COMISSÃO
EUROPEIA

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

Bruxelas, 19.7.2017
JOIN(2017) 30 final

RELATÓRIO CONJUNTO AO PARLAMENTO EUROPEU E AO CONSELHO

relativo à aplicação do Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia

1. INTRODUÇÃO

A UE está a enfrentar aquele que é um dos maiores desafios da sua história em matéria de segurança: cada vez mais, as ameaças assumem formas não convencionais, algumas físicas – como as novas formas de terrorismo –, outras que utilizam o espaço digital sob a forma de ciberataques complexos. Outras são mais subtis e visam a aplicação coerciva de pressão, incluindo campanhas de desinformação e a manipulação dos media. Estas ameaças visam minar os principais valores europeus, como a dignidade humana, a liberdade e a democracia. Os recentes ciberataques coordenados em todo o mundo, cuja autoria é difícil de determinar, revelaram as vulnerabilidades das nossas sociedades e instituições.

Em abril de 2016, a Comissão Europeia e a Alta Representante adotaram uma Comunicação conjunta em matéria de luta contra as ameaças híbridas[1] (Quadro comum). Reconhecendo a natureza complexa e transfronteiriça das ameaças híbridas, o quadro propõe uma abordagem de reforço da resiliência global das nossas sociedades que passa por envolver a totalidade das instâncias governativas. O Conselho[2] acolheu favoravelmente a iniciativa e as ações propostas e convidou a Comissão e a Alta Representante a apresentarem um relatório sobre os progressos em julho de 2017. Embora a UE possa ajudar os Estados-Membros a reforçar a sua resiliência contra as ameaças híbridas, a responsabilidade principal cabe aos próprios Estados-Membros, na medida em que a luta contra essas ameaças releva do foro da segurança e da defesa nacionais.

O Quadro comum em matéria de luta contra as ameaças híbridas constitui uma parte importante da abordagem global mais integrada da UE em matéria de segurança e defesa. Contribui para a criação de uma Europa que protege, tal como solicitado pelo Presidente Juncker no seu discurso sobre o Estado da União de setembro de 2016. Em 2016, a União Europeia lançou igualmente as bases para o reforço da política europeia de defesa com o intuito de satisfazer as expectativas dos cidadãos no sentido de um aumento da proteção. A estratégia global da UE para a política externa e de segurança[3] identificou a necessidade de uma abordagem integrada capaz de ligar a resiliência interna às ações externas da UE e preconizou sinergias entre a política de defesa e as políticas relativas ao mercado interno, à indústria, aos serviços policiais e aos serviços de informação. Na sequência da adoção, em novembro de 2016, do Plano de Ação Europeu no Domínio da Defesa, a Comissão apresentou iniciativas concretas destinadas a reforçar a capacidade da UE de dar resposta às ameaças híbridas, através da promoção da resiliência na cadeia de abastecimento da defesa e do reforço do mercado único da defesa. Entre elas destaca-se em especial o lançamento, em 7 de junho de 2017, do Fundo Europeu de Defesa, ao qual a Comissão propõe atribuir um financiamento de 600 milhões de euros até 2020 e de 1,5 mil milhões de euros anualmente após essa data. A Comunicação sobre a União da Segurança[4] reconheceu a necessidade de lutar contra as ameaças híbridas e a importância de assegurar uma maior coerência entre as ações internas e externas no domínio da segurança.

[1] Comunicação conjunta ao Parlamento Europeu e ao Conselho intitulada «Quadro comum em matéria de luta contra as ameaças híbridas — uma resposta da União Europeia», JOIN (2016) 18 final.
[2] «Conclusões do Conselho em matéria de luta contra as ameaças híbridas», Comunicado de Imprensa 196/16, 19 de abril de 2016.
[3] Apresentada pela Alta Representante ao Conselho Europeu em 28 de junho de 2016.
[4] COM(2016) 230 final, de 20.4.2016.

Os líderes da UE colocaram a segurança e a defesa no cerne do debate sobre o futuro da Europa[5]. Tal foi reconhecido na **Declaração de Roma**, de 25 de março de 2017, que definiu uma visão para uma União segura e protegida, empenhada em reforçar a sua segurança e defesa comuns. Os Presidentes do Conselho Europeu e da Comissão Europeia e o Secretário-Geral da NATO, assinaram em Varsóvia, em 8 de julho de 2016, uma Declaração Conjunta UE-NATO, com o objetivo de dar um novo impulso e um novo conteúdo à parceria estratégica UE-NATO. A Declaração Conjunta identificou sete domínios concretos, incluindo a luta contra as ameaças híbridas, em que a cooperação entre as duas organizações deve ser reforçada. Um conjunto comum de 42 propostas de aplicação foi posteriormente aprovado pelos Conselhos da UE e da NATO e um primeiro relatório, registando progressos consideráveis, foi publicado em junho de 2017[6].

O Documento de reflexão da Comissão sobre o futuro da defesa europeia[7], apresentado em junho de 2017, delineia diferentes cenários sobre como resolver as crescentes ameaças enfrentadas pela Europa em matéria de segurança e de defesa e reforçar as suas próprias capacidades de defesa até 2025. Nos três cenários, a segurança e a defesa são consideradas como parte integrante do projeto europeu, de modo a proteger e a promover os nossos interesses a nível interno e externo. A Europa deve tornar-se um garante da segurança e assegurar, progressivamente, a sua própria segurança. Por si só, nenhum Estado-Membro conseguirá enfrentar os desafios futuros, em especial o da luta contra as ameaças híbridas. Por conseguinte, a cooperação em matéria de defesa e segurança não é uma opção; é uma necessidade, para permitir à Europa proteger os seus cidadãos.

O objetivo do presente relatório é apresentar os progressos realizados e descrever as próximas etapas da aplicação das ações nos quatro domínios propostos no Quadro comum: melhorar o conhecimento da situação; reforçar a resiliência; reforçar a capacidade dos Estados-Membros e da União para prevenir e dar resposta às crises e para recuperar de forma coordenada; e reforçar a cooperação com a NATO a fim de assegurar a complementaridade das medidas. O relatório deve ser lido em conjunto com os relatórios mensais sobre os progressos alcançados na criação de uma União da Segurança genuína e eficaz.

2. RECONHECER O CARÁTER HÍBRIDO DE UMA AMEAÇA

As atividades de caráter híbrido estão a tornar-se cada vez mais frequentes no contexto da segurança europeia. A intensidade destas atividades está a aumentar, suscitando uma crescente preocupação com a possível interferência em atos eleitorais, com campanhas de desinformação, ciberatividades maliciosas e autores de atos híbridos que tentam radicalizar os membros mais vulneráveis da sociedade, convencendo-os a tornarem-se intervenientes por interposição. As vulnerabilidades às ameaças híbridas não estão limitadas às fronteiras nacionais; esse tipo de ameaças requer uma resposta coordenada também a nível da UE e da NATO. Os acontecimentos desde abril de 2016 revelam que, apesar de as ameaças serem ainda, muitas vezes, avaliadas isoladamente, existe um reconhecimento e uma compreensão

[5] Roteiro de Bratislava do Conselho Europeu, de 16 de setembro de 2016, e Declaração de Roma, assinada pelos dirigentes de 27 Estados-Membros e do Conselho Europeu, do Parlamento Europeu e da Comissão Europeia, de 25 de março de 2017.

[6] http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation

[7] Documento de reflexão sobre o futuro da defesa europeia, de 7.6.2017, https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_pt.pdf

crescentes na União quanto ao caráter híbrido de algumas das atividades observadas e à necessidade de uma ação coordenada. A UE continuará a envidar esforços para melhorar o conhecimento da situação e a cooperação.

<u>Ação 1</u>: Os Estados-Membros, com o apoio da Comissão e, eventualmente, da Alta Representante, são convidados a lançar um estudo sobre os riscos híbridos, a fim de identificar as principais vulnerabilidades, incluindo indicadores específicos ligados às ameaças híbridas, suscetíveis de afetar as estruturas e as redes nacionais e pan-europeias.

O Conselho criou um «grupo de amigos da Presidência» composto por peritos dos Estados-Membros cuja missão consiste em elaborar um estudo genérico que permita identificar melhor os principais indicadores de ameaças híbridas, integrá-los nos mecanismos existentes de alerta precoce e de avaliação dos riscos e, se for caso disso, partilhar esses indicadores. O mandato foi aprovado e os trabalhos já tiveram início. O estudo genérico deverá estar pronto até ao final de 2017, devendo os estudos dos Estados-Membros ter início em seguida. A proteção contra as ameaças híbridas deve contribuir para o reforço mútuo. Por conseguinte, os Estados-Membros são incentivados a realizar esses estudos o mais rapidamente possível, uma vez que os mesmos permitirão obter informações preciosas sobre o grau de vulnerabilidade em todos os países da UE.

a. MELHORAR O CONHECIMENTO DA SITUAÇÃO

A partilha dos trabalhos de análise e avaliação da informação é fundamental para reduzir a incerteza e reforçar o conhecimento da situação. Durante o ano passado foram feitos progressos significativos. Foi criada a Célula de Fusão da UE contra as ameaças híbridas, que está agora plenamente operacional; a *task force* «East Stratcom» está instituída e a Finlândia abriu o Centro Europeu para a Luta contra as Ameaças Híbridas. Uma parte significativa dos trabalhos centrou-se na análise das ferramentas e «alavancas» de desinformação ou propaganda, tendo-se verificado uma boa cooperação entre a *task force* «East Stratcom», a Célula de Fusão da UE contra as ameaças híbridas e a NATO. Existe assim uma boa base para reforçar a cultura de análise e avaliação das ameaças à nossa segurança interna e externa através de uma perspetiva híbrida.

<u>Célula de Fusão contra as ameaças híbridas</u>

<u>Ação 2</u>: Criação de uma Célula de Fusão da UE contra as ameaças híbridas no âmbito da estrutura existente do Centro de Análise de Informações da UE, capaz de receber e analisar informações sobre ameaças híbridas, tanto classificadas como provenientes de fontes abertas. Os Estados-Membros são convidados a criar pontos de contacto nacionais em matéria de ameaças híbridas para assegurar a cooperação e uma comunicação segura com a Célula de Fusão da UE contra as ameaças híbridas.

Esta célula foi criada no seio do Centro de Análise de Informações da UE para receber e analisar informações sobre ameaças híbridas, tanto classificadas como de fontes abertas, provenientes de diferentes partes interessadas. A análise é, em seguida, partilhada na UE e entre os Estados-Membros e em seguida integrada nos processos de tomada de decisões da UE, fornecendo inclusivamente elementos a integrar nas avaliações dos riscos para a segurança realizadas à escala da UE. A Direção de Informações do Estado-Maior da UE contribui para o trabalho da Célula de Fusão com análises militares. Até à data, foram realizadas mais de 50 avaliações e sessões de informação (*briefings*) sobre temas relacionados com as ameaças híbridas. Desde janeiro de 2017, a célula edita periodicamente o *Hybrid*

Bulletin (boletim de ameaças híbridas), que analisa as ameaças e questões híbridas atuais e é diretamente distribuído às instituições e órgãos da UE e aos pontos de contacto nacionais[8]. A capacidade operacional plena da célula foi alcançada, conforme previsto, em maio de 2017. Por último, o pessoal da célula mantém-se em estreito contato com o da recém-criada Célula de Análise de Ameaças Híbridas da NATO, partilhando quer os ensinamentos retirados da criação da Célula de Fusão quer informações (no pleno respeito das regras da UE relativas ao intercâmbio de informações classificadas). A Célula de Fusão da UE contra as ameaças híbridas está atualmente a identificar novas iniciativas para melhorar a cooperação futura e irá desempenhar um papel fundamental nos exercícios paralelos UE-NATO previstos para o outono de 2017, em que a capacidade de resposta da célula será testada e os ensinamentos adquiridos serão integrados.

Comunicação estratégica

Ação 3: A Alta Representante irá estudar com os Estados-Membros as formas de atualizar e coordenar as capacidades em matéria de fornecimento de comunicações estratégicas proativas e de otimização do recurso a especialistas em monitorização dos media e em linguística.

Nos últimos meses, o aumento das campanhas de desinformação e a divulgação sistemática de notícias falsas (*fake news*) nas redes sociais foram algumas das formas utilizadas para prejudicar os adversários. Nos casos em que as redes sociais são a plataforma preferencial, informações aparentemente fiáveis e legítimas podem influenciar a opinião pública em benefício de alguns indivíduos, organizações ou governos. Estas táticas híbridas têm o objetivo mais vasto de semear a confusão nas nossas sociedades e de desacreditar os governos democráticos e as nossas estruturas, instituições e eleições. As notícias falsas são, muitas vezes, divulgadas através de plataformas em linha (ver também a ação 17). A Comissão e a Alta Representante congratulam-se com as recentes medidas tomadas por plataformas em linha e pelos editores de alguns media noticiosos para combater a desinformação. A Comissão continuará a encorajar estas medidas voluntárias.

A Alta Representante criou a *task force* «East Stratcom» que prevê e responde aos casos e às campanhas de desinformação. Melhorou-se assim significativamente a comunicação sobre as políticas da União nos países da Vizinhança Oriental e, ao mesmo tempo, reforçou-se o ambiente mediático nesses países. Nos últimos dois anos, a *task force* detetou mais de 3 000 casos de desinformação em 18 línguas. O lançamento iminente de um novo sítio Web, intitulado «*# EUvsdisinformation*», que integra uma função de pesquisa em linha, permitirá melhorar significativamente o acesso dos utilizadores. No entanto, os trabalhos de investigação e análise revelam que o número de canais de desinformação e de mensagens propagadas quotidianamente é significativamente mais elevado. O projeto EU-STRAT, financiado pelo Horizonte 2020, analisa as políticas e os media nos países da Parceria Oriental.

A Alta Representante convida os Estados-Membros a apoiar o trabalho das *task forces* StratCom, a fim de combater mais eficazmente o surgimento de ameaças híbridas. Isto irá ajudar a *Task Force* Sul a melhorar a comunicação e a sensibilização do mundo árabe, incluindo em língua árabe, a desfazer mitos e a repor a verdade sobre União Europeia e as suas políticas. A interação com os jornalistas locais contribuirá para garantir que os produtos noticiosos estão

[8] Até à data, 21 Estados-Membros nomearam pontos de contacto nacionais. Trata-se de indivíduos que trabalham nas capitais dos Estados-Membros numa função política/ligada à resiliência.

em sintonia cultural. Ambas as *task forces*, apoiadas pela Célula de Fusão da UE contra as ameaças híbridas, destinam-se a apoiar e complementar os esforços dos Estados-Membros na matéria. Além disso, a Comissão cofinancia a Rede Europeia de Comunicações Estratégicas, uma rede de cooperação de 26 Estados-Membros que partilha análises, boas práticas e ideias sobre a utilização de comunicações estratégicas na luta contra o extremismo violento, inclusivamente no que diz respeito à desinformação.

Centro de excelência para a «luta contra as ameaças híbridas»

***Ação 4:* Os Estados-Membros são convidados a ponderar a criação de um centro de excelência para a «luta contra as ameaças híbridas».**

Em resposta ao apelo para criar um centro de excelência, em abril de 2017, a Finlândia lançou o Centro Europeu para a Luta contra as Ameaças Híbridas. Dez Estados-Membros da UE[9] e os EUA são membros, tendo a União Europeia e a NATO sido convidadas a apoiar o conselho diretivo[10]. A missão do Centro consiste em incentivar o diálogo estratégico e em realizar atividades de investigação e análise, em colaboração com as comunidades de interesse, para melhorar a resiliência e a capacidade de resposta, com vista a lutar contra as ameaças híbridas. Espera-se que o Centro sirva também de local para a realização de futuros exercícios relacionados com as ameaças híbridas. O Centro mantém já um contacto estreito com a Célula de Fusão da UE contra as ameaças híbridas; os trabalhos das duas organizações deverão complementar-se mutuamente. A UE está atualmente a avaliar de que forma pode prestar apoio concreto ao Centro.

b. REFORÇAR A RESILIÊNCIA

O Quadro comum coloca a resiliência (por exemplo, nos transportes, nas comunicações, na energia, nas finanças ou nas infraestruturas de segurança regionais) no centro da ação da UE com o objetivo de resistir às campanhas de propaganda e desinformação e às tentativas de prejudicar as empresas, as sociedades e os fluxos económicos, bem como aos ataques às infraestruturas das tecnologias da informação e do ciberespaço. O reforço da resiliência é considerado como uma ação de prevenção e dissuasão para tornar as sociedades mais fortes e evitar a escalada de crises, tanto dentro como fora da UE. O valor acrescentado da UE reside na capacidade de ajudar os Estados-Membros e os parceiros a reforçar a sua resiliência, com base numa ampla gama de instrumentos e programas existentes. Foram feitos progressos significativos nas ações destinadas a aumentar a resiliência em domínios como a cibersegurança, as infraestruturas críticas, a proteção do sistema financeiro contra as utilizações ilícitas e a luta contra o extremismo violento e a radicalização.

Proteção das infraestruturas críticas

Ação 5: A Comissão, em cooperação com os Estados-Membros e as partes interessadas, irá identificar instrumentos comuns, nomeadamente indicadores, com vista a aumentar a proteção e a resiliência das infraestruturas críticas contra as ameaças híbridas nos setores relevantes.

No contexto do Programa Europeu de Proteção das Infraestruturas Críticas (EPCIP), a Comissão prosseguiu os trabalhos destinados a identificar instrumentos comuns, incluindo

[9] Finlândia, França, Alemanha, Letónia, Lituânia, Polónia, Suécia, Reino Unido, Estónia e Espanha.
[10] O Centro está aberto à participação dos outros Estados-Membros da UE e dos aliados membros da NATO.

indicadores de vulnerabilidade, com vista a melhorar a resiliência das infraestruturas críticas contra as ameaças híbridas nos setores relevantes. Em maio de 2017, a Comissão organizou um seminário sobre as ameaças híbridas a infraestruturas críticas, que contou com a participação de quase todos os Estados-Membros, de operadores de infraestruturas críticas, da Célula de Fusão da UE contra as ameaças híbridas e da NATO na qualidade de observador. Foram acordados um roteiro comum e as etapas para os trabalhos futuros, com base num questionário enviado às autoridades nacionais dos Estados-Membros. A Comissão consultará novamente as partes interessadas no outono, com o objetivo de adotar indicadores até ao final de 2017.

A Agência Europeia de Defesa (AED) está a trabalhar para identificar as lacunas comuns em termos de capacidades e investigação decorrentes do nexo de causalidade ente as infraestruturas energéticas e as capacidades de defesa. No outono de 2017, a Agência irá elaborar um documento conceptual e desenvolver ações-piloto para a implementação de metodologias holísticas.

Aumentar a segurança do aprovisionamento energético da UE

Ação 6: A Comissão, em cooperação com os Estados-Membros, irá apoiar os esforços no sentido de diversificar as fontes de energia e promover normas de segurança e proteção para aumentar a resiliência das infraestruturas nucleares.

A Comissão apresentou propostas concretas no âmbito do pacote sobre a segurança do aprovisionamento em dezembro de 2016 e, em abril de 2017, o Conselho e o Parlamento Europeu chegaram a acordo quanto ao novo regulamento relativo à segurança do aprovisionamento de gás, que visa evitar as crises de aprovisionamento. As novas regras garantirão que os Estados-Membros adotam uma abordagem comum e coordenada a nível regional no que diz respeito às medidas de segurança do aprovisionamento, o que colocará a UE em melhor posição para se preparar para as falhas no abastecimento de gás e para gerir essas falhas em caso de crise ou ataque híbrido. Pela primeira vez, será aplicado o princípio da solidariedade: os Estados-Membros poderão ajudar os países vizinhos em caso de crise ou ataque grave, de forma a que as famílias e empresas europeias não sofram cortes totais de gás.

A UE alcançou igualmente progressos no desenvolvimento de projetos importantes para diversificar as suas rotas e fontes de aprovisionamento de energia, em conformidade com a Estratégia-quadro para a União da Energia e com a Estratégia Europeia de Segurança Energética. Por exemplo, no Corredor Meridional de Gás estão em curso obras de construção concretas em todos os principais projetos de gasodutos: a expansão do gasoduto do Cáucaso do Sul, do gasoduto transanatoliano e do gasoduto transadriático, os trabalhos do consórcio Shah Deniz II, a montante, e a expansão do Corredor Meridional de Gás até à Ásia Central, nomeadamente até ao Turquemenistão. As importações de gás natural liquefeito (GNL) na Europa estão a aumentar, sendo provenientes de novas fontes como, por exemplo, os EUA. O exemplo do terminal na Lituânia mostra como os projetos de diversificação podem reduzir a dependência de um único fornecedor. O incremento dos esforços em matéria de energia e a melhor utilização de fontes de energia endógenas, em especial as renováveis, contribuem também para a diversificação das rotas e das fontes de energia.

No domínio da segurança nuclear, a Comissão apoia ativamente — em particular através da realização de seminários com autoridades e reguladores nacionais — uma aplicação coerente e eficaz da diretiva relativas à segurança nuclear e da diretiva relativa às normas de segurança

de base, que os Estados-Membros são obrigados a transpor até ao final de 2017 e 2018, respetivamente. Além disso, o Programa Euratom de Investigação e Formação contribui para reforçar a segurança nuclear.

Transportes e segurança da cadeia de abastecimento

Ação 7: A Comissão irá acompanhar as ameaças emergentes em todo o setor dos transportes e atualizar a legislação, sempre que adequado. Na execução da estratégia de segurança marítima da UE e da estratégia da UE sobre gestão dos riscos aduaneiros e respetivos planos de ação, a Comissão e a Alta Representante (no âmbito das respetivas competências), em coordenação com os Estados-Membros, irão analisar de que modo se pode dar resposta às ameaças híbridas, em especial no domínio das infraestruturas críticas dos transportes.

Em conformidade com a Comunicação sobre a União da Segurança, a Comissão está a apoiar a realização de avaliações dos riscos para a segurança a nível da UE com os Estados-Membros, o Centro de Análise de Informações da UE e as agências pertinentes, a fim de identificar ameaças à segurança dos transportes e apoiar o desenvolvimento de medidas de atenuação eficazes e proporcionais. A queda do voo MH17 da Malaysia Airlines no Leste da Ucrânia em 2014 evidenciou o risco decorrente do sobrevoo de zonas de conflito. Em conformidade com as recomendações da *task force* europeia de alto nível sobre as zonas de conflito[11], a Comissão desenvolveu uma metodologia para a «avaliação conjunta dos riscos à escala da UE» com o apoio de peritos nacionais em segurança e aviação e do SEAE, permitindo o intercâmbio de informações classificadas e a definição de um quadro comum dos riscos. Em março de 2017, a Agência Europeia para a Segurança da Aviação (AESA) publicou o primeiro «Boletim de Informação sobre Zonas de Conflito»[12] com base nos resultados desta avaliação conjunta dos riscos à escala da UE. A Comissão está a ponderar alargar as atividades de avaliação dos riscos realizadas no domínio da segurança da aviação a outros modos de transporte (por exemplo, ferroviário, marítimo); as propostas serão apresentadas em 2018. Em junho de 2017, a Comissão, o SEAE e os Estados-Membros lançaram um exercício de avaliação dos riscos em matéria de segurança ferroviária para identificar lacunas e possíveis medidas suscetíveis de atenuar esses riscos.

Foram igualmente envidados esforços consideráveis no domínio da segurança da aviação e da gestão do tráfego aéreo em projetos de investigação sobre a segurança realizados no âmbito do 7.º Programa-Quadro e do Horizonte 2020. No domínio da aviação civil, a Comissão, juntamente com a Agência Europeia para a Segurança da Aviação e as partes interessadas, está a preparar duas novas iniciativas para reforçar a cibersegurança, que também visam lutar contra as ameaças híbridas: a criação da equipa de resposta a emergências informáticas no domínio da aviação e a criação de uma *task force* para a cibersegurança na Empresa Comum SESAR, responsável pela gestão do tráfego aéreo no Céu Único Europeu. A Agência Europeia de Defesa presta contributos militares no domínio da cibersegurança na aviação à Empresa Comum SESAR, bem como à Agência Europeia para a Segurança da Aviação através da «Plataforma Europeia de Coordenação Estratégica para a Cibersegurança» que, a pedido dos Estados-Membros e da indústria, irá ajudar na coordenação, à escala da UE, de todas as atividades no domínio da aviação. Em conformidade com o Roteiro relativo à cibersegurança no domínio da aviação, a Agência Europeia para a Segurança da Aviação

[11] https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf

[12] https://ad.easa.europa.eu/czib-docs/page-1

analisou, em 2016, as lacunas nas regras existentes e dedicou-se, nomeadamente, à definição e criação do Centro Europeu para a Cibersegurança no Domínio da Aviação; este último está agora operacional e coopera com a equipa de resposta a emergências informáticas da UE (CERT-UE) (o memorando de entendimento foi assinado em fevereiro de 2017), produzindo análises de ameaças no domínio da aviação, e com o EUROCONTROL (foi adotado um roteiro para a cooperação), tendo sido criado um sítio Web para a distribuição de análises de fontes abertas. Até ao outono de 2017, serão adotados um programa de normalização e um intercâmbio de informações seguro.

Gestão dos riscos aduaneiros

Do ponto de vista aduaneiro, a Comissão está a levar a cabo uma modernização considerável do sistema de informação antecipada sobre as mercadorias e de gestão dos riscos aduaneiros. Este sistema abrange todo conjunto de riscos aduaneiros, incluindo no que diz respeito às ameaças à segurança e à integridade das cadeias de abastecimento internacionais, bem como às infraestruturas críticas relevantes (por exemplo, as importações constituem ameaças diretas para as instalações portuárias marítimas, os aeroportos ou as fronteiras terrestres). A modernização do sistema tem como objetivo assegurar que as autoridades aduaneiras da UE obtêm dos comerciantes todas as informações necessárias no que se refere à circulação de mercadorias; podem partilhar essas informações de forma mais eficaz entre os Estados-Membros; aplicam disposições comuns, bem como as regras em matéria de riscos específicas de cada Estado-Membro; e são capazes de detetar mais eficazmente as remessas de alto risco através de uma cooperação mais intensa com outras autoridades, nomeadamente outros serviços policiais e agências de segurança. O desenvolvimento dos sistemas informáticos necessários à Comissão para implementar esta modernização está atualmente na sua fase inicial, estando previsto para os próximos meses o lançamento dos investimentos relevantes a nível central.

Espaço

Ação 8: **No contexto da Estratégia Espacial e do Plano de Ação Europeu no Domínio da Defesa, a Comissão irá propor a melhoria da resiliência das infraestruturas espaciais contra ameaças híbridas, nomeadamente através de um eventual alargamento do âmbito do Quadro de Apoio à Vigilância e ao Rastreio de Objetos no Espaço para cobrir as ameaças híbridas, da preparação da próxima geração de telecomunicações governamentais por satélite a nível europeu e da introdução do Galileo nas infraestruturas críticas dependentes da sincronização temporal.**

Na preparação, em 2018, do quadro regulamentar sobre telecomunicações governamentais por satélite (GovSatCom) e sobre a vigilância e o rastreio de objetos no espaço, a Comissão integrará na sua avaliação aspetos da resiliência contra as ameaças híbridas. Em conformidade com a Estratégia Espacial, na preparação da evolução do Galileo e do Copernicus a Comissão avaliará o potencial destes serviços para ajudar a reduzir a vulnerabilidade das infraestruturas críticas. O relatório de avaliação deverá estar pronto no outono de 2017 e a proposta relativa à próxima geração do Copernicus e do Galileo em 2018. A Agência Europeia de Defesa está a trabalhar em projetos colaborativos de desenvolvimento das capacidades nos domínios das comunicações espaciais, do posicionamento militar, da navegação e cronometria, bem como da observação da Terra. Todos os projetos incidirão nos requisitos de resiliência à luz das ameaças híbridas atuais e emergentes.

Capacidades de defesa

<u>Ação 9</u>: A Alta Representante, eventualmente com o apoio dos Estados-Membros, irá ,em articulação com a Comissão, apresentará propostas de adaptação das capacidades de defesa e desenvolvimento com interesse para a UE, com o intuito específico de fazer face às ameaças híbridas contra um ou vários Estados-Membros.

Em 2016 e 2017, a Agência Europeia de Defesa realizou, juntamente com a Comissão, o SEAE e peritos dos Estados-Membros, três exercícios teóricos baseados em cenários de ameaças híbridas. As conclusões destes exercícios serão tidas em conta na revisão do plano de desenvolvimento de capacidades, para que os desenvolvimentos das principais capacidades necessárias para lutar contra as ameaças híbridas sejam integrados nas novas prioridades da UE nesta matéria. Os trabalhos de revisão do catálogo de necessidades de 2005 terão em conta a dimensão das ameaças híbridas. Em abril de 2017, a Agência Europeia de Defesa concluiu um relatório de análise sobre as implicações militares decorrentes de ataques híbridos contra as infraestruturas portuárias críticas, as quais serão discutidas num seminário com peritos em assuntos marítimos em outubro de 2017. Uma outra análise específica do papel militar no contexto da luta contra os minidrones está prevista para 2018. Além disso, as prioridades em matéria de capacidades para reforçar a resiliência contra as ameaças híbridas identificadas pelos Estados-Membros também poderão ser elegíveis para apoio ao abrigo do Fundo Europeu de Defesa a partir de 2019. A Comissão apela aos colegisladores para que garantam uma adoção rápida e aos Estados-Membros para que apresentem propostas de projetos de capacidade destinados a reforçar a resiliência da UE contra as ameaças híbridas.

<u>Ação 10</u>: A Comissão, em cooperação com os Estados-Membros, irá melhorar o conhecimento da situação e a resiliência perante ameaças híbridas no âmbito dos mecanismos de preparação e de coordenação existentes, nomeadamente o Comité de Segurança da Saúde.

Com o objetivo de reforçar a preparação e a resiliência contra as ameaças híbridas, incluindo o reforço das capacidades dos sistemas de saúde e alimentares, a Comissão apoia os Estados-Membros através de ações de formação e exercícios de simulação, bem como facilitando o intercâmbio de experiências e financiando ações conjuntas. Estas atividades de apoio têm lugar, designadamente, ao abrigo do quadro de segurança da saúde da UE relativo a ameaças sanitárias transfronteiriças graves e ao abrigo do programa de saúde pública para aplicar o Regulamento Sanitário Internacional, um pilar legislativo que vincula 196 países, incluindo os Estados-Membros, e visa prevenir e responder a riscos para a saúde transfronteiriços e públicos graves a nível mundial. Para testar a preparação e a resposta intersetoriais no setor da saúde, os serviços da Comissão irão realizar um exercício sobre ameaças híbridas complexas e multidimensionais no outono de 2017. A Comissão e os Estados-Membros estão a preparar uma ação conjunta em matéria de vacinação, que incluirá previsões relativas à oferta e procura de vacinas e investigação sobre processos inovadores de fabrico de vacinas, com o objetivo de reforçar o fornecimento de vacinas e melhorar a segurança da saúde a nível da UE (2018-2020). Além disso, a Comissão colabora com a Autoridade Europeia para a Segurança dos Alimentos e com o Centro Europeu de Prevenção e Controlo das Doenças para se adaptar a técnicas de investigação científicas avançadas, com vista a poder identificar de forma mais precisa as fontes de ameaças para a saúde e, consequentemente, gerir rapidamente os surtos de doenças no domínio da segurança alimentar. A Comissão estabeleceu uma rede de financiadores da investigação – a iniciativa de colaboração mundial em investigação para a prevenção de doenças infeciosas – para, no prazo máximo de 48 horas, dar uma resposta coordenada (em termos de investigação) a qualquer surto significativo.

<u>Ação 11</u>: A Comissão incentiva os Estados-Membros a criar e a explorar plenamente, com caráter prioritário, uma rede que agrupe as 28 CSIRT (equipas de resposta a incidentes de segurança informática) e a CERT-UE (equipas de resposta a emergências informáticas para as instituições, órgãos e organismos da UE), bem como um quadro para a cooperação estratégica. A Comissão, em colaboração com os Estados-Membros, terá de assegurar que as iniciativas setoriais em matéria de ciberameaças (por exemplo, nos setores da aviação, da energia e marítimo) são coerentes com as capacidades intersetoriais cobertas pela Diretiva SRI, de modo a congregar informações, conhecimentos especializados e respostas rápidas.

Os recentes ciberataques mundiais através de *ransomware* (*software* de sequestro) e *malware* (*software* mal intencionado) para desativar milhares de sistemas informáticos salientaram a necessidade urgente de reforçar a ciber-resiliência e as ações em matéria de segurança na UE. Tal como anunciado na revisão intercalar do Mercado Único Digital, a Comissão e a Alta Representante estão agora a rever a Estratégia da UE para a Cibersegurança de 2013, nomeadamente com a adoção de um pacote previsto para setembro de 2017. O objetivo será dar uma resposta transetorial mais eficaz a estas ameaças, o que aumentará a confiança na sociedade digital e na economia. Além disso, será também revisto o mandato da ENISA, a Agência da UE para a Segurança das Redes e da Informação, com o objetivo de definir o papel desta agência no ecossistema em mutação da cibersegurança. O Conselho Europeu[13] acolheu com agrado a intenção da Comissão de rever a Estratégia para a Cibersegurança.

A adoção da Diretiva «Segurança das Redes e da Informação» (SRI)[14] em julho de 2016 constituiu um passo importante para o reforço da resiliência da cibersegurança a nível europeu. A diretiva estabelece as primeiras regras a nível da UE em matéria de cibersegurança, melhora as capacidades de cibersegurança e reforça a cooperação entre os Estados-Membros. Além disso, exige que as empresas de setores críticos tomem as medidas de segurança adequadas e notifiquem quaisquer incidentes cibernéticos graves à autoridade nacional competente. Esses setores incluem a energia, os transportes, a água, a saúde, a banca e as infraestruturas do mercado financeiro. Os mercados em linha, os serviços de computação em nuvem e os motores de pesquisa terão de tomar medidas semelhantes. A aplicação coerente nos diferentes setores e além-fronteiras será assegurada pelo grupo de cooperação para a segurança das redes e dos sistemas de informação (criado pela Comissão em 2016), que tem por missão evitar a fragmentação do mercado. Neste contexto, a Diretiva SRI é considerada o quadro de referência para quaisquer iniciativas setoriais no domínio da cibersegurança. Além disso, a diretiva cria a rede de equipas de resposta a incidentes de segurança informática (CSIRT), que reúne todas as partes interessadas relevantes. Paralelamente, a Comissão e a CERT-UE monitorizam ativamente o contexto das ameaças cibernéticas e procedem ao intercâmbio de informações com as autoridades nacionais, de forma a garantir que os sistemas de tecnologias da informação das instituições da UE são seguros e resilientes a ataques informáticos. O incidente de *ransomware* WannaCry, em maio de 2017, constituiu a primeira oportunidade para levar a cabo, no seio da rede, um intercâmbio de informações operacionais e atividades de cooperação mediante a divulgação de conselhos. A equipa de resposta a emergências informáticas da UE manteve-se também em estreito contacto com o Centro Europeu da Cibercriminalidade (EC3) da Interpol, com as equipas de resposta a incidentes de segurança informática (CSIRT) dos países afetados, com unidades de cibercriminalidade e com parceiros importantes do setor, a fim de reduzir a

[13] Conclusões do Conselho Europeu de 22-23 de junho de 2017.

[14] Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, JO L 194 de 19.7.2016, p. 1.

ameaça e prestar assistência às vítimas. A troca de relatórios de situação nacionais permitiu um conhecimento comum das situações em toda a UE. Esta experiência possibilitou que a rede estivesse mais bem preparada para os incidentes que se seguiram (por exemplo, "NonPetya"). Além disso, foram identificados vários problemas, cuja resolução está a ser estudada.

<u>Ação 12</u>: A Comissão, em coordenação com os Estados-Membros, irá colaborar com a indústria no âmbito de uma parceria público-privada contratual para a cibersegurança, com vista a desenvolver e testar tecnologias destinadas a proteger melhor os utilizadores e as infraestruturas contra os aspetos informáticos das ameaças híbridas.

Em julho de 2016, a Comissão, em coordenação com os Estados-Membros, assinou com a indústria uma Parceria Público-Privada contratual (PPPc) para a cibersegurança, tendo disponibilizado 450 milhões de euros ao abrigo do programa de investigação e inovação da UE Horizonte 2020, com o objetivo de desenvolver e testar tecnologias destinadas a melhor proteger os utilizadores e as infraestruturas contra ciberameaças e ameaças híbridas. A parceria produziu a primeira agenda de investigação estratégica pan-europeia, que visa, em especial, reforçar a resiliência das infraestruturas críticas e dos cidadãos contra os ciberataques. Além disso, reforçou a coordenação entre as partes interessadas, permitindo ganhos de eficiência e eficácia no financiamento da cibersegurança ao abrigo do Horizonte 2020. Paralelamente, a parceria está a trabalhar em questões relacionadas com a certificação das tecnologias da informação e comunicação para a cibersegurança, tentando igualmente encontrar formas de combater a escassez aguda de profissionais qualificados em matéria de cibersegurança no mercado. Tendo em conta as importantes necessidades da investigação civil e a elevada resiliência exigida no setor da defesa, o grupo de tecnologia e investigação cibernética da Agência Europeia de Defesa está a contribuir para os domínios de investigação identificados na agenda de investigação e inovação estratégica da Organização Europeia de Cibersegurança.

<u>Ação 13</u>: A Comissão irá publicar orientações destinadas aos proprietários de redes inteligentes para melhorar a cibersegurança das suas instalações. No contexto da iniciativa relativa à conceção do mercado da eletricidade, a Comissão ponderará propor «planos de preparação para os riscos» e regras de procedimento para a partilha de informações e para assegurar a solidariedade entre os Estados-Membros em situações de crise, incluindo regras relativas à forma de prevenir e reduzir os ciberataques.

No setor da energia, a Comissão está a preparar uma estratégia setorial relativa à cibersegurança com a criação de uma «Energy Expert Cybersecurity Platform» (plataforma de peritos em energia para a cibersegurança) para reforçar a aplicação da Diretiva SRI. Um estudo realizado em fevereiro de 2017 identificou as melhores técnicas disponíveis para reforçar o nível de cibersegurança dos contadores inteligentes, em apoio desta plataforma. Além disso, a Comissão criou uma plataforma na Internet, «*Incident and Threat Information Sharing EU Centre*», que analisa e partilha informações relativas a ciberameaças e incidentes cibernéticos no setor da energia.

<u>Reforçar a resiliência contra as ameaças híbridas do setor financeiro</u>

<u>Ação 14</u>: A Comissão, em cooperação com a ENISA[15], os Estados-Membros, as autoridades nacionais, europeias e internacionais competentes e as instituições financeiras, irá promover e facilitar a criação de plataformas e redes de partilha de informações sobre ameaças e estudará os fatores que dificultam o intercâmbio de tais informações.

Reconhecendo que as ciberameaças estão entre os principais riscos para a estabilidade financeira, a Comissão procedeu à revisão do quadro regulamentar em matéria de serviços de pagamento na União Europeia, que deverá agora ser implementado. A Diretiva relativa aos serviços de pagamento revista[16] introduziu novas disposições para reforçar a segurança dos instrumentos de pagamento e a autenticação forte do cliente, com o objetivo de reduzir a fraude, em especial nos pagamentos em linha. O novo quadro legislativo será aplicável a partir de janeiro de 2018. Atualmente, a Comissão, assistida pela Autoridade Bancária Europeia e em consulta com as partes interessadas, está a elaborar normas técnicas de regulamentação, que deverão ser publicadas até ao final de 2017, relativas à autenticação forte do cliente e à comunicação comum securizada para tornar operacional a segurança nas operações de pagamento. Além disso, no plano internacional, a Comissão trabalhou em estreita cooperação com os parceiros do G7 na elaboração dos «Princípios fundamentais do G7 para a cibersegurança no setor financeiro», aprovados em outubro de 2016 pelos ministros das Finanças e pelos governadores dos bancos centrais do G7. Estes princípios destinam-se a entidades do setor financeiro (privadas e públicas) e contribuem para uma abordagem coordenada no domínio da cibersegurança no setor financeiro, visando encontrar soluções comuns contra as ciberameaças, em particular a sua multiplicação e crescente sofisticação.

<u>Transportes</u>

<u>Ação 15</u>: A Comissão e a Alta Representante (no âmbito das respetivas áreas de competência), em coordenação com os Estados-Membros, irão examinar a resposta a dar às ameaças híbridas, nomeadamente as relacionadas com ciberataques no setor dos transportes.

A aplicação do Plano de Ação relativo à Estratégia de Segurança Marítima da UE[17] ajudará a combater a mentalidade de circuito fechado no que diz respeito ao intercâmbio de informações e à utilização partilhada dos recursos entre as autoridades civis e militares. A adoção da abordagem envolvendo a totalidade das instâncias governativas resultou numa maior cooperação entre os vários intervenientes. Prevê-se a conclusão da agenda estratégica conjunta da Comissão e do SEAE em matéria de investigação civil e militar até ao final de 2017, com um seminário final sobre a proteção das infraestruturas marítimas críticas. Estes trabalhos poderão, no futuro, ser alargados para passarem a proteger as condutas submarinas, as transferências de energia e os cabos de comunicação (quer de fibra ótica quer tradicionais) das ameaças emergentes representadas pelas interferências fora das águas nacionais.

[15] Agência da União Europeia para a Segurança das Redes e da Informação.
[16] Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno, JO L 337 de 23.12.2015, p. 35.
[17] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf e 2.º relatório sobre a aplicação do Plano de Ação relativo à Estratégia de Segurança Marítima da União Europeia (ESM-UE) apresentado aos Estados-Membros em 21 de junho de 2017.

Um estudo recente[18] examinou a capacidade de avaliação dos riscos das autoridades nacionais que desempenham funções de guarda costeira. O estudo identificou os obstáculos mais importantes à colaboração e recomendou formas práticas de reforçar a cooperação entre as autoridades marítimas, à escala nacional e à escala da UE, neste domínio específico. A avaliação dos riscos é essencial na luta contra as ameaças marítimas e mais importante ainda para a avaliação e a prevenção das ameaças híbridas, uma vez que estas requerem considerações adicionais e mais complexas. Os resultados deste estudo serão apresentados em diferentes fóruns de guardas costeiras, para que as recomendações propostas possam ser avaliadas e aplicadas a fim de reforçar a cooperação neste domínio, tendo a preparação e a capacidade de resposta a ameaças híbridas como principais objetivos.

Luta contra o financiamento do terrorismo

Ação 16: A Comissão irá aproveitar a aplicação do Plano de Ação sobre o financiamento do terrorismo para contribuir igualmente para a luta contra as ameaças híbridas.

Os autores de ameaças híbridas e os respetivos apoiantes necessitam de fundos para executar os seus planos. Os esforços da UE contra o financiamento da criminalidade e do terrorismo no âmbito da Agenda Europeia para a Segurança e do Plano de Ação sobre o financiamento do terrorismo podem igualmente contribuir para a luta contra as ameaças híbridas. Em dezembro de 2016, a Comissão apresentou três propostas legislativas, designadamente sobre as sanções penais aplicáveis ao branqueamento de capitais e aos pagamentos ilícitos em dinheiro, bem como sobre o congelamento e o confisco de bens[19].
Todos os Estados-Membros estavam obrigados a transpor até 26 de junho de 2017 a Quarta Diretiva relativa ao Branqueamento de Capitais[20]; em julho de 2016, a Comissão apresentou uma proposta legislativa específica para complementar e reforçar esta diretiva com medidas adicionais[21].

Em 26 de junho de 2017, a Comissão publicou a avaliação supranacional dos riscos prevista na Quarta Diretiva relativa ao Branqueamento de Capitais. Além disso, apresentou uma proposta de regulamento para impedir a importação e o armazenamento na UE de bens culturais ilicitamente exportados de países terceiros[22]. Ainda este ano, a Comissão irá comunicar os resultados da sua avaliação contínua da eventual necessidade de medidas suplementares para detetar o financiamento do terrorismo na UE. A Comissão está igualmente a rever a legislação relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário[23].

---

[18] Estudo intitulado *Evaluation of risk assessment capacity at the level of Member States' authorities performing coast guard functions*, 2017, https://ec.europa.eu/maritimeaffairs/documentation/studies

[19] Terceiro relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz, COM(2016) 831 final.

[20] Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2015, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo, que altera o Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho, e que revoga a Diretiva 2005/60/CE do Parlamento Europeu e do Conselho e a Diretiva 2006/70/CE da Comissão (texto relevante para efeitos do EEE), JO L 141 de 5.6.2015, pp. 73-117.

[21] Para mais informações, ver o Terceiro relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz (COM(2016) 831 final) e o Oitavo relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz (COM(2017) 354 final).

[22] COM(2017) de 26.6.2017, COM(2017) 340 final, SWD(2017) 275 final.

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

O Oitavo relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz aprofunda o ponto da situação da aplicação do Plano de Ação sobre o financiamento do terrorismo.

Promover os valores comuns da UE e as sociedades inclusivas, abertas e resilientes

Reforço da resiliência contra a radicalização e o extremismo violento

A radicalização religiosa e ideológica, os conflitos étnicos e os conflitos minoritários podem ser iniciados por intervenientes externos graças ao apoio de grupos específicos ou de esforços para alimentar conflitos entre grupos. Entretanto surgiram desafios adicionais, como as ameaças de intervenientes solitários, as novas vias de radicalização – potencialmente também no contexto da crise migratória –, o aumento do extremismo de direita (incluindo a violência contra os migrantes) e os riscos de polarização. Apesar de os trabalhos sobre a radicalização serem realizados no contexto da União da Segurança, podem também ser indiretamente pertinentes para a problemática das ameaças híbridas, uma vez que as pessoas vulneráveis à radicalização podem ser manipuladas pelos autores desse tipo de ameaças.

Ação 17: ***A Comissão está a implementar as ações contra a radicalização estabelecidas na Agenda Europeia para a Segurança e a analisar a necessidade de reforçar os procedimentos para a eliminação de conteúdos ilegais, solicitando aos intermediários que garantam a diligência devida na gestão das redes e sistemas.***

Prevenir a radicalização

Tal como preconizado na Comunicação sobre o apoio à prevenção da radicalização que conduz ao extremismo violento[24], a Comissão continua a implementar a sua resposta multifacetada à radicalização, que inclui ações importantes como a promoção da educação inclusiva e dos valores comuns, a luta contra a propaganda extremista em linha e a radicalização nas prisões, o reforço da cooperação com países terceiros e a intensificação da investigação, a fim de melhor compreender a natureza evolutiva da radicalização e de melhor definir as respostas políticas. A Rede de Sensibilização para a Radicalização (RSR) tem estado na vanguarda do trabalho da Comissão para apoiar os Estados-Membros neste domínio, em colaboração com os intervenientes locais à escala das comunidades. Mais informações no Oitavo relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz[25].

Radicalização e incitação ao ódio em linha

Em conformidade com a Agenda Europeia para a Segurança[26], a Comissão tomou medidas para reduzir a disponibilidade de conteúdos ilegais em linha, nomeadamente através da unidade da UE que, na Europol, se dedica à sinalização de conteúdos na Internet e do Fórum

[24] http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf
[25] COM(2017) 354 final.
[26] Mais informações no Oitavo relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz, COM(2017) 354 final.

da UE na Internet[27]. Foram igualmente efetuados progressos significativos no âmbito do código de conduta contra os discursos ilegais de incitação ao ódio em linha[28]. Mais informações no Oitavo relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz[29]. Estas ações serão reforçadas, também à luz das conclusões do Conselho Europeu[30], da Cimeira do G7[31] e da Cimeira do G20 em Hamburgo[32].

As plataformas em linha desempenham um papel fundamental na luta contra conteúdos ilegais ou potencialmente nocivos. No âmbito da Estratégia para o Mercado Único Digital, tal como indicado na revisão intercalar[33], a Comissão irá assegurar uma melhor coordenação dos diálogos no quadro da plataforma relativa aos mecanismos e às soluções técnicas para a remoção de conteúdos ilegais. Se for caso disso, o objetivo deve ser o de apoiar esses mecanismos com orientações sobre determinados aspetos, tais como a notificação e a remoção de conteúdos ilegais. A Comissão irá também fornecer orientações sobre as regras em matéria de responsabilidade.

Cooperação mais estreita com países terceiros

Ação 18: ***A Alta Representante, em coordenação com a Comissão, irá lançar um estudo sobre os riscos híbridos nas regiões vizinhas. A Alta Representante, a Comissão e os Estados-Membros utilizarão os instrumentos ao seu dispor para consolidar as capacidades dos parceiros e reforçar a resiliência destes face a ameaças híbridas. Poderão ser realizadas missões da PCSD, independentemente ou em complemento de instrumentos da UE, para ajudar os parceiros a reforçar as suas capacidades.***

No setor da segurança, a União Europeia reforçou a tónica no reforço das capacidades e da resiliência nos países parceiros, nomeadamente explorando a ligação entre segurança e desenvolvimento, reforçando a dimensão de segurança da Política Europeia de Vizinhança revista e encetando diálogos em matéria de segurança e luta contra o terrorismo com países da região do Mediterrâneo. Nesta ótica, foi lançado um estudo sobre os riscos no quadro de um projeto-piloto em cooperação com a República da Moldávia, cujo objetivo consiste em ajudar a identificar as principais vulnerabilidades do país e garantir que a assistência da UE visa especificamente esses domínios. Os resultados do projeto-piloto revelaram que o estudo em si foi considerado útil. Com base na experiência adquirida, a Comissão e o SEAE irão apresentar recomendações para dar prioridade às ações da componente relativa à eficácia, às comunicações estratégicas, à proteção das infraestruturas críticas e à cibersegurança.

No futuro, outros países vizinhos poderão beneficiar do estudo, com base nesta primeira experiência, embora com adaptações específicas para refletir a diversidade das situações locais e das ameaças enfrentadas por cada país, bem como para evitar a duplicação dos

[27] Mais informações no Oitavo relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz, COM(2017) 354 final.
[28] *Code of Conduct on illegal online hate speech*, de 31 de maio de 2016, http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf
[29] Mais informações no Oitavo relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz, COM(2017) 354 final.
[30] Conclusões do Conselho de 22-23 de junho de 2017.
[31] Cimeira do G7 em Taormina, Itália, 26-27.5.2017.
[32] Cimeira do G20 em Hamburgo, Alemanha, 7-8.7.2017.
[33] Ver a Comunicação da Comissão acima mencionada, COM(2017) 228 final.

diálogos em curso em matéria de segurança e antiterrorismo. De uma forma mais geral, em 7 de junho de 2017, a Comissão e a Alta Representante adotaram uma Comunicação conjunta intitulada «Uma abordagem estratégica em matéria de resiliência na ação externa da UE»[34]. O objetivo é ajudar os países parceiros a tornarem-se mais resilientes face aos desafios globais com que se deparam hoje em dia. A comunicação reconhece a necessidade de passar da mera contenção das crises para uma abordagem de longo prazo, mais estrutural, das vulnerabilidades, com destaque para a antecipação, a prevenção e a preparação.

Ciber-resiliência para o desenvolvimento

A UE presta apoio aos países de fora da Europa no sentido de reforçar a resiliência das suas redes de informação. O aumento da digitalização comporta uma dimensão de segurança intrínseca que levanta desafios específicos à resiliência dos sistemas de redes de informação à escala mundial, uma vez que os ciberataques não conhecem fronteiras. A UE ajuda países terceiros a reforçar a sua capacidade para prevenir e responder adequadamente a falhas acidentais e a ciberataques. Na sequência de um projeto-piloto de cibersegurança na antiga República jugoslava da Macedónia, no Kosovo[35] e na Moldávia, concluído em 2016, a Comissão irá lançar um novo programa para reforçar a ciber-resiliência de países terceiros, sobretudo em África e na Ásia, no período de 2017-2020, mas também na Ucrânia. O objetivo consiste em reforçar a segurança e a preparação das redes e infraestruturas de informação críticas nos países terceiros, com base numa abordagem envolvendo a totalidade das instâncias governativas, e, simultaneamente, assegurar a conformidade com os direitos humanos e o Estado de Direito.

Segurança da aviação

A aviação civil continua a ser um alvo principal e simbólico para os terroristas, mas também poderá vir a ser visada por uma campanha de ameaças híbridas. Apesar de a UE ter criado um quadro sólido em matéria de segurança da aviação, os voos provenientes de países terceiros podem ser mais vulneráveis. Em conformidade com a resolução 2309 (2016) do Conselho de Segurança das Nações Unidas, a Comissão está a intensificar os esforços de consolidação das capacidades de países terceiros. Em janeiro de 2017, a Comissão lançou uma nova avaliação integrada dos riscos a fim de garantir a prioridade e a coordenação dos esforços de consolidação das capacidades envidados a nível da UE e dos Estados-Membros, bem como com os parceiros internacionais. Em 2016, a Comissão lançou um projeto com a duração de quatro anos sobre a segurança da aviação civil em África e na Península Arábica, com o intuito de combater a ameaça do terrorismo contra a aviação civil. O projeto centra-se na partilha de conhecimentos especializados entre Estados parceiros e peritos dos países membros da Conferência Europeia da Aviação Civil, bem como em atividades de mentoria, formação e *coaching*. Estas atividades serão intensificadas no decurso de 2017.

[34]Comunicação Conjunta ao Parlamento Europeu e ao Conselho: Uma abordagem estratégica em matéria de resiliência na ação externa da UE, JOIN (2017) 21 final.

[35] Esta designação não prejudica as posições relativas ao estatuto e está em conformidade com a RCSNU 1244 e com o parecer do TJI sobre a Declaração de Independência do Kosovo.

c. PREVENÇÃO E RESPOSTA A SITUAÇÕES DE CRISE E RECUPERAÇÃO

Embora as consequências possam ser atenuadas através de políticas de longo prazo a nível nacional e da UE, continua a ser essencial, a curto prazo, reforçar a capacidade dos Estados-Membros e da União para prevenir, responder e recuperar de ameaças híbridas de uma forma rápida e coordenada. É fundamental dar resposta rápida aos acontecimentos desencadeados por ameaças híbridas. Foram já alcançados progressos consideráveis neste domínio no último ano através de um protocolo operacional agora em vigor na UE que define o processo de gestão da crise no caso de um ataque híbrido. Daqui para a frente, haverá monitorização e exercícios regulares.

Ação 19: ***A Alta Representante e a Comissão, em coordenação com os Estados-Membros, irão estabelecer um protocolo operacional comum e realizar exercícios regulares para melhorar a capacidade de tomada de decisões estratégicas em resposta a ameaças híbridas complexas com base nos procedimentos de gestão da crise e no mecanismo integrado de resposta política a situações de crise.***

O Quadro comum recomendou a criação de mecanismos de resposta rápida a acontecimentos desencadeados por ameaças híbridas, com vista à coordenação entre os mecanismos de resposta da UE[36] e os sistemas de alerta precoce. Para o efeito, os serviços da Comissão e o SEAE publicaram o Protocolo operacional da UE para a luta contra as ameaças híbridas (*EU Playbook*)[37], que estabelece as modalidades para a coordenação; a fusão e análise de informação; a informação dos processos de decisão política; os exercícios e a formação; e a cooperação com organizações parceiras, nomeadamente a NATO, no caso de uma ameaça híbrida. De igual modo, a NATO produziu um manual para a interação reforçada NATO-UE na prevenção e na luta contra as ameaças híbridas nos domínios da ciberdefesa, das comunicações estratégicas, do conhecimento da situação e da gestão de crises. O protocolo operacional será testado através de um exercício no outono de 2017, como parte do Exercício Paralelo e Coordenado da União Europeia, que implica uma interação com a NATO.

Ação 20*: A Comissão e a Alta Representante, nos respetivos domínios de competência, irão analisar a aplicabilidade e as implicações práticas do artigo 222.º do TFUE e do artigo 42.º, n.º 7, do TUE, caso se verifiquem ameaças híbridas graves e de grande amplitude.*

O artigo 42.º, n.º 7, do TUE refere-se a uma agressão armada no território de um Estado-Membro, ao passo que o artigo 222.º do TFUE (cláusula de solidariedade) se refere a um ataque terrorista ou a um desastre natural ou de origem humana no território de um Estado-Membro. Este último é mais suscetível de ser utilizado no caso de ataques híbridos, que são uma combinação de ações subversivas e criminosas. A invocação da cláusula de solidariedade desencadeia a coordenação a nível do Conselho (Mecanismo Integrado de Resposta Política a Situações de Crise, IPCR) e o envolvimento das instituições, agências e órgãos pertinentes da UE, bem como os programas e mecanismos de assistência da UE. A Decisão 2014/415/UE do Conselho define as regras de execução da cláusula de solidariedade pela União. Estas modalidades de aplicação permanecem válidas, não havendo necessidade de rever a decisão do Conselho. Caso um ataque híbrido inclua uma agressão armada, o

[36] O Mecanismo Integrado de Resposta Política a Situações de Crise (IPCR) do Conselho, o sistema ARGUS da Comissão e o mecanismo de resposta a situações de crise do SEAE.
[37] Documento de trabalho dos serviços da Comissão (2016) 227, adotado em 7 de julho de 2016.

artigo 42.º, n.º 7, também poderá ser invocado. Nesse caso, a ajuda e a assistência serão prestadas tanto pelos Estados-Membros como pela UE. A Comissão e a Alta Representante continuarão a avaliar as formas mais eficazes de fazer face a esses ataques.

A adoção do já mencionado protocolo operacional da UE contribui diretamente para esta avaliação; o protocolo será posto em prática no âmbito do Exercício Paralelo e Coordenado (PACE) da UE em outubro de 2017. Este exercício irá testar os diferentes mecanismos da UE e a sua capacidade de interação, com o objetivo de acelerar a tomada de decisões caso a ambiguidade desencadeada por uma ameaça híbrida prejudique a clareza.

***Ação 21:* A Alta Representante, em coordenação com os Estados-Membros, irá integrar, explorar e coordenar as capacidades de ação militar na luta contra as ameaças híbridas no âmbito da Política Comum de Segurança e Defesa.**

Em resposta à missão de integração das capacidades militares em apoio da PESC/PCSD, o parecer militar relativo ao documento *The EU military contribution to countering hybrid threats within the CSDP* (contribuição militar da UE para a luta contra as ameaças híbridas no âmbito da PCSD) ficou concluído em julho de 2017, após um seminário que reuniu peritos militares em dezembro de 2016 e seguindo as orientações do grupo de trabalho do Comité Militar da União Europeia, de maio de 2017. Este parecer terá aplicação concreta no plano de aplicação da elaboração de conceitos.

d. COOPERAÇÃO UE-NATO

***Ação 22*: A Alta Representante, em coordenação com a Comissão, irá prosseguir o diálogo informal e reforçar a cooperação e a coordenação com a NATO em matéria de conhecimento da situação, comunicações estratégicas, cibersegurança e prevenção e resposta às crises, para lutar contra as ameaças híbridas, no respeito dos princípios da inclusividade e da autonomia do processo de tomada de decisões de cada organização.**

Com base na Declaração Conjunta assinada pelos Presidentes do Conselho Europeu e da Comissão Europeia, juntamente com o Secretário-Geral da NATO, em Varsóvia, em 8 de julho de 2016, a UE e a NATO desenvolveram um conjunto comum de 42 propostas de aplicação, que foi posteriormente aprovado em processos paralelos e separados, em 6 de dezembro de 2016, pelos Conselhos da UE e da NATO[38]. Em junho de 2017, a Alta Representante/Vice-Presidente e o Secretário-Geral da NATO publicaram um relatório sobre os progressos gerais realizados no que diz respeito às 42 ações da Declaração Conjunta. A luta contra as ameaças híbridas é um dos sete domínios de cooperação identificados na Declaração Conjunta, representando dez das 42 ações. O relatório revela que os esforços conjuntos envidados durante o ano passado produziram resultados consideráveis. Muitas das ações específicas destinadas a lutar contra as ameaças híbridas já foram mencionadas, incluindo o Centro Europeu de Excelência para a Luta contra as Ameaças Híbridas, um melhor conhecimento da situação, a criação da Célula de Fusão da UE contra as ameaças híbridas e a sua interação com a recém-criada célula de análise de ameaças híbridas da NATO, bem como a colaboração entre equipas de comunicação estratégica. Pela primeira vez, o pessoal da NATO e o pessoal da UE irão realizar um exercício conjunto de resposta a um cenário de ameaças híbridas, que deverá servir para testar a aplicação de mais de um terço das

[38] http://www.consilium.europa.eu/en/press/press-releases/2016/12/06-eu-nato-joint-declaration/

propostas comuns. A UE realizará este ano o seu próprio exercício paralelo e coordenado e está a preparar-se para assumir um papel de liderança em 2018.

No que diz respeito à resiliência, o pessoal da UE e o pessoal da NATO estão a levar a cabo sessões de informação (*briefings*) cruzadas, inclusivamente no que diz respeito ao Mecanismo Integrado da UE de Resposta Política a Situações de Crise. Os contactos regulares entre o pessoal da NATO e o da UE, incluindo através de seminários ou da participação no Conselho Diretivo da Agência Europeia de Defesa, permitiram intercâmbios de informação sobre os requisitos de base da NATO em matéria de resiliência nacional. Estão previstos para este outono outros intercâmbios entre a Comissão e a NATO sobre os meios para reforçar a resiliência. O próximo relatório sobre os progressos da cooperação UE-NATO irá propor formas de alargar a cooperação entre as duas organizações.

3. CONCLUSÃO

O Quadro comum define as ações destinadas a lutar contra as ameaças híbridas e a reforçar não só a resiliência da UE e dos Estados-Membros, mas também a dos parceiros. Apesar de a Comissão e a Alta Representante estarem a obter resultados em todos os domínios em estreita cooperação com os Estados-Membros e os parceiros, é fundamental manter esta dinâmica face a ameaças híbridas persistentes e em constante evolução. Incumbe aos Estados-Membros a responsabilidade principal pela luta contra as ameaças híbridas relacionadas com a segurança nacional e com a manutenção da lei e da ordem. A resiliência nacional e os esforços coletivos para assegurar proteção contra as ameaças híbridas devem ser entendidos como elementos de um mesmo esforço global que se reforçam mutuamente. Por conseguinte, os Estados-Membros são incentivados a realizar, o mais rapidamente possível, estudos sobre os riscos híbridos, uma vez que estes irão fornecer informações preciosas sobre o grau de vulnerabilidade e de preparação em toda a Europa. O potencial da Célula de Fusão da UE contra as ameaças híbridas deverá ser maximizado com base nos progressos significativos realizados em matéria do conhecimento da situação. A Alta Representante convida os Estados-Membros a apoiar o trabalho das *task forces* StratCom, a fim de combater mais eficazmente o surgimento de ameaças híbridas. A UE apoia totalmente o Centro Europeu para a Luta contra as Ameaças Híbridas liderado pela Finlândia.

O trunfo único da UE reside na ajuda dada aos Estados-Membros e aos parceiros para que estes reforcem a sua resiliência, com base numa ampla gama de instrumentos e programas existentes. As ações destinadas a aumentar a resiliência em domínios como os transportes, a energia, a cibersegurança, as infraestruturas críticas, a proteção do sistema financeiro contra as utilizações ilícitas e a luta contra o extremismo violento e a radicalização registaram progressos significativos. A ação da UE para reforçar a resiliência irá evoluir em paralelo com a natureza das ameaças híbridas. A UE irá designadamente desenvolver indicadores com vista a reforçar a proteção e a resiliência das infraestruturas críticas contra as ameaças híbridas nos setores relevantes.

O Fundo Europeu de Defesa poderá vir a cofinanciar, juntamente com os Estados-Membros, as capacidades consideradas prioritárias para reforçar a resiliência contra as ameaças híbridas. O anunciado pacote de medidas em matéria de cibersegurança, bem como as medidas intersetoriais destinadas a aplicar a diretiva relativa à segurança das redes e da informação, fornecerão novas plataformas de luta contra as ameaças híbridas em toda a UE.

A Comissão e a Alta Representante urgem os Estados-Membros e as partes interessadas a alcançar, se necessário, um acordo rápido e a garantir a aplicação célere e eficaz das muitas medidas destinadas a reforçar a resiliência estabelecidas na presente comunicação. A UE irá consolidar e aprofundar a sua já frutuosa cooperação com a NATO.

A União continua empenhada em mobilizar todos os instrumentos pertinentes ao seu dispor para fazer face a ameaças híbridas complexas. Apoiar os esforços dos Estados-Membros continua a ser a prioridade da União, que, ao lado dos seus principais parceiros, atua como um garante da segurança mais vigoroso e mais reativo.