Conselho da
União Europeia

Bruxelas, 27 de maio de 2022
(OR. en)

9563/22

JAI 761	**DROIPEN 69**
COSI 149	**COPEN 210**
ENFOPOL 298	**FREMP 110**
ENFOCUSTOM 89	**JAIEX 61**
IXIM 145	**CFSP/PESC 705**
CT 99	**COPS 238**
CRIMORG 81	**HYBRID 49**
FRONT 218	**DISINFO 47**
ASIM 47	**TELECOM 248**
VISA 87	**DIGIT 108**
CYBER 191	**COMPET 408**
DATAPROTECT 175	**RECH 307**
CATS 30	

NOTA DE ENVIO

de:	Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora
data de receção:	25 de maio de 2022
para:	Secretariado-Geral do Conselho
n.° doc. Com.:	COM(2022) 252 final
Assunto:	COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO relativa ao quarto relatório intercalar sobre a execução da Estratégia para a União da Segurança

Envia-se em anexo, à atenção das delegações, o documento COM(2022) 252 final.

Anexo: COM(2022) 252 final

COMISSÃO
EUROPEIA

Bruxelas, 25.5.2022
COM(2022) 252 final

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

relativa ao quarto relatório intercalar sobre a execução da Estratégia para a União da Segurança

I. INTRODUÇÃO

A guerra de agressão russa contra a Ucrânia domina a atual agenda de segurança da UE. A guerra não só ameaça a Ucrânia, mas procura prejudicar a estabilidade e a segurança a nível mundial. No interior da UE, comporta uma série de riscos para a segurança dos cidadãos. Existem novas incertezas quanto ao aprovisionamento de energia e de outras matérias-primas e as infraestruturas críticas podem ser alvo de ciberataques. A segurança interna da UE é comprometida por eventuais ataques ou acidentes resultantes de agentes químicos, biológicos ou radiológicos na zona de guerra. As vulnerabilidades de milhões de pessoas que fugiram da guerra podem ser rapidamente exploradas pela criminalidade organizada, através do tráfico de mulheres e crianças, que estão especialmente em risco.

Face a estas ameaças novas e potenciais, a UE manteve-se determinada e unida. Embora, até à data, o impacto da guerra se tenha limitado sobretudo ao território da Ucrânia, a UE intensificou a *vigilância e a coordenação*, com um maior acompanhamento do panorama das ameaças, e trabalhou no sentido de reforçar a resiliência para assegurar a *preparação*.

Na Declaração de Versalhes, de 10 e 11 de março de 2022[1], os líderes europeus salientaram a necessidade de preparação para os desafios que rapidamente vão surgindo, nomeadamente «protegendo-nos contra uma guerra híbrida em constante expansão, reforçando a nossa ciber-resiliência, protegendo as nossas infraestruturas – em especial as nossas infraestruturas críticas – e combatendo a desinformação».

O quadro da União da Segurança é fundamental para garantir a segurança em toda a UE. As quatro prioridades estratégicas definidas na Estratégia para a União da Segurança[2] continuam a ser diretamente pertinentes para esta função no atual contexto geopolítico: i) um ambiente de segurança a longo prazo, ii) fazer face à evolução das ameaças, iii) proteger os europeus do terrorismo e da criminalidade organizada, e iv) um sólido ecossistema europeu de segurança. A guerra sublinhou a necessidade de a UE e os seus Estados-Membros utilizarem plenamente os instrumentos legislativos e políticos já disponíveis no âmbito da Estratégia para a União da Segurança, que sustentam o apoio coordenado da UE aos Estados-Membros em questões como a criminalidade organizada e o terrorismo, a cibersegurança e as ameaças híbridas.

As agências europeias no domínio da justiça e dos assuntos internos intensificaram igualmente os seus esforços em resposta à guerra na Ucrânia, desempenhando um papel fundamental na avaliação das ameaças e no apoio às respostas operacionais[3]. O reforço contínuo da prática operacional e da governação do espaço Schengen é outro fator importante.

Este quarto relatório intercalar sobre a União da Segurança centra-se nos desenvolvimentos dos últimos meses desde o início da guerra de agressão russa contra a Ucrânia. Apresenta uma panorâmica das medidas tomadas em todas as vertentes da União da Segurança e tem em conta as necessidades de preparação suscitadas por eventuais ameaças à segurança decorrentes da guerra na Ucrânia. Os progressos realizados em relação a outros dossiês da União da Segurança constam do anexo.

---

1 https://www.consilium.europa.eu/media/54786/20220311-versailles-declaration-pt.pdf.

2 COM(2020) 605.

3 *Joint Statement from EU Justice and Home Affairs Agencies on Ukraine* (não traduzida para português) | Agência da União Europeia para o Asilo (europa.eu).

II. CIBERSEGURANÇA E INFRAESTRUTURAS CRÍTICAS

Desde o início da guerra, os intervenientes privados e as operações criminosas publicitaram o facto de estarem a realizar ciberatividades para apoiar uma das partes. O ativismo háquer[4] constitui uma ameaça devido ao risco de efeitos induzidos na UE contra serviços críticos, ao risco de ataques provenientes de redes oficiais ou a outros efeitos induzidos imprevistos. Embora, até à data, a guerra tenha sido, em grande medida, travada por meios convencionais, com efeitos induzidos limitados, o risco de escalada neste domínio é real.

Por conseguinte, a UE intensificou a sua coordenação e preparação. As ameaças suscitadas pela guerra sublinham a necessidade de criar uma cultura de intercâmbio de informações e conhecimentos especializados entre a UE e os Estados-Membros, bem como entre as comunidades de cibersegurança. Tal inclui a criação de um conhecimento situacional integrado, partilhado pelas instituições, órgãos e organismos da UE e pelos Estados-Membros, em especial no que diz respeito às infraestruturas críticas de que depende o bom funcionamento do mercado interno.

Atribuição de ciberataques contra a Ucrânia

Os ciberataques contra a própria Ucrânia tiveram início antes da agressão russa e, nos primeiros dias da guerra[5], visavam comprometer as contas de utilizador dos militares da Ucrânia e afetar os serviços essenciais, incluindo o controlo fronteiriço e as telecomunicações.

Em 14 de janeiro de 2022, o alto representante fez uma declaração[6], em nome da União Europeia, condenando os ciberataques contra a Ucrânia e reiterando o apoio inequívoco da UE à Ucrânia.

Em 10 de maio, a União Europeia e os seus Estados-Membros, juntamente com parceiros internacionais, condenaram veementemente[7] a ciberatividade maliciosa contra a Ucrânia, em 24 de fevereiro, que visou a rede de satélite Ka-Sat, explorada pela Viasat, e atribuiu diretamente o ataque à Federação da Rússia. Este ciberataque teve um impacto significativo, causando interrupções e perturbações indiscriminadas de comunicação em várias autoridades públicas, empresas e utilizadores na Ucrânia, tendo afetado também vários Estados-Membros da UE.

---

4 Um exemplo recente de ativismo háquer consiste na utilização de «protestware» para difundir *software* malicioso aos IP russos através de um pacote popular de fonte aberta, o que pode conduzir a riscos na cadeia de aprovisionamento e à perda de confiança na comunidade de fonte aberta. A Comissão deixou claro que os ciberataques (mesmo bem-intencionados) contra a Rússia são ilegais.

5 Relatório especial da Microsoft: *An overview of Russia's cyberattack activity in Ukraine* (não traduzido para português); *The hybrid war in Ukraine – Microsoft On the Issues* (não traduzido para português).

6 https://www.consilium.europa.eu/pt/press/press-releases/2022/01/14/ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-cyberattack-against-ukraine/.

7 Ciberoperações russas contra a Ucrânia: Declaração do alto representante em nome da União Europeia (europa.eu).

Vigilância e coordenação

Desde o início da guerra de agressão da Rússia contra a Ucrânia, o acompanhamento da situação em matéria de cibersegurança nos Estados-Membros e nas instituições da UE aumentou. A ENISA, a Agência da UE para a Cibersegurança, o Centro Europeu da Cibercriminalidade da Europol e da CERT-UE, a Equipa de Resposta a Emergências Informáticas para as instituições e agências da UE, e o Centro de Situação e de Informações da UE (INTCEN) contribuíram para o conhecimento situacional comum da UE, nomeadamente ao realizarem a monitorização regular das ciberatividades suspeitas, incluindo em setores específicos como a energia, os transportes e a aviação, e forneceram avaliações para orientar a ação preventiva.

Também foi intensificada a coordenação e o intercâmbio de informações com redes de cibersegurança, como a Rede de Organizações de Coordenação de Cibercrises (CyCLONe), que inclui agências nacionais de cibersegurança, a Comissão e a ENISA. A fim de refletir esta abordagem a nível interno nas instituições da UE, um mecanismo de coordenação, o grupo de trabalho para cibercrises, permite o intercâmbio de informações entre todos os serviços, órgãos e agências competentes, incluindo a ENISA, o Centro Europeu da Cibercriminalidade da Europol e o CERT-UE. São necessários esforços constantes para garantir canais de comunicação entre os níveis político, operacional e técnico, bem como para reforçar a cooperação com a rede de equipas de resposta a incidentes de segurança informática (CSIRT).

A Europol também acionou o Protocolo da UE relativo à resposta de emergência dos serviços repressivos, que permite reforçar a monitorização das ciberameaças e o intercâmbio de informações entre um vasto leque de partes interessadas, a fim de criar um quadro abrangente de ciberinformações.

Para além das ciberameaças, verifica-se uma maior vigilância por parte dos Estados-Membros, do SEAE e dos serviços da Comissão no que diz respeito à exposição das infraestruturas críticas a ameaças físicas, não cibernéticas. As infraestruturas críticas e as entidades que as exploram podem estar expostas a riscos físicos, como a sabotagem por parte de um Estado ou por intervenientes patrocinados por um Estado, no âmbito de eventuais medidas de retaliação contra a UE.

Preparação

A preparação no domínio da cibersegurança e da segurança das infraestruturas críticas é mais essencial do que nunca, dado o aumento da exposição da Europa a uma acumulação de ameaças decorrentes da guerra. Os esforços para intensificar a preparação incluíram uma série de ações diretas, entre as quais algumas já previstas antes da agressão da Rússia contra a Ucrânia. Incluem exercícios, orientações, medidas legislativas, aumento da resiliência em setores críticos e colaboração com parceiros.

No início de 2022, a Presidência francesa do Conselho da União Europeia, juntamente com o Serviço Europeu para a Ação Externa (SEAE) e a Agência da União Europeia para a Cibersegurança (ENISA), organizaram um exercício baseado em cenários, designado EU CyCLES (*Cyber Crisis Linking Exercise on Solidarity*), com o objetivo de promover a

sensibilização a nível político e reforçar a cooperação entre os níveis operacional e político em caso de um ciberataque em grande escala.

Em fevereiro, a ENISA e a CERT-UE publicaram **orientações** sobre a forma de aumentar a resiliência e a preparação na UE[8], que incentivam todas as organizações dos setores público e privado da UE a adotarem um conjunto mínimo de boas práticas em matéria de cibersegurança, a fim de melhorar substancialmente a cultura de cibersegurança. Em março, a CERT-UE publicou orientações técnicas de acompanhamento, com o apoio da ENISA[9], bem como orientações em matéria de segurança para reforçar a configuração das aplicações Signal[10], com uma série de recomendações práticas para as organizações melhorarem a sua postura no domínio da cibersegurança.

Iniciativas legislativas

A situação atual sublinha a urgência de **executar a legislação em vigor** e de acelerar a **adoção de iniciativas pendentes**.

A Comissão está a apoiar os Estados-Membros na execução da **Diretiva SRI**[11], que exige que os Estados-Membros estejam devidamente equipados, por exemplo, com uma Equipa de Resposta a Incidentes de Segurança Informática (CSIRT) e ao definirem as autoridades competentes. Proporciona uma base para uma cooperação eficaz entre os Estados-Membros. O acordo político alcançado pelos colegisladores sobre a **Diretiva SRI 2**[12] constitui mais um avanço na criação de um sólido quadro de preparação da UE.

SRI 2 – Continuar a reforçar a preparação

- A nova diretiva relativa às redes e aos sistemas de informação dará resposta às deficiências da anterior Diretiva SRI, a fim de a adaptar às necessidades atuais e preparando-a para o futuro. Estabelece regras mínimas para um quadro regulamentar, bem como mecanismos para uma cooperação eficaz entre as autoridades competentes em cada Estado-Membro.
- Alarga o âmbito das regras, aditando novos setores críticos para a economia e a sociedade (por exemplo, os setores farmacêutico e dos dispositivos médicos ou da produção alimentar). Todas as entidades de média e grande dimensão que operam nos setores ou prestam serviços abrangidos pela diretiva serão abrangidas pelo seu âmbito. São igualmente abrangidas as entidades da administração pública a nível central (excluindo o sistema judiciário, os parlamentos e os bancos centrais), bem como a nível regional. Além disso, os Estados-Membros podem decidir se é aplicável a essas entidades a nível local.
- A SRI 2 definirá a base de referência para as medidas de gestão dos riscos de cibersegurança e estabelecerá formalmente a Rede Europeia de Organizações de

[8] *Boosting your Organisation's Cyber Resilience – Joint Publication* (não traduzido para português), de 14 de fevereiro de 2022.

[9] *CERT-EU Security Guidance 22-001 – Cybersecurity mitigation measures against critical threats* (não traduzido para português).

[10] *CERT-EU Security Guidance 22-002 – Hardening Signal* (não traduzido para português).

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

[12] COM(2020) 823.

Coordenação de Cibercrises, a UE-CyCLONe, que apoiará a gestão coordenada de incidentes de cibersegurança em grande escala.

- A proposta introduz igualmente disposições mais precisas sobre o processo de notificação de incidentes, o teor dos relatórios e os prazos, e prevê vias de recurso e sanções para assegurar a execução.
- Os Estados-Membros terão 21 meses, após a entrada em vigor da diretiva, para proceder à incorporação das disposições na sua legislação nacional.

Os progressos no âmbito da SRI 2 devem ser seguidos, o mais rapidamente possível, pela conclusão das negociações sobre a proposta de **diretiva relativa à resiliência das entidades críticas**[13] («Diretiva REC»), que, uma vez adotada e executada, deverá aumentar a resiliência das entidades críticas a uma série de ameaças, incluindo ataques terroristas, ameaças internas ou sabotagem. É igualmente essencial que o nível de ambição da diretiva relativa à resiliência das entidades críticas corresponda ao da proposta da Comissão e que seja mantida a coerência com o compromisso político alcançado sobre a SRI 2. Em conjunto, estas medidas reforçarão a resiliência e a preparação, ao instituir um sistema mais coerente e sólido, nomeadamente através de planos nacionais de resposta a incidentes e crises. Fizeram igualmente parte da recomendação da Comissão do ano passado[14] que cria a **ciberunidade conjunta**, que define a forma como os diferentes intervenientes no ecossistema de cibersegurança (diplomáticos, policiais, civis e, se for caso disso, do setor defesa) devem cooperar a nível operacional. O atual panorama de ameaças sublinha o valor de tal cooperação eficaz entre os principais intervenientes.

A Comissão continua a acompanhar a execução do conjunto de instrumentos em matéria de cibersegurança das redes **5G**[15]. Neste contexto, em 11 de maio, o grupo de cooperação SRI adotou um relatório sobre a segurança da Open RAN[16]. Continua também a colaborar com os Estados-Membros para que o Centro Europeu de Competências em Cibersegurança fique plenamente operacional.

Em 22 de março de 2022, a Comissão propôs **novas regras para estabelecer medidas comuns de cibersegurança e segurança da informação em todas as instituições, órgãos e organismos da UE**. Estas regras reforçarão a resiliência e a capacidade de resposta da administração da UE face a ciberameaças e incidentes. Ao colocar estas atividades num quadro comum, reforçar-se-á a cooperação interinstitucional e a exposição ao risco será minimizada. A proposta de **regulamento relativo à cibersegurança nas instituições, órgãos e organismos da União**[17] reforçará o mandato da CERT-UE e conduzirá à criação de um Conselho Interinstitucional para a Cibersegurança, reforçará as capacidades em matéria de cibersegurança e estimulará avaliações periódicas da maturidade e uma melhor ciber-higiene. A proposta de **regulamento relativo à segurança da informação**[18] criará um conjunto mínimo de regras e normas de segurança da informação para o tratamento e o intercâmbio

[13] COM(2020) 829.
[14] Recomendação relativa à criação de uma ciberunidade conjunta | Estratégia Digital Europeia (não traduzido para português) (europa.eu).
[15] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.
[16] Grupo de cooperação SRI, Relatório sobre a cibersegurança da Open RAN, 11 de maio de 2022.
[17] COM(2022) 122.
[18] COM(2022) 119.

seguros de informações de todas as instituições, órgãos e organismos da União, a fim de assegurar uma proteção reforçada e coerente contra a evolução das ameaças às suas informações. A Comissão insta o Parlamento Europeu e o Conselho a adotarem rapidamente estas medidas.

A Comissão concluiu agora a sua consulta pública sobre as medidas destinadas a reforçar a **ciber-resiliência** dos produtos digitais, preparando uma proposta a publicar no outono[19]. Tal dará resposta às vulnerabilidades dos produtos digitais e dos serviços auxiliares que, embora criem oportunidades para as economias e as sociedades da UE, também conduzem a novos desafios, uma vez que quanto mais tudo estiver ligado, mais fácil é que um incidente de cibersegurança afete todo um sistema e, por conseguinte, perturbe as atividades económicas e sociais.

Em 9 de março de 2022, os ministros da UE responsáveis pelas telecomunicações adotaram por unanimidade o Apelo Nevers para reforçar as capacidades da UE em matéria de cibersegurança, que incluía «a execução de um novo Fundo de Resposta de Emergência para a Cibersegurança, a criar pela Comissão»[20]. A Comissão está a refletir sobre a melhor utilização dos fundos existentes para apoiar ações preventivas e de resposta.

Setores críticos

A segurança do aprovisionamento **energético** da UE é fundamental para o bem-estar dos cidadãos e para o bom funcionamento das nossas economias, e a situação atual destacou a necessidade de regras claras em matéria de cibersegurança neste setor. A Comissão está a trabalhar num código de rede para a cibersegurança dos fluxos transfronteiriços de eletricidade, conforme exigido pelo Regulamento Eletricidade[21], a fim de estabelecer regras em matéria de avaliação dos riscos, requisitos mínimos comuns, planeamento, acompanhamento, elaboração de relatórios e gestão de crises. Desde o início da guerra de agressão da Rússia contra a Ucrânia, os objetivos previstos para o código de rede para a cibersegurança são ainda mais pertinentes. A Comissão lançou igualmente uma cooperação estrutural entre a ENISA, a REORTE[22], a REORTG[23] e a Comunidade da Energia no acompanhamento regular da situação da cibersegurança no setor da energia.

A UE tem envidado esforços para proteger a segurança dos parceiros sem criar riscos para si própria. A sincronização de emergência das redes elétricas da Ucrânia e da Moldávia com a rede europeia continental teve lugar em março de 2022, após a adoção de medidas de atenuação dos riscos, nomeadamente em termos de cibersegurança.

A guerra e as sanções criaram também muitos desafios para os **transportes** da UE, desde riscos para a segurança da aviação civil da UE e dos condutores de camiões em zonas de

---

19 Diretiva Ciber-Resiliência: novas regras em matéria de cibersegurança para produtos digitais e serviços auxiliares.

20 *08/03/2022 – Déclaration conjointe des ministres de l'Union européenne chargés du numérique et des communications électroniques adressée au secteur numérique – Presse – Ministère des Finances (economie.gouv.fr)* (não traduzido para português).

21 Regulamento (UE) 2019/943 do Parlamento Europeu e do Conselho, de 5 de junho de 2019, relativo ao mercado interno da eletricidade (JO L 158 de 14.6.2019, p. 54). A proposta está atualmente a ser analisada pela Agência de Cooperação dos Reguladores da Energia.

22 Rede Europeia dos Operadores das Redes de Transporte de Eletricidade.

23 Rede Europeia dos Operadores das Redes de Transporte de Gás.

conflito, até à destruição das infraestruturas de transporte ucranianas, cortando as cadeias de aprovisionamento e ameaçando a segurança alimentar mundial. A Agência da União Europeia para a Segurança da Aviação, em estreita cooperação com a Comissão e o Eurocontrol, a Organização Europeia para a Segurança da Navegação Aérea, aconselhou os operadores, desde o início da guerra, a não operarem no espaço aéreo da Ucrânia e a evitarem utilizar o espaço aéreo a menos de 100 milhas náuticas da fronteira bielorussa e entre a Rússia e a Ucrânia.

A Comissão tem trabalhado no sentido de reforçar a preparação e a resiliência do setor dos transportes da UE. Em especial, um novo plano de contingência para os transportes[24], adotado em 23 de maio, retira ensinamentos da pandemia de COVID-19 e da agressão militar da Rússia contra a Ucrânia. Propõe um conjunto de 10 ações destinadas a orientar a UE e os seus Estados-Membros na introdução de medidas de emergência de resposta a crises, incluindo garantir a conectividade mínima, reforçar a resiliência cibernética e a ameaças híbridas e reforçar a cooperação com parceiros internacionais em matéria de preparação e resposta a situações de crise. Salienta igualmente a importância de testes regulares da resiliência para diferentes cenários de crise, reunindo as agências competentes da UE ou outros intervenientes e baseando-se nos processos existentes.

No âmbito do quadro de **Segurança da Saúde da UE**, o intercâmbio de informações com base no Sistema de Alerta Rápido e de Resposta, incluindo o apoio às evacuações médicas da Ucrânia, tem de ser protegido de ciberataques, pelo que a segurança do sistema está a ser reforçada.

Cooperação com parceiros

A UE continua a trabalhar com os seus parceiros internacionais a fim de prevenir, desencorajar, dissuadir e dar resposta a comportamentos maliciosos no ciberespaço. A guerra de agressão da Rússia contra a Ucrânia tornou mais importante do que nunca a cooperação neste domínio. A este respeito, o SEAE tem vindo a trabalhar no intercâmbio de conhecimentos situacionais e na coordenação da resposta às ciberatividades maliciosas que visam a Ucrânia, bem como no apoio à Ucrânia e a outros países da região, ao colaborar com parceiros, incluindo os EUA e a OTAN, a fim de assegurar a complementaridade e evitar sobreposições.

A estreita cooperação com os EUA intensificou-se igualmente no contexto do Conselho de Comércio e Tecnologia UE-EUA (CCT). A declaração conjunta[25] na sequência da reunião ministerial realizada em Paris, em maio, destacou o papel central do CCT na parceria transatlântica renovada, que visa coordenar as medidas conjuntas da UE e dos EUA face à agressão russa contra a Ucrânia. Ambas as partes concordaram que uma cooperação estreita para promover a resiliência das cadeias de aprovisionamento é mais importante do que nunca. Além disso, foi criado um grupo de trabalho específico para o financiamento público de infraestruturas digitais seguras e resilientes em países terceiros, a fim de preparar o caminho para o financiamento público conjunto pelos Estados Unidos e a UE de projetos digitais em países terceiros, com base num conjunto de princípios gerais comuns.

A Bússola Estratégica adotada em março de 2022 (consultar secção VII) reforçará ainda mais o conjunto de instrumentos de ciberdiplomacia da UE e desenvolverá a política da UE para a

[24] COM(2022) 21.

[25] https://ec.europa.eu/commission/presscorner/detail/pt/STATEMENT_22_3108.

ciberdefesa, a fim de haver uma melhor preparação face a ciberataques e de lhes dar resposta, no âmbito de uma estratégia mais ampla para reforçar a capacidade da UE de agir em situações de crise e defender os seus interesses.

Apoio de cibersegurança à Ucrânia e aos países vizinhos

Antes da guerra, a UE já apoiava a ciber-resiliência da Ucrânia. Já em junho de 2021, a UE e a Ucrânia realizaram um primeiro ciberdiálogo, e a UE prestou apoio à cibersegurança e à transformação digital resiliente através do programa EU4Digital Ucrânia no valor de 25 milhões de EUR. Foi concebido um outro programa de geminação, dotado de 1,5 milhões de EUR, a fim de ajudar as instituições ucranianas de cibersegurança a alinhar-se pelas normas da UE.

Na sequência do início de guerra, a UE está a promover a cooperação entre peritos no domínio cibernético da UE e da Ucrânia e a coordenar a prestação de assistência técnica e o fornecimento de equipamento, *software* e serviços pertinentes, a fim de reforçar a ciber-resiliência e a ciberdefesa da Ucrânia.

Além disso, a UE está a trabalhar no sentido de avaliar o eventual apoio a médio prazo à Moldávia, à Geórgia e aos Balcãs Ocidentais. Em 3 e 4 de março de 2022, realizou-se uma missão de avaliação conjunta das necessidades de cibersegurança na Moldávia, que resultou na adoção de uma medida específica de resposta a situações de crise para intensificar rapidamente a cibersegurança no país. Está a ser preparado um apoio de resposta rápida semelhante para um número restrito de países dos Balcãs Ocidentais, considerados particularmente expostos a riscos devido ao seu alinhamento com as sanções da UE. Está também a ser avaliada a possibilidade de prestar assistência adicional à Moldávia através do Mecanismo Europeu de Apoio à Paz.

III. CRIMINALIDADE ORGANIZADA E TERRORISMO

A guerra de agressão da Rússia contra a Ucrânia obrigou milhões de pessoas a abandonarem as suas casas, aumentando consideravelmente a circulação através das fronteiras externas da UE. Até 18 de maio, tinham chegado à UE cerca de 6 milhões de pessoas provenientes da Ucrânia e da Moldávia e, até à data, 2,8 milhões tinham solicitado para proteção temporária na UE. A UE procurou proporcionar o acolhimento mais rápido e flexível possível às pessoas que fugiam da guerra, sem comprometer a segurança nas fronteiras externas da UE. A UE tomou medidas sem precedentes para proporcionar proteção temporária às pessoas que fugiam da guerra e está empenhada em tratar sem discriminação todos os recém-chegados. Ao mesmo tempo, os riscos potenciais que possam advir da circulação de tantas pessoas não podem ser negligenciados e a UE, com o forte apoio das agências competentes da UE, permanece vigilante em relação aos novos desenvolvimentos no domínio da criminalidade organizada e do terrorismo.

Um espaço Schengen forte num momento de aumento das ameaças

A garantia de um elevado nível de segurança no espaço **Schengen** e na UE nunca foi tão importante como na atmosfera de aumento das ameaças que decorre da guerra, logo além das fronteiras externas da UE.

Cumprindo a ambiciosa agenda para o espaço Schengen definida na estratégia de junho de 2021, a Comissão adotou, em maio, o primeiro Relatório sobre o Estado de Schengen[26]. O ciclo anual de Schengen proporciona um novo modelo de governação para o espaço Schengen, com um controlo regular do estado de Schengen, o que contribuirá para assegurar a rápida identificação de deficiências, bem como procedimentos de acompanhamento eficazes, a fim de tornar o espaço Schengen mais forte e resiliente.

Este primeiro relatório reconhece a necessidade de intensificar os esforços no sentido de executar as principais iniciativas a nível da UE, incluindo controlos sistemáticos de todos os viajantes nas fronteiras externas, tirando pleno partido dos mandatos da Frontex e da Europol, bem como dos instrumentos propostos e disponíveis de cooperação policial transfronteiriça.

Em especial, a nova arquitetura dos sistemas de informação da UE para as fronteiras, a migração e a segurança, bem como a sua interoperabilidade, são a pedra angular dos esforços para melhorar a segurança interna e a gestão das fronteiras. Será crucial a execução efetiva de todos os elementos do quadro de interoperabilidade, em consonância com os prazos acordados.

Vigilância e coordenação

O reforço da cooperação policial em todos os Estados-Membros e com países terceiros é fundamental a fim de garantir a sensibilização para as ameaças criminosas e terroristas emergentes, bem como a ação contra as redes criminosas e as pessoas que possam tentar tirar partido da guerra contra a Ucrânia. Os Estados-Membros e os parceiros operacionais partilham ativamente as informações disponíveis e as informações criminais pertinentes com a Europol, que procede a controlos cruzados e à análise das informações e as transformam em notificações operacionais acionáveis das informações, como notificações de alerta precoce e avaliações de ameaças, que são partilhadas com os parceiros.

Criminalidade organizada

A criminalidade organizada já está a encontrar formas de explorar a situação atual. A análise inicial dos serviços de informação identificou padrões de criminalidade numa série de domínios, incluindo o tráfico de seres humanos, as falsas declarações de mercadorias importadas e exportadas, a fraude em linha, a cibercriminalidade e o tráfico de armas de fogo. Existem igualmente provas de que os cibercriminosos simulam angariações de fundos destinados à Ucrânia, a fim de roubarem dinheiro e criptomoedas[27]. As organizações criminosas da Ucrânia podem tentar deslocalizar-se devido à situação atual e prosseguir as suas atividades na UE.

[26] COM(2022) 301.

[27] O Grupo de Análise de Ameaças da Google constatou um número crescente de autores de ameaça que utilizam a guerra na Ucrânia como isco em campanhas de mistificação da interface (*phishing*) e de *software* malicioso (*malware*). Os investigadores da Cyren, uma empresa de segurança da Internet, referem um aumento das fraudes com criptomoedas que tiram partido do conflito através da utilização de sítios Web destinados a falsas doações.

A Comissão e a Presidência francesa do Conselho trabalharam em conjunto, bem como com as agências JAI da UE, nomeadamente a Europol, a fim de mobilizar a Plataforma Multidisciplinar Europeia contra as Ameaças Criminosas (**EMPACT**), com o objetivo de avaliar, antecipar, prevenir e combater as ameaças da criminalidade grave e organizada existentes ou emergentes. Em 7 de abril de 2022, a Europol organizou uma reunião da EMPACT que reuniu representantes e peritos dos Estados-Membros da UE e da comunidade de segurança da UE, a fim de se centrar nas ameaças da criminalidade grave e organizada que surgiram em resultado da guerra na Ucrânia. As medidas concretas debatidas incluíram a recolha de mais informações, a execução de ações operacionais de emergência e a reorientação das ações existentes, bem como jornadas de ação conjunta *ad hoc*.

A **CELBET** – Customs Eastern and South-Eastern Land Border Expert Team (Equipa de peritos nas alfândegas das fronteiras terrestres de Leste e de Sudeste), um projeto de colaboração financiado pela Comissão Europeia, está a acompanhar os desenvolvimentos na fronteira, no âmbito da sua missão de prestar orientação e apoio operacional aos funcionários aduaneiros, bem como as apreensões aduaneiras nos pontos de passagem da fronteira da UE (Polónia, Eslováquia, Hungria e Roménia) com a Ucrânia.

Atividades criminosas e terroristas

Embora ainda não tenha surgido uma ameaça terrorista imediata na UE relacionada com a invasão russa da Ucrânia, a necessidade de vigilância é evidente.

Os riscos acrescidos de atividades criminosas e terroristas sublinham a importância de os Estados-Membros utilizarem as bases de dados pertinentes da UE, como o Sistema de Informação de Schengen, de modo a introduzirem dados sempre que necessário e de as consultarem no decurso de controlos das pessoas que entram na UE, o que contribuirá para garantir que as pessoas que representam uma ameaça para a segurança interna da UE sejam identificadas nas fronteiras externas. A eu-LISA, a Agência da União Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça, continua a assegurar a plena disponibilidade e eficácia dos sistemas de gestão das fronteiras da UE. As orientações[28] destinadas aos Estados-Membros clarificaram a forma de equilibrar a necessidade de assegurar um tratamento harmonioso das pessoas que chegam às fronteiras externas, sem deixar de efetuar os controlos de segurança necessários.

Preparação

Para além das orientações e da coordenação, a preparação da UE foi reforçada através do destacamento de pessoal das agências da UE.

A **Europol** destacou equipas operacionais para os Estados-Membros da UE vizinhos da Ucrânia. Essas equipas incluíam agentes convidados da Europol provenientes dos Estados-Membros e peritos da Europol na Eslováquia, na Hungria, na Lituânia, na Polónia e na

[28] Comunicação da Comissão que fornece orientações operacionais para a gestão das fronteiras externas a fim de facilitar as passagens de fronteira nas fronteiras entre a UE e a Ucrânia (2022/C 104 I/01).

Roménia, bem como na Moldávia[29]. Os agentes convidados da Europol apoiam as autoridades nacionais com controlos de segurança de segunda linha nas fronteiras externas da UE. Os peritos da Europol prestam apoio através da recolha e avaliação de informações para detetar ameaças terroristas e criminosas, apoiar as investigações e identificar as pessoas que representam um risco ao tentarem entrar na UE. Estas equipas operacionais recolhem informações que contribuem para as avaliações das ameaças criminosas à disposição dos Estados-Membros. Esta atividade de recolha de informações permite à Europol antecipar os desenvolvimentos e coordenar as atividades operacionais com os Estados-Membros da UE, a fim de dar resposta às atividades dos grupos criminosos que procuram tirar partido da guerra na Ucrânia, bem como para desenvolver o compromisso ativo da Europol com as autoridades policiais ucranianas através do agente de ligação ucraniano presente na sede da Europol nos Países Baixos.

A **Agência Europeia da Guarda de Fronteiras e Costeira** (**Frontex**) também está presente nos Estados-Membros e nos países vizinhos da UE para apoiar operações de controlo fronteiriço: estão atualmente destacados mais de 2 100 guardas de fronteira em toda a UE, nos Balcãs Ocidentais e na Moldávia. O **Gabinete Europeu de Apoio em matéria de Asilo** (**EASO**) destacou quase 750 funcionários para os Estados-Membros meridionais da UE e para a Lituânia, a fim de apoiar atividades operacionais, reforçar as capacidades de acolhimento e ajudar nos procedimentos de asilo.

Com base na atual **Decisão Prüm**[30], que estabelece um quadro para os Estados-Membros destacarem agentes da autoridade para operações conjuntas, como patrulhas conjuntas, a Comissão e a Presidência francesa do Conselho da União Europeia enviaram uma carta conjunta a todos os Estados-Membros para identificar as necessidades e solicitar o destacamento de agentes policiais, a fim de lançar patrulhas conjuntas nos Estados-Membros de primeira linha da UE mais afetados pelas passagens de fronteira em massa resultantes da guerra. A Comissão financiará estes destacamentos ao abrigo do Fundo para a Segurança Interna – Polícia.

Luta contra o tráfico de seres humanos

Desde os primeiros dias da guerra, a UE tem sido alertada para os riscos de um domínio específico de atividade criminosa que pode beneficiar da enorme circulação de pessoas em busca de segurança na UE. Tem sido essencial evitar que os traficantes de seres humanos visem pessoas vulneráveis em circulação, na sua maioria **mulheres e crianças**, utilizando, por exemplo, falsas ofertas de transporte ou alojamento.

Em março, a Europol e a Eurojust emitiram notificações de alerta precoce às autoridades nacionais competentes sobre o eventual tráfico de seres humanos e a exploração das vítimas provenientes da Ucrânia. A Eurojust contribui para reforçar o intercâmbio de informações e acelerar a cooperação judiciária, nomeadamente com a Ucrânia. Além disso, as investigações sobre o tráfico de seres humanos foram remetidas para a agência para coordenação.

[29] A partir de 3 de maio, a Europol destacou um funcionário da Europol e três agentes convidados para a Eslováquia, um agente da Europol para a Polónia, um agente da Europol e quatro agentes convidados para a Roménia, bem como dois agentes convidados para a Hungria. Um funcionário da Europol e dois agentes convidados estão destacados para a Moldávia.

[30] 2008/615/JAI, 2008/616/JAI.

O Coordenador da Luta Antitráfico da UE realizou reuniões com a rede da UE de relatores nacionais ou mecanismos equivalentes, as agências encarregadas da justiça e dos assuntos internos e a Plataforma da sociedade civil da UE de luta contra o tráfico de seres humanos, a fim de proceder ao intercâmbio de informações sobre as medidas necessárias para prevenir e combater os abusos e proteger as vítimas. Foram abertos inquéritos em vários Estados-Membros sobre eventuais processos.

A UE tem sido rápida e enérgica na garantia de uma resposta coordenada a esta ameaça real para as pessoas que necessitam da ajuda da UE. Foram rapidamente disponibilizadas orientações operacionais[31], nomeadamente sobre o desafio do tráfico de seres humanos, aos Estados-Membros que transpuseram a Diretiva de Proteção Temporária, a fim de apoiar as pessoas que fogem da guerra na Ucrânia. No âmbito do plano de 10 pontos para reforçar a coordenação europeia em matéria de acolhimento das pessoas que fogem da guerra da Ucrânia[32], apresentado no Conselho «Justiça e Assuntos Internos» de 28 de março de 2022, o Coordenador da Luta Antitráfico da UE, em cooperação com as agências da UE e os Estados-Membros, elaborou um plano comum de luta contra o tráfico de seres humanos[33] sobre a prevenção do tráfico de seres humanos e a ajuda às vítimas. O registo de entidades e pessoas (incluindo voluntários) que pretendem disponibilizar alojamento, transporte e outros tipos de assistência, bem como a realização de verificações de antecedentes, é uma prioridade especial. A Comissão estabeleceu igualmente uma ligação com a EASO para apoiar a deteção de vítimas de tráfico de seres humanos quando são realizados exames médicos nos centros de acolhimento. As crianças não acompanhadas ou separadas correm um risco especial de abuso, exploração sexual ou criminalidade forçada. As orientações operacionais acima referidas também fornecem orientações para ajudar os Estados-Membros que lidam com a chegada, o acolhimento e o apoio às crianças e, em especial, aos menores não acompanhados. A fim de sensibilizar as pessoas em risco, a Comissão lançou igualmente um sítio Web específico com uma secção que inclui aconselhamento prático sobre como evitar os traficantes.

Embora tenham sido tomadas algumas medidas para reforçar a preparação, especificamente em resposta à nova situação suscitada pela guerra, outras medidas fundamentais decorrem de **iniciativas legislativas** já em preparação antes da guerra de agressão da Rússia contra a Ucrânia.

A Comissão congratula-se com o acordo alcançado em fevereiro de 2022 relativo ao mandato revisto da **Europol**[34], que, uma vez executado, permitirá à Europol apoiar melhor os Estados-Membros na luta contra a criminalidade organizada e o terrorismo. A agência disporá então das garantias e dos instrumentos adequados para apoiar as forças policiais na análise de megadados, a fim de investigar a criminalidade, e no desenvolvimento de métodos de vanguarda para combater a cibercriminalidade. Estas alterações são acompanhadas por um quadro reforçado em matéria de proteção de dados, bem como por um reforço da supervisão e da responsabilização parlamentar.

[31] C/2022/1806, EUR-Lex – 52022XC0321(03) – PT – EUR-Lex (europa.eu).
[32] https://ec.europa.eu/home-affairs/10-point-plan-stronger-european-coordination-welcoming-people-fleeing-war-ukraine_en.
[33] https://ec.europa.eu/home-affairs/news/new-anti-trafficking-plan-protect-people-fleeing-war-ukraine-2022-05-11_en.
[34] COM(2020) 796.

O pacote sobre **cooperação policial** apresentado pela Comissão em 8 de dezembro de 2021[35], e atualmente em negociação, reforçará a cooperação entre os agentes da autoridade dos Estados-Membros, ao tornar o intercâmbio de dados mais rápido, fácil e seguro, bem como ao reforçar e tornar mais eficaz a cooperação policial operacional no terreno. A Comissão insta o Parlamento Europeu e o Conselho a adotarem rapidamente este pacote.

Uma vez adotadas e executadas, estas propostas legislativas apoiarão a aplicação da lei na luta contra a criminalidade organizada transfronteiriça, o que será especialmente importante num contexto em que as organizações criminosas da Ucrânia podem tentar deslocalizar-se devido à situação atual e prosseguir as suas atividades na UE.

A **Missão de Aconselhamento da UE na Ucrânia** tem vindo a apoiar a reforma das instituições de aplicação da lei e do Estado de direito no país desde 2014. Em março de 2022, o mandato da missão foi revisto, permitindo o apoio nos pontos de passagem de fronteira da Ucrânia com a Eslováquia, a Polónia e a Roménia, contribuindo para o conhecimento situacional sobre as atividades criminosas transfronteiriças, incluindo o tráfico de seres humanos, bem como para o fluxo da ajuda humanitária para a Ucrânia.

IV. ARMAS, MATERIAIS PERIGOSOS E INCIDENTES CRÍTICOS

A guerra aumentou drasticamente a circulação de armas de fogo e de outras armas na própria Ucrânia, o que representa novos riscos para a UE e outros Estados vizinhos da Ucrânia.

Vigilância e coordenação

As orientações operacionais emitidas em março forneceram aconselhamento aos Estados-Membros sobre como enfrentar o desafio da crescente circulação de armas de fogo num momento de chegada em massa às fronteiras externas da UE[36]. Estas orientações sublinham que a presença de armas de fogo deve ser continuamente verificada e que ninguém sem autorização deve ser autorizado a entrar na UE com uma arma de fogo. Quando alguma destas armas de fogo for declarada pelas autoridades ucranianas como desaparecida, os Estados-Membros devem comunicá-las no Sistema de Informação de Schengen.

É fundamental que todas as remessas de armas de fogo para a Ucrânia sejam devidamente registadas, com todas as informações pertinentes (incluindo o tipo, o país e o ano de fabrico, a marca, o modelo, o calibre e o número de série), a fim de facilitar a rastreabilidade dessas armas de fogo, tanto na Ucrânia como na UE.

A UE lamentou publicamente os ataques militares imprudentes da Rússia em instalações civis nucleares, biológicas e químicas na Ucrânia, bem como nas suas proximidades diretas, além de todos os atos que comprometam a segurança dessas instalações. A Comissão acompanha a situação na Ucrânia, prestando especial atenção à ameaça radiológica que constitui a maior preocupação do ponto de vista da segurança interna da UE[37]. A Comissão acompanha

[35] COM(2021) 780, COM(2021) 782, COM(2021) 784.

[36] Comunicação da Comissão que fornece orientações operacionais para a gestão das fronteiras externas a fim de facilitar as passagens de fronteira nas fronteiras entre a UE e a Ucrânia, 2022/C 104 I/01.

[37] A Comissão organizará, em cooperação com os parceiros dos EUA, um seminário centrado nos riscos relacionados com materiais radiológicos localizados em hospitais que saem do controlo regulamentar.

igualmente as potenciais ameaças químicas e criou um mecanismo de coordenação interna caso seja necessária uma avaliação rápida dos riscos.

Preparação

A Ucrânia já é um dos países identificados como fundamentais para ações específicas a nível externo no Plano de Ação da UE sobre o Tráfico de Armas de Fogo para 2020-2025. Existe igualmente uma ação operacional específica na região, incluindo a Ucrânia, no quadro da EMPACT para as armas de fogo. Todavia, tendo em conta os riscos de desvio de armas de fogo, serão necessários projetos específicos financiados pela UE, bem como a cooperação operacional com a Europol, a Frontex e a vertente da EMPACT para as armas de fogo. Em breve, a Comissão apresentará uma proposta de revisão do regulamento relativo às armas de fogo[38] no que respeita às exportações, importações e trânsito de armas de fogo para utilização civil, no âmbito do quadro jurídico e operacional geral para prevenir, detetar, investigar e reprimir o tráfico de armas de fogo.

A fim de melhorar a preparação e a resposta da UE aos riscos para a saúde pública, como as ameaças QBRN, a Comissão está a criar reservas estratégicas de capacidades de resposta através do Mecanismo de Proteção Civil da União Europeia (MPCUE), financiado pela Autoridade de Preparação e Resposta a Emergências Sanitárias (HERA)[39]. Os serviços da Comissão estão a colaborar no desenvolvimento de uma reserva estratégica rescEU de 540,5 milhões de EUR. Esta reserva consistirá de equipamento e medicamentos, vacinas e outras terapêuticas para o tratamento de doentes expostos a agentes de emergência QBRN, bem como de uma reserva de descontaminação rescEU vocacionada para o fornecimento de equipamento de descontaminação e a disponibilização de equipas de resposta especializadas. Como primeiro passo imediato, a UE mobilizou a sua reserva médica rescEU para adquirir comprimidos de iodeto de potássio que podem ser utilizados para proteger as pessoas dos efeitos nocivos das radiações, bem como outros artigos urgentemente necessários na Ucrânia. Já foram entregues à Ucrânia quase três milhões de comprimidos de iodeto através do MPCUE, com a ajuda de França e de Espanha.

V. AÇÃO COORDENADA PARA RESPONSABILIZAR A AGRESSÃO RUSSA

A UE está a desempenhar um papel decisivo nas ações da comunidade internacional no sentido de pressionar a Rússia a pôr termo à sua agressão contra o Estado ucraniano e os civis apanhados no conflito, o que é inaceitável e contrário ao direito internacional. Esta pressão inclui medidas que visam indicar as consequências para os autores, incluindo sanções severas, bem como ações para identificar e facilitar a instauração de processos penais por crimes de guerra.

[38] Regulamento (UE) n.º 258/2012 do Parlamento Europeu e do Conselho, de 14 de março de 2012, que aplica o artigo 10.º do Protocolo das Nações Unidas contra o fabrico e o tráfico ilícitos de armas de fogo, das suas partes e componentes e de munições, adicional à Convenção das Nações Unidas contra o Crime Organizado Transnacional (Protocolo das Nações Unidas sobre as armas de fogo), e estabelece autorizações de exportação e medidas de importação e de trânsito de armas de fogo, suas partes, componentes e munições.

[39] Plano de Trabalho da HERA para 2022 (europa.eu).

Medidas restritivas e confisco

Desde que a Rússia reconheceu as zonas não controladas pelo Estado dos *oblasts* de Donetsk e de Luhansk na Ucrânia, em 21 de fevereiro de 2022, e da invasão da Ucrânia, em 24 de fevereiro de 2022, a UE impôs a maior série de medidas restritivas de sempre contra a Rússia. Até à data, foram adotados cinco pacotes de sanções. Estas medidas centram-se em setores fundamentais, incluindo as finanças, o comércio, os transportes, a defesa e os meios de comunicação social, e visam as elites políticas e militares, bem como os proeminentes oligarcas russos e bielorrussos. As listas incluem já mais de 1 000 pessoas e 80 entidades. Está a ser debatido no Conselho um sexto pacote de sanções.

O impacto destas e das anteriores medidas restritivas contra pessoas e empresas russas e bielorrussas será tão forte quanto a sua aplicação. A coordenação da UE pode dar um contributo importante para colmatar eventuais lacunas e a Comissão prestou um amplo apoio às partes interessadas, por meio de orientações escritas, reuniões das partes interessadas e de um grupo de peritos específico, bem como de uma série de recursos para facilitar o seu cumprimento.

Além disso, a Comissão criou um Grupo de Missão Congelar e Apreender, que reúne os serviços da Comissão, os Estados-Membros, a Eurojust e a Europol. Até à data, os Estados-Membros comunicaram o congelamento de ativos no valor de 9,89 mil milhões de EUR[40]. Em 11 de abril, a Europol, em conjunto com os Estados-Membros, a Eurojust e a Frontex, lançou a Operação Oscar para apoiar investigações financeiras e criminais que visam bens de origem criminosa detidos por pessoas singulares e coletivas abrangidas por sanções da UE relacionadas com a guerra da Rússia contra a Ucrânia. O Grupo de Missão Congelar e Apreender da UE colabora estreitamente com o grupo de trabalho sobre elites, intermediários e oligarcas russos (REPO), criado por países do G7 (Alemanha, Canadá, Estados Unidos, França, Itália, Japão e Reino Unido) e por parceiros que partilham as mesmas ideias, como a Austrália, bem como com o grupo de trabalho KleptoCapture dos EUA e o grupo de trabalho ucraniano.

O Grupo de Missão Congelar e Apreender serve de plataforma para coordenar e facilitar o intercâmbio de informações e experiências entre os Estados-Membros, bem como para proporcionar orientações sobre a aplicação de sanções e para facilitar o intercâmbio de boas práticas em matéria de investigações criminais e confisco. Em especial, é importante que as autoridades policiais estejam alerta e sejam pró-ativas em relação a potenciais crimes cometidos pelas pessoas e entidades sancionadas. O grupo de trabalho visa igualmente fazer avançar os debates sobre a eventual mobilização dos fundos confiscados, por exemplo, para contribuir para a reconstrução da Ucrânia.

A Comissão adota hoje um pacote de **recuperação e confisco de bens**[41], que tem em conta os ensinamentos retirados da aplicação das medidas restritivas da União contra pessoas e entidades russas e bielorrussas. Facilitará a aplicação efetiva das medidas restritivas da União em toda a UE, ao permitir a deteção e a identificação rápidas de bens detidos ou controlados por pessoas ou entidades sujeitas a essas medidas. O quadro reforçado de recuperação e confisco de bens aplicar-se-á igualmente à violação das medidas restritivas, assegurando

[40] Existe igualmente um montante de ativos bloqueados do Banco Central da Rússia de aproximadamente 23 mil milhões de EUR.

[41] COM(2022) 245.

assim a deteção, o congelamento, a gestão e o confisco eficazes dos produtos resultantes da violação das medidas restritivas. A fim de assegurar que os bens das pessoas e entidades que violam as medidas restritivas possam ser efetivamente confiscados, a Comissão hoje adota também propostas de decisão do Conselho no sentido de aditar a violação de sanções à lista de crimes da UE constante do artigo 83.º, n.º 1, do TFUE[42], acompanhada de uma comunicação[43], com vista a propor uma diretiva que aproxime a definição de infrações penais e de sanções aplicáveis às violações das medidas restritivas.

De uma forma mais geral, este pacote constitui um passo crucial na luta contra a criminalidade organizada. Decorre dos compromissos assumidos pela Comissão na Estratégia para a União da Segurança e na estratégia para lutar contra a criminalidade Organizada (2020-2025)[44]. Revê a Diretiva Perda de 2014, a Decisão do Conselho de 2007 relativa aos gabinetes de recuperação de bens (ARO) e a Decisão-Quadro de 2005 relativa à perda de produtos, instrumentos e bens relacionados com o crime, a fim de reforçar as capacidades de deteção e identificação e, em última análise, confiscar ganhos ilícitos, dando resposta às taxas muito baixas de confisco na UE[45]. O pacote alarga o âmbito das infrações penais abrangidas e amplia as regras em matéria de confisco nos casos em que não é possível uma condenação por um crime específico, mas em que os bens provêm claramente de atividades criminosas. A revisão reforça igualmente a gestão eficaz dos bens congelados e confiscados e reforça a capacidade dos ARO para detetar e identificar bens ilícitos. O novo quadro da UE para a recuperação de bens foi concebido para dar resposta ao complexo *modus operandi* das organizações criminosas, que operam frequentemente além-fronteiras e utilizam diferentes métodos para dissimular os seus bens, nomeadamente através de criptoativos.

Resposta judicial coordenada

Estão também em curso trabalhos a nível da UE para assegurar uma resposta judicial coordenada à **criminalidade internacional** alegadamente cometida na Ucrânia, de modo que os autores possam ser responsabilizados.

Dois Estados-Membros e a Ucrânia criaram uma equipa de investigação conjunta (EIC) para investigar crimes de guerra, crimes contra a humanidade e outros crimes internacionais alegadamente cometidos no território ucraniano. A Eurojust presta apoio jurídico, analítico, financeiro e logístico a esta EIC. Em 25 de abril de 2022, o Gabinete do Procurador do Tribunal Penal Internacional (OTP-TPI) aderiu à EIC na qualidade de participante[46], prevendo-se a adesão de outros participantes em breve.

Em 25 de abril de 2022, a Comissão apresentou uma proposta de alteração do Regulamento Eurojust[47], a fim de que a Eurojust conserve, analise e armazene provas dos principais crimes internacionais. A Eurojust e a Europol continuarão a colaborar estreitamente ao longo deste processo. A Rede Genocídio desempenha igualmente um papel fundamental na coordenação da resposta judicial. A Eurojust acolhe o secretariado desta rede, que elaborou um atlas das

[42] COM(2022) 247.
[43] COM(2022) 249.
[44] COM(2021) 170.
[45] A Europol estima que apenas 2 % dos bens de origem criminosa são congelados (2,4 mil milhões de EUR) e 1 % confiscados (1,2 mil milhões de EUR), embora as receitas provenientes da criminalidade nos principais mercados criminosos da UE tenham ascendido a 139 mil milhões de EUR em 2019 (1 % do PIB da UE).
[46] https://www.eurojust.europa.eu/eurojust-and-the-war-in-ukraine.
[47] COM(2022) 187 final.

ONG atualmente ativas na Ucrânia e apoia os profissionais dos Estados-Membros e da Ucrânia que lidam com processos ativos relacionados com a guerra.

Em abril de 2022, o Conselho procedeu novamente à revisão do mandato da **Missão de Aconselhamento da UE na Ucrânia**, abrindo caminho ao apoio da missão às autoridades ucranianas na investigação e repressão de quaisquer crimes internacionais cometidos no contexto da agressão militar da Rússia. A missão prestará aconselhamento estratégico às autoridades ucranianas sobre a investigação e a repressão de crimes internacionais, as alterações necessárias da legislação ucraniana, a estratégia de comunicação, bem como formação sobre matérias conexas. A missão faz parte de uma série de iniciativas de coordenação neste contexto e, juntamente com a delegação da UE, faz parte do grupo consultivo EUA-UE para a Ucrânia sobre as atrocidades.

VI. MANIPULAÇÃO DA INFORMAÇÃO E INGERÊNCIA ESTRANGEIRAS

Os atuais desenvolvimentos geopolíticos sublinharam os riscos de ingerência estrangeira. A agressão militar da Rússia contra a Ucrânia tem sido acompanhada de atividades de **ingerência e manipulação** das informações. Registaram-se alegações infundadas de «nazismo» e «genocídio» contra o Governo ucraniano, operações de falsa bandeira e acusações infundadas contra a OTAN e o Ocidente a fim de justificar ataques brutais contra a Ucrânia, enquanto a liberdade de expressão e a denúncia independente na Rússia foram suprimidas. Persiste o risco de manipulação de material audiovisual e de desinformação que a Rússia possa tentar utilizar como pretexto para novos ataques militares, enfraquecer a determinação da resistência ucraniana, dividir a comunidade internacional na sua oposição à guerra ou suscitar dúvidas quanto às violações do direito internacional pela Rússia. Na Bússola Estratégica, a UE comprometeu-se a dar uma resposta firme à manipulação da informação e ingerência estrangeiras e a reforçar a sua resiliência e capacidade para combater essas ameaças[48]. A manipulação do debate democrático na UE é objeto do Plano de Ação para a Democracia Europeia, o plano coordenado da Comissão para combater a desinformação e reforçar a resiliência democrática[49].

Vigilância e coordenação

A União Europeia respondeu à campanha de desinformação da Rússia no contexto da agressão militar contra a Ucrânia através de uma ação decisiva e coordenada. A UE colaborou estreitamente com os seus Estados-Membros por meio do sistema de alerta rápido e com parceiros internacionais, como a OTAN, os EUA, o Canadá e o mecanismo de resposta rápida do G7, a fim de partilhar informações sobre as tendências e táticas de manipulação utilizadas pelo Kremlin. O trabalho de desconstrução das manipulações do Kremlin intensificou-se, nomeadamente através do sítio Web EUvsDisinfo, que transmite em inglês, russo, ucraniano e outras línguas, a fim de disponibilizar informações factuais na UE, na Ucrânia e na região, bem como na Rússia. Desde 2 de março, suspendeu-se a transmissão e a radiodifusão na UE ou dirigidas à UE dos canais RT e Sputnik dos meios de comunicação social do Estado russo, em consequência das medidas restritivas adotadas pela UE. As plataformas em linha, as principais redes sociais, os anunciantes e os signatários do Código de Conduta sobre Desinformação[50] pertencentes ao setor da publicidade estão a tomar

[48] https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/pt/pdf.
[49] COM(2020) 790.
[50] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

medidas urgentes para limitar a desinformação relacionada com a agressão russa à Ucrânia. A Comissão e o SEAE estão a acompanhar estes esforços. As informações facultadas demonstram que as plataformas reforçaram os seus instrumentos de acompanhamento e intervenção relacionados com a guerra.

Além disso, estão a ser rapidamente implementadas ações para apoiar os países da Ásia Central e dos Balcãs Ocidentais no reforço da resiliência da informação e no combate contra a manipulação da informação e ingerência estrangeiras.

Preparação

A utilização dissimulada de manipulação da informação e ingerência estrangeiras, incluindo a desinformação como um dos instrumentos das ameaças híbridas, implicou uma maior urgência no acompanhamento do Plano de Ação para a Democracia Europeia. Nos últimos meses, as instituições da UE apoiaram os Estados-Membros no combate à manipulação da informação e ingerência estrangeiras, especialmente no âmbito do sistema de alerta rápido, ao partilhar informações sobre as táticas utilizadas pelos agentes de manipulação da informação e ingerência estrangeiras e sobre as estratégias de resposta. Estão em curso debates para reforçar a resposta geral da UE à manipulação da informação e ingerência estrangeiras, com base num documento de síntese apresentado pelo SEAE sobre o desenvolvimento de um **conjunto de instrumentos** específico para fazer face a esta ameaça, o que reúne as medidas internas em vigor e os novos instrumentos da UE no âmbito da Política Externa e de Segurança Comum. Beneficiará igualmente do reforço da ação do Serviço Europeu para a Ação Externa Stratcom[51] e da Comissão.

O Observatório Europeu dos Meios de Comunicação Digitais («EDMO») criou um grupo de trabalho sobre a desinformação na sequência do início da guerra na Ucrânia e coordena as ações dos verificadores de factos e dos investigadores na sua rede. Analisou a forma como os autores de teorias da conspiração sobre a COVID-19 passaram rapidamente à divulgação de embustes pró-russos, uma alteração observada em vários Estados-Membros[52].

A proposta de Regulamento Serviços Digitais procura adaptar-se às tecnologias digitais em rápida evolução e ao que significam para os desafios tecnológicos e democráticos, como o discurso de incitação ao ódio, a desinformação em linha e as estratégias de desestabilização. A consecução de progressos significativos nas negociações pelo Parlamento Europeu e pelo Conselho deverá permitir a rápida adoção do pacote.

VII. PREPARAÇÃO MAIS AMPLA

Numa altura em que a guerra regressou à Europa, bem como num momento de grandes alterações geopolíticas, a coordenação da segurança na UE acelerou, com base em iniciativas já em preparação antes da guerra de agressão da Rússia contra a Ucrânia. As iniciativas que

[51] A comunicação estratégica, os grupos de trabalho e a divisão de análise de informações do Serviço Europeu para a Ação Externa prestam apoio à comunicação estratégica na execução da Política Externa e de Segurança da UE em regiões prioritárias conexas (vizinhança meridional e oriental, Balcãs Ocidentais) através do desenvolvimento e da execução de ações específicas de comunicação estratégica centradas na promoção das políticas, dos valores, dos objetivos e dos interesses da UE.

[52] https://edmo.eu/2022/03/30/how-covid-19-conspiracy-theorists-pivoted-to-pro-russian-hoaxes/.

visam principalmente a segurança externa da UE têm fortes implicações na agenda interna da União da Segurança.

Em 15 de fevereiro de 2022, a Comissão apresentou o **pacote Defesa**[53], com uma série de iniciativas em domínios críticos para a defesa e a segurança na UE. Esta contribuição da Comissão para a defesa e a segurança europeias abrange toda a gama de desafios. Propõe medidas concretas no sentido de um mercado europeu da defesa mais integrado e competitivo, nomeadamente através do reforço da cooperação na UE e da criação de economias de escala. Implica igualmente um roteiro sobre tecnologias críticas para a segurança e a defesa, a fim de impulsionar a investigação, o desenvolvimento tecnológico e a inovação nestes setores, bem como reduzir as dependências nas tecnologias críticas e nas cadeias de valor. O pacote visa igualmente reforçar a dimensão de defesa do espaço a nível da UE. Além disso, analisa a forma como a Comissão poderá intensificar as suas ações contra as ameaças híbridas, nomeadamente no domínio cibernético, reforçar a mobilidade militar dentro e fora da Europa e continuar a dar resposta aos desafios das alterações climáticas relacionados com a defesa. A fim de complementar este trabalho, a Comunicação Conjunta intitulada ***Análise dos défices de investimento na defesa e rumo a seguir***[54], de 18 de maio, tem em consideração as lacunas industriais e em termos de capacidades que têm de ser colmatadas com vista a apoiar os Estados-Membros da UE mais expostos e a identificar medidas para atenuar as insuficiências identificadas.

A resiliência da UE a estas ameaças implica igualmente abordagens orientadas para as capacidades em todos os setores da segurança, conforme defendido no plano de ação da Comissão sobre as sinergias entre as indústrias civis, da defesa e do espaço[55]. Estão em curso trabalhos para promover abordagens orientadas para as capacidades no domínio da segurança interna e da aplicação da lei.

Em 21 de março de 2022, o Conselho adotou a **Bússola Estratégica para a Segurança e a Defesa**[56], aprovada pouco depois pelo Conselho Europeu. A Bússola define um plano de ação ambicioso para reforçar a política de segurança e defesa da UE até 2030. O objetivo consiste em tornar a UE um garante da segurança mais forte e mais capaz, que protege os seus cidadãos e contribui para a paz e a segurança internacionais. Contém propostas concretas, com um calendário de execução muito preciso, a fim de melhorar a capacidade da UE para agir de forma decisiva em situações de crise.

Um dos resultados da Bússola Estratégica consiste no desenvolvimento de um **conjunto de instrumentos da UE contra as ameaças híbridas** que deverá fornecer um enquadramento para uma resposta coordenada às campanhas híbridas que afetam a UE e os seus Estados-Membros, incluindo medidas internas e externas. Na sequência da identificação das bases de referência de resiliência setorial realizada no início de 2022[57], será concluída uma análise das lacunas e necessidades. É neste enquadramento que a UE continuará a desenvolver a preparação, a resiliência e a resposta às ameaças decorrentes da agressão da Rússia e de

[53] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/contributing-european-defence_en.
[54] JOIN(2022) 24.
[55] COM(2021) 70.
[56] Bússola Estratégica para a Segurança e a Defesa – Por uma União Europeia que protege os seus cidadãos, os seus valores e os seus interesses e contribui para a paz e a segurança internacionais, disponível em https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/pt/pdf.
[57] SWD(2022) 21 final.

quaisquer outras tentativas de desestabilização das democracias e da ordem multilateral assente em regras.

VIII. PERSPETIVAS FUTURAS

Numa perspetiva de futuro, a UE terá de permanecer extremamente vigilante face à evolução das ameaças e reforçar **a preparação e a resiliência perante qualquer eventualidade**. As repercussões da guerra podem assumir diferentes formas, que ainda não é possível avaliar.

Ainda se desconhece a extensão da deslocação das redes criminosas ucranianas. Os processos anteriores da Eurojust indicam uma tendência para o tráfico de heroína do Afeganistão para a UE através da Ucrânia, conforme corroborado pelo Observatório Europeu da Droga e da Toxicodependência (OEDT)[58]. A instabilidade pode dificultar a ação contra o tráfico de heroína através desta rota, o que acarreta o risco de um eventual aumento do fluxo de drogas para a UE.

O aumento de alguns riscos para a UE é mais suscetível no final ou durante eventuais pausas nos combates. Será prestada especial atenção à circulação de armas de fogo, com o aumento do risco quando os combates na Ucrânia subsistirem. A experiência anterior aponta igualmente para o risco de que o regresso de combatentes estrangeiros que adquiriram experiência de combate e que possam ter contactado com grupos extremistas possa resultar em ações terroristas na UE numa fase posterior. Este potencial fenómeno deve ser cuidadosamente acompanhado e a Comissão já está a facilitar os debates entre os Estados-Membros sobre os desafios colocados pelo regresso de voluntários estrangeiros com antecedentes extremistas violentos.

Tendo em conta estas eventuais ameaças, é importante que a execução da Estratégia para a União da Segurança prossiga, nomeadamente com a execução de estratégias fundamentais como a Estratégia de Cibersegurança da UE para a Década Digital, a estratégia para lutar contra a criminalidade organizada (2020-2025), a Agenda da UE em matéria de Luta contra o Terrorismo (2020-2025), o Plano de Ação da UE sobre o Tráfico de Armas de Fogo (2020-2025), a Estratégia da UE em matéria de luta contra o tráfico de seres humanos (2021-2025) e a Estratégia da UE em matéria Drogas (2021-2025).

Prosseguirão os esforços para dotar a UE do quadro legislativo necessário. Por exemplo, a Comissão está a elaborar a avaliação de impacto de uma proposta que regulamenta a comercialização e a utilização de substâncias químicas de elevado risco.

[58] *Report on the drug and alcoholic situation in Ukraine for 2020 (according to 2019 data)* (não traduzido para português), OEDT; *Stopping the trafficking of a heroin substitute in France, Poland and Ukraine, including the planning and execution of a controlled delivery* (não traduzido para português), 2021/00446, Eurojust, maio de 2020.

IX. CONCLUSÃO

A União da Segurança continua a desempenhar o seu papel na preparação da UE e dos seus Estados-Membros para combater as ameaças existentes e potenciais. A guerra de agressão da Rússia contra a Ucrânia demonstrou a rapidez com que as ameaças teóricas podem concretizar-se e sublinha a importância da vigilância, da coordenação e da preparação.

Este quarto relatório intercalar sobre a Estratégia para a União da Segurança demonstra que a UE é capaz de se adaptar, mesmo perante ameaças excecionais e inesperadas, como a guerra de agressão da Rússia contra a Ucrânia. A execução determinada da Estratégia para a União da Segurança é mais importante do que nunca.