Centro de Situação e de Informações da UE (INTCEN) e o conjunto de instrumentos de ciberdiplomacia; a Capacidade Única de Análise de Informações (SIAC); os ciberprojetos no quadro da cooperação estruturada permanente (CEP), nomeadamente as «equipas de resposta rápida a ciberataques e assistência mútua no domínio da cibersegurança» (CRRT).

[75]«Uma União mais ambiciosa — O meu programa para a Europa», Orientações Políticas para a próxima Comissão Europeia 2019-2024 pela candidata à função de Presidente da Comissão Europeia, Ursula von der Leyen.

[76]Projeto de Recomendação C (2017) 6100 final, de 13.9.2017, sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala.

cooperação operacional com o setor privado. A Ciberunidade deverá melhorar e acelerar a coordenação, bem como permitir à UE assumir o desafio e responder aos incidentes e crises de larga escala no ciberespaço.

A Ciberunidade Conjunta não seria um organismo suplementar autónomo, nem afetaria as competências e os poderes das autoridades nacionais de cibersegurança ou dos participantes da UE. Pelo contrário, esta Ciberunidade pode servir de mecanismo de salvaguarda sempre que os participantes possam contar com o apoio e as competências especializadas uns dos outros, especialmente no caso de várias cibercomunidades terem de trabalhar em estreita colaboração. Ao mesmo tempo, os acontecimentos recentes demonstram a necessidade de a UE reforçar o seu nível de ambição e disponibilidade para enfrentar o panorama e as realidades das ciberameaças. No âmbito do seu contributo para a Ciberunidade Conjunta, os intervenientes da UE (Comissão e agências e organismos da UE) estarão, por conseguinte, prontos a aumentar significativamente os seus recursos e capacidades, a fim de aumentar a sua preparação e resiliência.

A Ciberunidade Conjunta poderá cumprir três propósitos fundamentais. Primeiro, garantir a **preparação** em todas as comunidades de cibersegurança; segundo, através da partilha de informações, fomentar um **conhecimento** partilhado e contínuo da situação; terceiro, reforçar uma **resposta** e recuperação coordenadas. Para alcançar estes objetivos, a Ciberunidade deve alicerçar-se em **pilares e metas** bem definidos, nomeadamente garantir uma **partilha de informações segura e rápida**, melhorar a **cooperação** entre os participantes, incluindo a interação entre os Estados-Membros e as entidades pertinentes da UE, estabelecer **parcerias estruturadas com uma base industrial de confiança** e viabilizar uma abordagem coordenada da **cooperação com os parceiros externos**. Para o efeito, tendo por base um levantamento das capacidades disponíveis aos níveis nacional e da UE, a Ciberunidade pode facilitar a elaboração de um quadro de cooperação.

No sentido de tornar a Ciberunidade Conjunta o motor central da cooperação operacional da UE em matéria de cibersegurança, a Comissão irá colaborar com os Estados-Membros e as instituições, organismos e agências da UE pertinentes, incluindo a ENISA, a CERT-UE e a Europol, com vista a promover uma **abordagem progressiva e inclusiva**, no pleno respeito das competências e dos mandatos de todos os interessados. Em consonância com esta abordagem, a Ciberunidade pode contribuir para intensificar a cooperação entre os integrantes de uma cibercomunidade específica, caso esses integrantes o considerem necessário.

Propõem-se quatro etapas principais para a concretização da Ciberunidade Conjunta:

- *Definir*, através do levantamento das capacidades disponíveis aos níveis nacional e da UE;
- *Preparar*, através do estabelecimento de um quadro de cooperação estruturada e de assistência;
- *Implantar*, através da execução de um quadro alicerçado nos recursos fornecidos pelos participantes, por forma a operacionalizar a Ciberunidade Conjunta;
- *Expandir*, através do reforço de uma capacidade de resposta coordenada, com contributos da indústria e dos parceiros.

Tendo por base os resultados da consulta dos Estados-Membros e das instituições, organismos e agências da UE[77], a Comissão, com a participação do Alto Representante, apresentará, até fevereiro de 2021, o processo, as metas intermédias e o calendário para a **definição, preparação, implantação e expansão da Ciberunidade Conjunta**.

2.2 Combater a cibercriminalidade

A nossa dependência de ferramentas em linha conduziu a um aumento exponencial da superfície de ataque para os cibercriminosos e a uma situação em que a investigação de quase todos os tipos de crime tem uma componente digital. Além disso, setores nucleares da nossa sociedade enfrentam uma ameaça colocada pelos agentes do ciberespaço e por quem utiliza ciberferramentas para planear e executar ações ilícitas. Existem, por conseguinte, relações estreitas com a política global de segurança da UE, tal como refletem os elementos de cibersegurança incluídos na Estratégia da UE para a União da Segurança de 2020 e na Agenda da UE de Luta contra o Terrorismo[78].

Combater eficazmente a cibercriminalidade é um fator essencial para garantir a cibersegurança: a dissuasão não pode ser alcançada unicamente através da resiliência, mas exige igualmente a identificação e a penalização dos infratores. É essencial, portanto, promover a cooperação e o intercâmbio dos intervenientes no domínio da cibersegurança com as autoridades policiais. Por conseguinte, a nível da UE, a Europol e a ENISA já estabeleceram uma forte cooperação, que se traduziu na organização de conferências e seminários conjuntos e na apresentação de relatórios conjuntos à Comissão, aos Estados-Membros e a outras partes interessadas sobre ameaças à cibersegurança e desafios tecnológicos. A Comissão continuará a apoiar esta abordagem integrada, a fim de assegurar uma resposta coerente e eficaz, baseada numa visão abrangente.

Sendo um importante elemento dessa resposta, as autoridades nacionais e da UE devem alargar e melhorar a capacidade das autoridades policiais para investigar a cibercriminalidade, respeitando plenamente os direitos fundamentais e procurando o equilíbrio necessário entre vários direitos e interesses. A UE deve ser capaz de combater a cibercriminalidade através de uma legislação aplicada na íntegra e ajustada à sua finalidade, com uma tónica especial no combate ao abuso sexual de crianças em linha e nas investigações digitais, incluindo da criminalidade na «Internet obscura». Os serviços policiais devem estar munidos de todas as ferramentas adequadas para realizar investigações digitais. Por conseguinte, a Comissão apresentará um plano de ação para melhorar a capacidade digital dos serviços policiais, dotando-os das qualificações e dos instrumentos necessários. Concretamente, a Europol reforçará o seu papel enquanto centro especializado para apoiar as autoridades policiais nacionais na luta contra a criminalidade dependente e possibilitada pelo ciberespaço, contribuindo para a elaboração de normas forenses comuns (por intermédio do laboratório e polo de inovação da Europol). Será necessário que todas estas atividades sejam devidamente adotadas pelos Estados-Membros, os quais são convidados a fazer pleno uso dos programas nacionais ao abrigo do Fundo para a Segurança Interna e a propor projetos em resposta aos convites à apresentação de propostas no âmbito do instrumento temático.

[77]Consulta dos Estados-Membros (incluindo durante o exercício «Blue OLEx 2020», que reuniu os chefes das autoridades nacionais de cibersegurança) e das instituições, organismos e agências da UE realizada entre julho e novembro de 2020.

[78]Comunicação da Comissão intitulada «*A Counter-Terrorism Agenda for the EU: Anticipated, Prevent, Protect, Respond*», de 9.12.2020 [COM(2020) 795 final].

A Comissão utilizará todos os meios adequados, incluindo processos por infração, para garantir a transposição e aplicação na íntegra da Diretiva de 2013 relativa a ataques contra os sistemas de informação[79], nomeadamente o fornecimento de estatísticas pelos Estados-Membros. Procurará impedir melhor o abuso de nomes de domínio, nomeadamente, se for caso disso, para fins de distribuição de conteúdos ilegais, e fomentar a disponibilidade de dados de registo exatos, continuando a colaborar com a Sociedade Internet para os Nomes e Números Atribuídos (ICANN) e com outras partes interessadas no sistema de governação da Internet, designadamente por intermédio do Grupo de Trabalho sobre Segurança Pública do Comité Consultivo Governamental da ICANN. Neste sentido, a proposta de Diretiva SRI revista prevê a manutenção de bases de dados exatas e completas dos nomes de domínio e dados de registo, ou «dados WHOIS», bem como a concessão de um acesso legal a esses dados, tendo em conta o seu caráter fundamental para garantir a segurança, a estabilidade e a resiliência do DNS.

A Comissão continuará igualmente a disponibilizar canais adequados e a clarificar as regras aplicáveis à obtenção de acesso transnacional a provas eletrónicas para efeitos de investigação penal (necessárias em 85 % das investigações, enquanto 65 % do total dos pedidos se destinam a prestadores estabelecidos noutra jurisdição), facilitando a adoção e a subsequente aplicação do «pacote relativo às provas eletrónicas» e das medidas práticas[80]. A rápida adoção pelo Parlamento Europeu e pelo Conselho das propostas relativas às provas eletrónicas é fundamental para proporcionar aos profissionais um instrumento eficiente. Tendo em conta que as provas eletrónicas devem ser legíveis, a Comissão intensificará os seus esforços para apoiar a capacidade dos serviços repressivos no domínio das investigações digitais, nomeadamente no que se refere à gestão da cifragem sempre que necessário nas investigações penais, isto sem deixar de cumprir plenamente a sua função relativa à proteção dos direitos fundamentais e da cibersegurança.

2.3 Conjunto de instrumentos de ciberdiplomacia da UE

A UE tem vindo a utilizar o seu **conjunto de instrumentos de ciberdiplomacia**[81] para prevenir, desincentivar, dissuadir e responder a ciberatividades maliciosas. Após instituir, em maio de 2019[82], o quadro jurídico das medidas restritivas específicas contra os ciberataques, em julho de 2020[83], a UE incluiu no regime de sanções seis pessoas e três entidades que

[79]Diretiva 2013/40/UE relativa a ataques contra os sistemas de informação.
[80]COM(2018) 225 e 226; C(2020) 2779 final. Concretamente, o projeto SIRIUS beneficiou recentemente de financiamento adicional no âmbito do Instrumento de Parceria para melhorar os canais de obtenção de acesso transnacional lícito a provas eletrónicas para efeitos de investigação penal (necessárias em 85 % das investigações relativas a crimes graves, enquanto 65 % do total dos pedidos se destinam a prestadores estabelecidos noutra jurisdição), bem como estabelecer regras compatíveis a nível internacional.
[81] https://www.consilium.europa.eu/pt/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/.
[82]Decisão (PESC) 2019/797 do Conselho, de 17 de maio de 2019, relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados- Membros (JO L 129I de 17.5.2019, p. 13); e o Regulamento (UE) 2019/796 do Conselho
de 17 de maio de 2019, relativo a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros (JO L 129I de 17.5.2019, p. 1).
[83] Decisão (PESC) 2020/1127 do Conselho, de 30 de julho de 2020, que altera a Decisão (PESC) 2019/797 relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros (ST/9564/2020/INIT) (JO L 246 de 30.7.2020, p. 12); e Regulamento de Execução (UE) 2020/1125 do Conselho, de 30 de julho de 2020, que dá execução ao Regulamento (UE) 2019/796 relativo a

foram responsáveis ou participaram em ciberataques que afetaram a UE e os seus Estados-Membros. A essa lista foram adicionadas duas pessoas e um organismo em outubro de 2020[84]. As ciberatividades maliciosas, incluindo as que têm uma evolução lenta, devem ser combatidas através de um quadro eficaz e abrangente para uma resposta diplomática conjunta da UE, que explore plenamente as medidas disponíveis ao nível da UE.

Para uma resposta diplomática conjunta da UE célere e eficaz, é necessário promover um conhecimento partilhado e sólido da situação e assegurar a capacidade de preparar rapidamente uma posição conjunta da UE. O Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança irá incentivar e facilitar a criação de um **grupo de trabalho sobre ciberinformações dos Estados-Membros da UE**, tutelado pelo Centro de Situação e de Informações da UE (INTCEN), a fim de desenvolver a cooperação em matéria de informações estratégicas sobre ciberameaças e ciberatividades. Este trabalho permitirá reforçar o apoio ao conhecimento situacional da UE e à tomada de decisão relativamente a uma resposta diplomática conjunta. Caberá ao grupo de trabalho associar-se às estruturas existentes[85], incluindo, se necessário, as que intervêm sobre a ameaça mais global da interferência híbrida e estrangeira, com o intuito de recolher e avaliar o conhecimento situacional.

A fim de reforçar a capacidade da UE para prevenir, desincentivar, dissuadir e responder a comportamentos maliciosos no ciberespaço, o Alto Representante, com o envolvimento da Comissão no âmbito das suas competências, apresentará uma proposta no sentido de a UE definir melhor a sua **posição de dissuasão no ciberespaço**. Aproveitando o trabalho desenvolvido até à data no âmbito do conjunto de instrumentos de ciberdiplomacia, essa posição deve contribuir para um comportamento e uma cooperação responsáveis dos Estados no ciberespaço, devendo ser particularmente orientada para o combate aos ciberataques cujos efeitos são mais significativos, nomeadamente os que afetam as nossas infraestruturas críticas e instituições e processos democráticos[86], bem como aos ataques contra as cadeias de abastecimento e ao roubo de propriedade intelectual possibilitado pelo ciberespaço. A posição deve descrever a forma como a UE e os Estados-Membros podem alavancar os seus instrumentos políticos, económicos, diplomáticos, jurídicos e de comunicação estratégica contra as ciberatividades maliciosas, bem como analisar o modo como a UE e os Estados-Membros podem aumentar a sua capacidade de atribuição da autoria de ciberatividades maliciosas. Além disso, o Alto Representante pretende, juntamente com o Conselho e a Comissão, equacionar **medidas suplementares no âmbito do conjunto de instrumentos de ciberdiplomacia**, incluindo a possibilidade de estudar novas opções de medidas restritivas, bem como explorar a **votação por maioria qualificada (VMQ) para as listas ao abrigo do regime horizontal de sanções contra ciberataques**. De resto, a UE deve envidar esforços

---

medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros (ST/9568/2020/INIT) (JO L 246 de 30.7.2020, p. 4).

[84] Decisão (PESC) 2020/1537 do Conselho, de 22 de outubro de 2020, que altera a Decisão (PESC) 2019/797 relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros (JO L 351I de 22.10.2020, p. 5); e Regulamento de Execução (UE) 2020/1536 do Conselho, de 22 de outubro de 2020, que dá execução ao Regulamento (UE) 2019/796 relativo a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros (JO L 351I de 22.10.2020, p. 1).

[85] A saber, a Capacidade Única de Análise de Informações da UE (SIAC) e, se necessário, os projetos pertinentes estabelecidos no âmbito da CEP, assim como o sistema de alerta rápido de 2018 criado para apoiar a abordagem global da UE em matéria de combate à desinformação.

[86] Procurando, em particular, estabelecer sinergias com as iniciativas no âmbito do Plano de Ação para a Democracia Europeia.

suplementares no sentido de **reforçar a cooperação com os parceiros internacionais**, incluindo a NATO, para consolidar um conhecimento partilhado do cenário de ameaças, desenvolver mecanismos de cooperação e identificar respostas diplomáticas colaborativas.

O Alto Representante, com o envolvimento da Comissão, vai também propor uma atualização das **orientações de execução para o conjunto de instrumentos de ciberdiplomacia**[87], nomeadamente com vista a aumentar a eficiência do processo decisório, e continua a organizar regularmente exercícios e avaliações do conjunto de instrumentos de ciberdiplomacia. Ademais, a UE deve prosseguir a **integração do conjunto de instrumentos de ciberdiplomacia nos mecanismos da UE de gestão de crises**, bem como procurar sinergias com os esforços de luta contra as ameaças híbridas, a desinformação e as interferências estrangeiras, no âmbito do quadro comum em matéria de luta contra as ameaças híbridas[88] e do Plano de Ação para a Democracia Europeia. Neste contexto, a UE deve considerar uma interação entre o conjunto de instrumentos de ciberdiplomacia e a possível aplicação do artigo 42.º, n.º 7, do TUE e do artigo 222.º do TFUE[89].

2.4 Promover as capacidades de ciberdefesa

É necessário que a UE e os Estados-Membros aumentem a sua capacidade para prevenir e responder a ciberameaças, em conformidade com o nível de ambição da UE decorrente da sua estratégia global de 2016[90]. Para o efeito, o Alto Representante, em cooperação com a Comissão, apresentará uma **revisão do Quadro Estratégico para a Ciberdefesa (QEC)**, a fim de reforçar a coordenação e a cooperação entre os intervenientes da UE[91], bem como entre os Estados-Membros, incluindo no que respeita às missões e operações da Política Comum de Segurança e Defesa (PCSD). O QEC deve contribuir com informações para as futuras orientações estratégicas[92], zelando por uma maior integração da cibersegurança e da ciberdefesa no âmbito mais vasto da agenda de segurança e defesa.

Em 2018, a UE classificou o ciberespaço como um domínio da atividade militar[93]. A futura **«Visão e Estratégia Militar para o Ciberespaço como Domínio da Atividade Militar»**, a elaborar pelo Comité Militar da UE, deverá definir melhor de que modo o ciberespaço, enquanto domínio da atividade militar, possibilita missões e operações militares no âmbito da PCSD da UE. A **rede de CERT militares**[94], em processo de criação pela Agência Europeia de Defesa (AED), contribuirá igualmente para um aumento significativo da cooperação entre os Estados-Membros. Além disso, com vista a garantir a cibersegurança de infraestruturas espaciais críticas sob a responsabilidade do Programa Espacial, a Agência Europeia para o Programa Espacial e, mais particularmente, o Centro Galileo de Acompanhamento de Segurança serão reforçados e o respetivo mandato será alargado a outros ativos críticos do Programa Espacial.

---

[87] 13007/17.
[88] https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.
[89] Respetivamente, a cláusula de defesa mútua e a cláusula de solidariedade.
[90] Conclusões (14149/16) do Conselho sobre a aplicação da estratégia global da UE no domínio da segurança e da defesa.
[91] Tais como o SEAE, o Estado-Maior da UE (EMUE), a Academia Europeia de Segurança e Defesa (AESD), a Comissão e as agências da UE, nomeadamente a Agência Europeia de Defesa (AED).
[92] Conclusões do Conselho sobre segurança e defesa, de 17 de junho de 2020 (8910/20).
[93] https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/pt/pdf.
[94] A criação de uma rede da UE de CERT militares dá resposta a um objetivo identificado no Quadro Estratégico para a Ciberdefesa de 2018 e visa promover uma interação ativa e a partilha de informações entre as CERT militares dos Estados-Membros da UE.

A UE e os Estados-Membros devem dar um novo impulso ao **desenvolvimento de capacidades avançadas de ciberdefesa**, mediante diferentes políticas e instrumentos da UE, nomeadamente o QEC e, se relevante, aproveitar o trabalho da AED. Para tal, será necessário dar especial primazia ao desenvolvimento e à utilização de tecnologias fulcrais, como a IA, a cifragem e a computação quântica. Em consonância com as prioridades da UE em matéria de desenvolvimento de capacidades[95], de 2018, e tendo por base as conclusões do primeiro relatório completo de Análise Anual Coordenada em matéria de Defesa (CARD)[96], a UE deve reforçar a promoção da cooperação entre os Estados-Membros quanto à **investigação, inovação e desenvolvimento de capacidades no domínio da ciberdefesa**, incentivando os Estados-Membros a explorar todo o potencial da **cooperação estruturada permanente (CEP)**[97] e do **FED**[98]**.**

O futuro **plano de ação da Comissão sobre sinergias entre as indústrias civis, da defesa e do espaço**, que deverá ser apresentado no primeiro trimestre de 2021, incluirá ações para apoiar sinergias entre programas, tecnologias, inovação e empresas em fase de arranque, de acordo com a governação dos respetivos programas[99].

Adicionalmente, devem ser desenvolvidas as sinergias e interfaces relevantes entre as iniciativas de ciberdefesa apresentadas noutros quadros, incluindo os projetos colaborativos relacionados com o ciberespaço[100] dos Estados-Membros no âmbito da CEP, bem como as estruturas de cibersegurança da UE, a fim de apoiar a partilha de informações e a ajuda mútua.

Iniciativas estratégicas

A UE deve:

- Concluir o quadro europeu de gestão de crises de cibersegurança e definir o processo, as metas intermédias e o calendário para a criação da Ciberunidade Conjunta;
- Prosseguir a execução da agenda para a luta contra a cibercriminalidade, no âmbito da Estratégia para a União da Segurança;
- Incentivar e facilitar a criação de um grupo de trabalho sobre ciberinformações dos Estados-Membros da UE, tutelado pelo INTCEN UE;
- Promover a sua posição de dissuasão no ciberespaço para prevenir, desincentivar,

[95] Em junho de 2018, os Estados-Membros decidiram, no Comité Diretor da AED, definir orientações ao nível da UE para a cooperação em matéria de defesa.
[96] Aprovado em novembro de 2020 pelos ministros da Defesa, reunidos no Comité Diretor da AED. https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card)
[97] Estão atualmente em curso vários projetos CEP relacionados com o ciberespaço, designadamente a plataforma de partilha de informações relativas às ciberameaças e à resposta a incidentes informáticos, as equipas de resposta rápida a ciberataques e assistência mútua no domínio da cibersegurança, a Academia e Plataforma de Inovação da UE no domínio da cibernética e o centro de coordenação no domínio da cibernética e da informação (CIDCC).
[98] No âmbito do FED, a Comissão já identificou possíveis oportunidades de ações colaborativas na investigação e desenvolvimento em matéria de ciberdefesa, destinadas a reforçar a cooperação, a capacidade de inovação e a competitividade da indústria de defesa.
[99] Tais como o Horizonte Europa, Europa Digital e FED.
[100] https://pesco.europa.eu/.

dissuadir e responder a ciberatividades maliciosas;

- Rever o Quadro Estratégico para a Ciberdefesa;
- Intermediar a conceção de uma «Visão e Estratégia Militar para o Ciberespaço como Domínio da Atividade Militar» para as missões e operações militares da PCSD;
- Apoiar as sinergias entre as indústrias civis, da defesa e do espaço; e
- Reforçar cibersegurança de infraestruturas espaciais críticas no âmbito do Programa Espacial.

3 PROMOVER UM CIBERESPAÇO MUNDIAL E ABERTO

A UE deve continuar a cooperar com os parceiros internacionais na promoção de um modelo e de uma visão políticos do ciberespaço alicerçados no Estado de direito, nos direitos humanos, nas liberdades fundamentais e nos valores democráticos, que propiciem um desenvolvimento social, económico e político à escala mundial e contribuam para uma União da Segurança. A cooperação internacional é determinante para manter um ciberespaço global, aberto, estável e seguro. Para o efeito, a UE deve continuar a trabalhar com países terceiros, organizações internacionais e a comunidade multilateral, no intuito de elaborar e aplicar uma política internacional do ciberespaço coerente e holística, que atente devidamente na crescente interligação entre os aspetos económicos das novas tecnologias, da segurança interna e das políticas externa, de segurança e defesa. Enquanto bloco económico e comercial forte, assente nos valores democráticos basilares, no respeito pelo Estado de direito e nos direitos fundamentais, a UE tem também condições únicas para assumir uma posição de liderança na definição e promoção de normas e padrões internacionais.

3.1 Liderança da UE em matéria de normas, regras e quadros no ciberespaço

Intensificar a normalização internacional

A fim de promover e defender a sua visão do ciberespaço na cena internacional, a UE terá de **intensificar o seu empenho e a sua liderança nos processos de normalização internacional, bem como reforçar a sua representação nos organismos internacionais e europeus de normalização e noutras organizações de elaboração de normas**[101]. Atendendo à rápida evolução das tecnologias digitais, as normas internacionais ganham uma crescente importância para complementar os tradicionais esforços de regulamentação em domínios como a IA, a nuvem, a computação quântica e a comunicação quântica. A normalização internacional é cada vez mais utilizada pelos países terceiros para promoverem a sua agenda política e ideológica, que, muitas vezes, não se coaduna com os valores da UE. Por outro lado, existe um risco cada vez maior de serem definidos enquadramentos concorrentes da normalização internacional, resultando numa fragmentação.

É essencial que a conceção das normas internacionais nas áreas das tecnologias emergentes e da arquitetura central da Internet seja consentânea com os valores da UE, por forma a

[101] Por exemplo, a Organização Internacional de Normalização (ISO), a Comissão Eletrotécnica Internacional (CEI), a União Internacional das Telecomunicações (UIT), o Comité Europeu de Normalização (CEN), o Comité Europeu de Normalização Eletrotécnica (Cenelec), o Instituto Europeu de Normalização das Telecomunicações (ETSI), o Grupo de Missão de Engenharia da Internet (IETF), o Projeto de Parceria de 3.ª Geração (3GPP) e o Instituto de Engenharia Elétrica e Eletrónica (IEEE).

assegurar que a Internet continue a ser global e aberta, que as tecnologias sejam centradas no ser humano e na privacidade e que a sua utilização seja lícita, segura e ética. No quadro da sua futura estratégia de normalização, a UE deverá definir os seus **objetivos quanto à normalização internacional** e organizar ações de divulgação proativas e coordenadas, a fim de promover esses objetivos no plano internacional. Deve ser procurada uma cooperação mais sólida e uma partilha dos esforços com parceiros imbuídos do mesmo espírito e partes interessadas europeias.

Fomentar o comportamento responsável dos Estados no ciberespaço

A UE continua a colaborar com os parceiros internacionais no desenvolvimento e na promoção de um ciberespaço global, aberto, estável e seguro, no qual **seja respeitado o direito internacional, em especial a Carta das Nações Unidas (ONU)**[102], e sejam observadas as **normas, regras e princípios não vinculativos e voluntários relativos ao comportamento responsável dos Estados**[103]. Com a deterioração das possibilidades de um debate multilateral efetivo sobre a segurança internacional no ciberespaço, existe uma clara necessidade de a UE e os Estados-Membros terem uma atitude mais proativa nas conversações na ONU e demais instâncias internacionais relevantes. A União Europeia é a organização indicada para **fomentar, coordenar e consolidar as posições dos Estados-Membros nas instâncias internacionais** e deve **desenvolver uma posição da UE sobre a aplicação do direito internacional no ciberespaço.** Juntamente com os Estados-Membros, o Alto Representante pretende igualmente apresentar uma proposta inclusiva e consensual relativa a um compromisso político com um **programa de ação para fomentar o comportamento responsável dos Estados no ciberespaço (Programa de Ação)**[104] na ONU. Tendo por base o atual acervo validado pela Assembleia Geral das Nações Unidas[105], o Programa de Ação fornece uma plataforma de cooperação e intercâmbio de boas práticas no seio das Nações Unidas e propõe ainda a criação de um mecanismo para instituir as normas relativas ao comportamento responsável dos Estados, bem como promover a criação de capacidades. Além disso, o Alto Representante pretende fortalecer e incentivar a aplicação de **medidas de reforço da confiança** entre os Estados através do intercâmbio de boas práticas aos níveis regional e multilateral e da contribuição para a cooperação transregional.

Uma maior conectividade global não deve dar azo a censura, vigilância maciça, violações da privacidade dos dados e repressão contra a sociedade civil, a comunidade académica e os cidadãos. A UE deve continuar a liderar na esfera da proteção e promoção dos **direitos humanos e das liberdades fundamentais** em linha. Para o efeito, a UE deve promover uma observação mais rigorosa do direito e das normas internacionais em matéria de direitos humanos[106], operacionalizar o seu Plano de Ação da UE para os Direitos Humanos e a Democracia 2020-2024[107] e fomentar as suas orientações em matéria de direitos humanos

[102] https://www.un.org/en/sections/un-charter/un-charter-full-text/.
[103] Tal como refletido nos relatórios sobre esta matéria dos grupos de peritos governamentais no domínio da informação e das telecomunicações, no contexto da segurança internacional (GPG da ONU), aprovados pela AGNU, nomeadamente os relatórios de 2015, 2013 e 2010.
[104] https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf.
[105] Tal como refletido nos relatórios sobre esta matéria dos grupos de peritos governamentais no domínio da informação e das telecomunicações, no contexto da segurança internacional (GPG da ONU), aprovados pela AGNU: Relatórios de 2010. 2013 e 2015.
[106] Designadamente a Carta das Nações Unidas e a Declaração Universal dos Direitos do Homem.
[107] https://www.consilium.europa.eu/pt/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/.

relativas à liberdade de expressão em linha e fora da Internet[108], **conferindo um novo ímpeto à aplicação prática dos seus instrumentos**. A UE deve realizar esforços contínuos no sentido de **proteger os ativistas pelos direitos humanos, a sociedade civil e a comunidade académica que desenvolvem trabalho sobre matérias como a cibersegurança, a privacidade dos dados, a vigilância e a censura em linha.** Neste sentido, a UE deve fornecer mais orientações práticas, promover as boas práticas e intensificar os seus esforços para prevenir a utilização abusiva das tecnologias emergentes, recorrendo, particularmente, a medidas diplomáticas, sempre que necessário, bem como ao controlo das exportações de tecnologias deste tipo. A UE deve igualmente continuar a pugnar pela proteção em linha dos membros mais vulneráveis da sociedade, apresentando legislação tendente a proteger melhor as crianças contra o abuso e a exploração sexual de menores, assim como uma estratégia sobre os direitos da criança.

Convenção de Budapeste sobre a Cibercriminalidade

A UE continua a apoiar os países terceiros que pretendem aderir à **Convenção de Budapeste sobre a Cibercriminalidade do Conselho da Europa** e trabalhar na conclusão do Segundo Protocolo Adicional à Convenção de Budapeste, o qual inclui medidas e salvaguardas destinadas a melhorar a cooperação internacional entre as autoridades policiais e judiciais, bem como entre as autoridades e os prestadores de serviços noutros países, e cujas negociações contam com a participação da Comissão em nome da UE[109]. A atual iniciativa para um novo instrumento jurídico relativo à cibercriminalidade ao nível da ONU comporta um risco de agravamento das divisões e de procrastinação das reformas tão necessárias à escala nacional e dos esforços de reforço das capacidades, podendo obstar a uma cooperação internacional eficaz contra a cibercriminalidade; a UE discorda da necessidade de qualquer novo instrumento jurídico relativo à cibercriminalidade ao nível da ONU. A UE continua empenhada em **intercâmbios multilaterais sobre a cibercriminalidade**, a fim de assegurar o respeito pelos direitos humanos e pelas liberdades fundamentais, através da inclusividade e da transparência, e tomando em consideração os conhecimentos especializados disponíveis, com o objetivo de gerar valor acrescentado para todos.

3.2 Cooperação com os parceiros e com a comunidade multilateral

A UE **fortalecerá e alargará os seus ciberdiálogos com os países terceiros** no sentido de promover os seus valores e visão para o ciberespaço, partilhar boas práticas e estimular uma cooperação mais eficaz. A UE deve igualmente estabelecer **intercâmbios estruturados com as organizações regionais**, tais como a União Africana, o Fórum Regional da ASEAN, a Organização dos Estados Americanos e a Organização para a Segurança e a Cooperação na Europa. Paralelamente, a UE deve procurar encontrar plataformas de entendimento, sempre que possível e oportuno, com outros parceiros, baseadas em questões de interesse comum. Em colaboração com as delegações da UE e, se for caso disso, com as embaixadas dos Estados-Membros em todo o mundo, a UE deve constituir uma **rede informal de ciberdiplomacia da UE** a fim de promover a visão da UE para o ciberespaço, proceder ao intercâmbio de informações e de se coordenar regularmente sobre a evolução do ciberespaço[110].

[108] https://www.consilium.europa.eu/media/28348/142549.pdf.
[109] Decisão do Conselho de junho de 2019 (9116/19).
[110] Se necessário, poderá igualmente tirar partido das atividades da rede informal de diplomacia digital da UE, que incorpora os ministérios dos negócios estrangeiros dos Estados-Membros.

Tendo por base as declarações conjuntas de 8 de julho de 2016[111] e de 10 julho de 2018[112], a UE deve continuar a desenvolver a **cooperação UE-NATO**, especialmente no atinente aos requisitos de interoperabilidade da ciberdefesa. Neste contexto, a UE deve prosseguir a associação das estruturas relevantes da PCSD às Redes de Missão Federadas da NATO, possibilitando uma interoperabilidade das redes com a NATO e com os parceiros, quando necessário. Além disso, importa explorar melhor a cooperação entre a UE e a NATO em matéria de ensino, formação e realização de exercícios, nomeadamente procurando criar sinergias entre a Academia Europeia de Segurança e Defesa e o Centro de Excelência Cooperativo da NATO para a Ciberdefesa.

Em consonância com os seus valores, a UE preconiza e promove o **modelo multilateral de governação da Internet**. Nenhum governo, entidade ou organização internacional deve tentar controlar individualmente a Internet. A UE deve continuar a participar em instâncias[113] que visam reforçar a cooperação e assegurar a proteção dos direitos e liberdades fundamentais, nomeadamente o direito à dignidade, à vida privada e à liberdade de expressão e de informação. Com vista a desenvolver a cooperação multilateral sobre questões de cibersegurança, a Comissão e o Alto Representante, de acordo com as respetivas competências, pretendem fortalecer **intercâmbios regulares e estruturados com as partes interessadas**, incluindo o setor privado, o meio académico e a sociedade civil, salientando que a natureza interligada do ciberespaço exige que todas as partes interessadas mantenham intercâmbios e assumam as suas responsabilidades, a fim de preservar um ciberespaço aberto, estável e seguro a nível mundial. Estes esforços representarão um contributo valioso para eventuais ações fundamentais à escala da UE.

3.3 Reforçar as capacidades mundiais para aumentar a ciber-resiliência mundial

Para garantir que todos os países consigam aproveitar as vantagens sociais, económicas e políticas da Internet e da utilização das tecnologias, a UE mantém o apoio aos seus parceiros, a fim de reforçarem a sua ciber-resiliência e as suas capacidades para investigar e julgar cibercrimes, bem como enfrentar as ciberameaças. Com vista a assegurar um quadro geral coerente, a UE deve elaborar uma **agenda da UE para o reforço das cibercapacidades externas** que oriente estes esforços de forma consonante com as suas orientações para o reforço das cibercapacidades externas[114] e a Agenda 2030 para o Desenvolvimento Sustentável[115]. A Agenda deve tirar proveito das competências especializadas dos Estados-Membros e das instituições, organismos e agências da UE e iniciativas pertinentes, incluindo a rede da UE de reforço das cibercapacidades[116], de acordo com os respetivos mandatos. Deve ser criado um **comité de reforço das cibercapacidades da UE**, a fim de englobar as partes interessadas institucionais relevantes da UE e de acompanhar os progressos realizados, bem como a identificação de novas sinergias e possíveis lacunas. Esse comité poderia, além do mais, apoiar uma cooperação reforçada com os Estados-Membros e com os parceiros dos setores público e privado, além de outros organismos internacionais pertinentes, a fim de assegurar uma coordenação dos esforços e de evitar duplicações.

---

[111] https://www.consilium.europa.eu/pt/press/press-releases/2016/07/08/eu-nato-joint-declaration/.
[112] https://www.consilium.europa.eu/pt/press/press-releases/2018/07/10/eu-nato-joint-declaration/.
[113] Tais como a Corporação da Internet para Atribuição de Nomes e Números (ICANN) e o Fórum sobre a Governação da Internet.
[114] https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf.
[115] https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm.
[116] https://www.eucybernet.eu/.

O **reforço das cibercapacidades da UE** deve continuar a centrar-se nos países dos Balcãs Ocidentais e da vizinhança da UE, bem como nos países parceiros que atravessam um rápido desenvolvimento digital. A atuação da UE deve apoiar a elaboração de atos legislativos e políticas dos países parceiros conformes com as políticas e normas de ciberdiplomacia aplicáveis na UE. Neste contexto, as iniciativas da UE para o reforço das capacidades no domínio da digitalização devem incluir a cibersegurança como característica de referência. Para o efeito, a UE deve desenhar um programa de formação destinado ao pessoal da UE encarregado de pôr em prática as iniciativas da UE de reforço das capacidades digitais e cibercapacidades externas. A UE deve igualmente prestar assistência a estes países, para que possam ultrapassar o problema cada vez mais presente das ciberatividades maliciosas, que prejudicam o desenvolvimento das suas sociedades e a **integridade e segurança dos sistemas democráticos**, em conformidade com os esforços envidados no âmbito do Plano de Ação para a Democracia Europeia. A aprendizagem interpares entre os Estados-Membros, as agências relevantes da UE e os países terceiros poderia revelar-se particularmente útil nesta matéria.

Por último, no contexto do pacto sobre a vertente civil da PCSD[117], de 2018, as missões civis da PCSD podem igualmente contribuir para o âmbito mais vasto da resposta da UE aos desafios da cibersegurança, nomeadamente através do reforço do Estado de direito e das capacidades das autoridades policiais e administrações civis nos países parceiros.

Iniciativas estratégicas

A UE deve:

- Definir um conjunto de objetivos nos processos de normalização internacional e promovê-los no plano internacional;
- Desenvolver a segurança e a estabilidade internacionais no ciberespaço, nomeadamente através de uma proposta da UE e dos seus Estados-Membros relativa a um programa de ação para fomentar o comportamento responsável dos Estados no ciberespaço (Programa de Ação) na ONU;
- Formular orientações práticas sobre a aplicação dos direitos humanos e das liberdades fundamentais no ciberespaço;
- Proteger melhor as crianças contra o abuso e a exploração sexual de menores, assim como apresentar uma estratégia sobre os direitos da criança;
- Reforçar e promover a Convenção de Budapeste sobre a Cibercriminalidade, nomeadamente através do trabalho realizado em relação ao Segundo Protocolo Adicional à Convenção de Budapeste;
- Alargar o ciberdiálogo com os países terceiros e as organizações regionais e internacionais, incluindo através de uma rede informal de ciberdiplomacia da UE;
- Fortalecer os intercâmbios com a comunidade multilateral, nomeadamente através de intercâmbios regulares e estruturados com o setor privado, a comunidade académica e a sociedade civil; e

[117] https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/pt/pdf.

- Propor uma agenda da UE para o reforço das cibercapacidades externas e a criação de um comité de reforço das cibercapacidades da UE.

III. CIBERSEGURANÇA NAS INSTITUIÇÕES, ORGANISMOS E AGÊNCIAS DA UE

Em virtude do seu perfil altamente político, das suas missões e operações críticas na coordenação de questões extremamente sensíveis e do seu papel na gestão de grandes quantias de dinheiro público, **as instituições, organismos e agências da UE são frequentemente alvo de ciberataques** e, especialmente, da ciberespionagem. Contudo, o nível de ciber-resiliência e a capacidade de detetar e responder a ciberatividades maliciosas varia significativamente entre estas entidades em termos de maturidade. Por conseguinte, é necessário aumentar o nível geral de cibersegurança por meio de regras coerentes e homogéneas.

No domínio da segurança da informação, foram realizados progressos, com um reforço da coerência das **regras de proteção quer das informações classificadas da UE, quer das informações sensíveis não classificadas.** No entanto, a interoperabilidade dos sistemas de informações classificadas permanece reduzida, o que impede uma transferência de informações contínua entre as várias entidades. Deverão ser alcançados progressos suplementares para permitir uma abordagem interinstitucional do tratamento de informações classificadas e de informações sensíveis não classificadas da UE, que poderia servir também de modelo para uma interoperabilidade entre os Estados-Membros. Deveria igualmente ser definida uma base de referência, a fim de simplificar os procedimentos com os Estados-Membros. A UE deve igualmente continuar a desenvolver a sua capacidade de comunicar de forma segura com os parceiros pertinentes, com base, na medida do possível, nos acordos e procedimentos existentes.

Conforme anunciado na Estratégia para a União da Segurança, a Comissão apresentará, neste sentido, propostas relativas a **regras vinculativas comuns em matéria de segurança da informação e regras vinculativas comuns em matéria de cibersegurança para todas as instituições, organismos e agências da UE, em 2021**, com base nas atuais conversações interinstitucionais ao nível da UE sobre cibersegurança[118].

As tendências atuais e futuras de teletrabalho também exigirão investimentos adicionais em equipamentos, infraestruturas e ferramentas seguros, que permitam trabalhar à distância com ficheiros sensíveis e classificados.

Além disso, o cenário de ciberameaça cada vez mais hostil e a crescente ocorrência de ciberataques mais sofisticados, que afetam as instituições, organismos e agências da UE, justificam a necessidade de reforçar os investimentos para atingir um elevado nível de maturidade cibernética. Está em curso a conceção de um programa de cibersensibilização destinado a todas as instituições, organismos e agências da UE, que terá por finalidade consciencializar os funcionários, fomentar a «ciber-higiene» e sustentar uma cultura de cibersegurança.

Será necessário **reforçar a CERT-UE mediante um mecanismo de financiamento melhorado**, a fim de aumentar a sua capacidade para ajudar as instituições, organismos e

[118] As conversações interinstitucionais ao nível da UE sobre cibersegurança fazem parte de intercâmbios mais amplos sobre as oportunidades e os desafios da transformação digital para as instituições da UE.

agências da UE a aplicarem as novas regras em matéria de cibersegurança e a aperfeiçoarem a sua ciber-resiliência. Importa igualmente reforçar o mandato da CERT-UE, a fim de lhe conferir atribuições sólidas para cumprir os referidos objetivos.

Iniciativas estratégicas

1. Regulamento relativo à segurança da informação nas instituições, organismos e agências da UE
2. Regulamento relativo a regras comuns em matéria de cibersegurança para as instituições, organismos e agências da UE
3. Nova base jurídica para a CERT-UE, com vista a reforçar o seu mandato e financiamento

IV. CONCLUSÕES

A aplicação concertada desta estratégia contribuirá para uma década digital cibersegura na UE, para a realização da União da Segurança e para o fortalecimento da posição da UE à escala mundial.

A UE deve impulsionar o estabelecimento de padrões e normas para soluções de craveira mundial e padrões de cibersegurança aplicáveis aos serviços essenciais e às infraestruturas críticas, bem como o desenvolvimento e a aplicação das novas tecnologias. Todas as organizações e os particulares que utilizam a Internet fazem parte da solução que visa garantir uma transformação digital cibersegura.

A Comissão e o Alto Representante, de acordo com as respetivas competências, procederão ao acompanhamento dos progressos alcançados no âmbito desta estratégia e elaborarão critérios de avaliação. Entre os contributos para esse acompanhamento deverão incluir-se os relatórios da ENISA e os relatórios periódicos da Comissão sobre a União da Segurança. Os resultados ajudarão a cumprir os futuros objetivos da década digital[119]. De acordo com as respetivas competências, a Comissão e o Alto Representante continuarão a estabelecer ligações com os Estados-Membros no sentido de identificar medidas práticas para, sempre que necessário, fazer a ponte entre as quatro comunidades de cibersegurança na UE, designadamente, a resiliência das infraestruturas críticas e do mercado interno, a justiça e aplicação da lei, a ciberdiplomacia e a ciberdefesa. Além do mais, a Comissão e o Alto Representante continuarão a colaborar com a comunidade multilateral, sublinhando a necessidade de todos os utilizadores da Internet desempenharem o seu papel na preservação de um ciberespaço global, aberto, estável e seguro, onde todos possam viver uma vida digital em segurança.

[119] Conforme anunciado no Programa de Trabalho da Comissão para 2021.

Apêndice: Passos seguintes para a cibersegurança das redes 5G

Com base nos resultados da revisão da Recomendação da Comissão sobre a cibersegurança das redes 5G[120], os passos seguintes no trabalho coordenado ao nível da UE devem centrar-se nos três objetivos fundamentais e nas principais ações a curto e médio prazo descritos no quadro infra, que deverão ser prosseguidos pelas autoridades dos Estados-Membros, pela Comissão e pela ENISA.

A primeira prioridade para a próxima fase será **concluir a aplicação do conjunto de instrumentos à escala nacional e solucionar os problemas identificados no relatório intercalar de julho de 2020**. Neste contexto, algumas das medidas estratégicas do conjunto de instrumentos seriam mais bem aplicadas com um **reforço do trabalho de coordenação ou do intercâmbio de informações** no âmbito do fluxo de trabalho relativo à SRI, tal como identificado anteriormente no relatório intercalar, o que poderia conduzir à formulação de **boas práticas ou de orientações**. No que respeita a medidas técnicas, a ENISA poderia prestar um maior apoio, aproveitando o trabalho que já desenvolveu e examinando determinados temas mais a fundo, além de **elaborar uma panorâmica abrangente de todas as orientações relevantes sobre os requisitos de cibersegurança das redes 5G aplicáveis aos operadores de redes móveis**.

Em segundo lugar, os Estados-Membros destacaram a importância de seguir de perto o desenvolvimento, mediante o **acompanhamento constante das evoluções tecnológicas, da arquitetura 5G, das ameaças e dos casos de utilização e aplicações 5G, bem como os fatores externos**, a fim de conseguirem **identificar e lidar com riscos novos ou emergentes**. Por outro lado, é necessário atentar mais profundamente em vários aspetos da análise inicial dos riscos, nomeadamente para assegurar que engloba o ecossistema 5G na íntegra, incluindo todas as partes relevantes da infraestrutura de redes e da cadeia de abastecimento 5G. Embora o conjunto de instrumentos tenha sido concebido por forma a ser flexível e adaptável, se necessário, poderão ser tomadas medidas a médio prazo para ser alargado ou modificado, no sentido de assegurar que permaneça exaustivo e atualizado.

Em terceiro lugar, importa continuar a tomar **medidas ao nível da UE** para apoiar e complementar os objetivos do conjunto de instrumentos, bem como integrá-los plenamente nas correspondentes políticas da União e da Comissão, dando seguimento, em particular, às ações anunciadas pela Comissão, na sua Comunicação de 29 de janeiro de 2020 sobre o conjunto de instrumentos[121], e relativas a um leque alargado de domínios (por exemplo, financiamento pela UE de redes 5G seguras, investimentos nas tecnologias 5G e pós-5G, instrumentos de defesa comercial e concorrência para evitar distorções no mercado de abastecimento 5G, etc.).

Nos casos em que se justifique, os principais intervenientes deverão estabelecer, no início de 2021, mecanismos detalhados e metas intermédias para as principais ações descritas a seguir.

[120] Relatório sobre os impactos da Recomendação (UE) 2019/534 da Comissão, de 26 de março de 2019, sobre a cibersegurança das redes 5G.
[121] Comunicação da Comissão, de 29 de janeiro de 2020, intitulada «Implantação segura de redes 5G na UE — Aplicação do conjunto de instrumentos da UE» [COM(2020) 50].

Objetivo fundamental 1: Assegurar abordagens nacionais convergentes em matéria de atenuação dos riscos em toda a UE		
Domínios	**Principais ações a curto e médio prazo**	**Principais intervenientes**
Aplicação do conjunto de instrumentos pelos Estados-Membros	Concluir a aplicação das medidas recomendadas nas conclusões sobre o conjunto de instrumentos até ao segundo trimestre de 2021, com a realização periódica de balanços no âmbito do fluxo de trabalho relativo à SRI.	Autoridades dos Estados-Membros
Intercâmbio de informações e de boas práticas sobre as medidas estratégicas relativas aos fornecedores	Intensificar os intercâmbios de informações e considerar possíveis boas práticas, particularmente sobre: - Restrições impostas aos fornecedores de alto risco (SM03) e medidas relativas à prestação de serviços geridos (SM04); - Segurança e resiliência da cadeia de abastecimento, dando seguimento, em particular, ao inquérito levado a cabo pelo ORECE sobre SM05-SM06.	Autoridades dos Estados-Membros, Comissão
Reforço de capacidades e orientações sobre medidas técnicas	Conduzir exames técnicos aprofundados e elaborar orientações e instrumentos comuns, incluindo: - Uma matriz completa e dinâmica de controlos de segurança e de boas práticas quanto à segurança das redes 5G; Orientações de apoio à aplicação de medidas técnicas selecionadas com base no conjunto de instrumentos.	ENISA, autoridades dos Estados-Membros
Objetivo fundamental 2: Apoiar um intercâmbio de conhecimentos permanente e o reforço de capacidades		
Domínios	**Principais ações a curto e médio prazo**	**Principais intervenientes**
Aquisição contínua de conhecimentos	Organizar atividades de aquisição de conhecimentos sobre tecnologia e desafios correlatos (arquiteturas abertas, funções 5G — p. ex., virtualização, contentorização, divisão, etc.), desenvolvimentos no cenário de ameaças, incidentes na vida real, etc.	ENISA, autoridades dos Estados-Membros, outras partes interessadas
Avaliações dos riscos	Atualizar e partilhar informações sobre avaliações dos riscos à escala nacional atualizadas	Autoridades dos Estados-Membros, Comissão, ENISA
Projetos conjuntos financiados pela UE para apoiar a aplicação do conjunto de instrumentos	Conceder ajuda financeira a projetos que apoiem a aplicação do conjunto de instrumentos com recurso a fundos da UE, nomeadamente ao abrigo do programa Europa Digital (p. ex., projetos de reforço das capacidades destinados a autoridades nacionais, bancos de ensaio ou outras capacidades avançadas, etc.)	Autoridades dos Estados-Membros, Comissão
Cooperação entre as partes interessadas	Fomentar a colaboração e cooperação entre as autoridades nacionais empenhadas na área da cibersegurança das redes 5G (por exemplo, o grupo de cooperação SRI, autoridades de cibersegurança, entidades reguladoras das telecomunicações) e com as partes interessadas do setor privado	Autoridades dos Estados-Membros, Comissão, ENISA

Objetivo fundamental 3: Promover a resiliência das cadeias de abastecimento e outros objetivos estratégicos da UE no domínio da segurança		
Domínios	**Principais ações a curto e médio prazo**	**Principais intervenientes**
Normalização	Definir e executar um plano de ação concreto para reforçar a representação da UE nos organismos de elaboração de normas, no âmbito das próximas etapas do trabalho do subgrupo SRI para a normalização, a fim de concretizar objetivos de segurança específicos, incluindo a promoção de interfaces interoperáveis para impulsionar uma diversificação dos fornecedores.	Autoridades dos Estados-Membros
Resiliência das cadeias de abastecimento	- Efetuar uma análise aprofundada do ecossistema e da cadeia de abastecimento 5G, a fim de identificar e acompanhar melhor os ativos essenciais e as dependências críticas potenciais - Assegurar que o funcionamento do mercado e da cadeia de abastecimento 5G é compatível com as regras e os objetivos da UE em matéria comercial e de concorrência, tal como definido na Comunicação da Comissão de 29 de janeiro de 2020, e que é efetuada uma análise do investimento direto estrangeiro nos desenvolvimentos de investimentos suscetíveis de afetar a cadeia de valor 5G, tendo em conta os objetivos do conjunto de instrumentos - Acompanhar as tendências atuais e previstas do mercado e avaliar os riscos e as oportunidades no domínio da Rede de Acesso Rádio aberta (Open RAN), nomeadamente através de um estudo independente	Autoridades dos Estados-Membros, Comissão
Certificação	Iniciar os trâmites relativos ao(s) sistema(s) de certificação candidato(s) para componentes 5G essenciais e processos dos fornecedores, a fim de ajudar a eliminar determinados riscos relacionados com vulnerabilidades técnicas, definidos nos planos de atenuação dos riscos do conjunto de instrumentos.	Comissão, ENISA, autoridades nacionais, outras partes interessadas
Implantação de capacidades e de redes seguras da UE	- Investir na ID e nas capacidades, nomeadamente mediante a adoção da parceria para redes e serviços inteligentes - Instituir as condições de segurança adequadas para os programas de financiamento e instrumentos financeiros da UE (internos e externos), conforme anunciado na Comunicação da Comissão de 29 de janeiro de 2020	Estados-Membros, Comissão, partes interessadas da indústria 5G
Aspetos externos	Responder favoravelmente às solicitações dos países terceiros que pretendam compreender e, possivelmente, utilizar a abordagem do conjunto de instrumentos desenvolvida pela UE.	Estados-Membros, Comissão, SEAE, delegações da UE