COMISSÃO
EUROPEIA

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

Bruxelas, 6.4.2016
JOIN(2016) 18 final

COMUNICAÇÃO CONJUNTA AO PARLAMENTO EUROPEU E AO CONSELHO

Quadro comum em matéria de luta contra as ameaças híbridas

uma resposta da União Europeia

1. INTRODUÇÃO

Nos últimos anos, o contexto de segurança da União Europeia mudou radicalmente. Os principais desafios para a paz e a estabilidade nas regiões vizinhas a Leste e a Sul da UE continuam a realçar a necessidade de uma adaptação e de um aumento das capacidades da União como garante da segurança, com uma forte ênfase na estreita relação entre segurança externa e segurança interna. Um grande número dos desafios que se colocam atualmente em matéria de paz, segurança e prosperidade tem origem na instabilidade nas regiões limítrofes da UE e na evolução a nível das formas que assumem as ameaças. Nas suas orientações políticas de 2014, o Presidente da Comissão Europeia, Jean-Claude Juncker, sublinhou a necessidade de «trabalhar para reforçar a Europa em matéria de segurança e de defesa» e de combinar os instrumentos europeus e nacionais de forma mais eficaz do que no passado. Além disso, na sequência do convite dirigido pelo Conselho dos Negócios Estrangeiros de 18 de maio de 2015, a Alta Representante, em estreita cooperação com os serviços da Comissão e a Agência Europeia de Defesa (AED), e em consulta com os Estados-Membros da UE, iniciou os trabalhos para este quadro conjunto com propostas suscetíveis de conduzirem a ações para ajudar a fazer face às ameaças híbridas e reforçar a resiliência da UE e dos seus Estados-Membros, bem como dos seus parceiros[1]. Além disso, em junho de 2015, o Conselho Europeu recordou a necessidade de mobilizar os instrumentos da UE para ajudar a fazer face às ameaças híbridas[2].

Embora as definições de ameaças híbridas variem e tenham de permanecer flexíveis para responder à sua natureza evolutiva, o conceito destina-se a abarcar a combinação de atividades coercivas com atividades subversivas, de métodos convencionais com métodos não convencionais (ou seja, diplomáticos, militares, económicos, tecnológicos) que podem ser utilizados de forma coordenada por intervenientes estatais ou não estatais para atingir objetivos específicos, mantendo-se, no entanto, abaixo do limiar de uma guerra formalmente declarada. Em geral, coloca-se a ênfase na exploração das vulnerabilidades do objetivo e na criação de ambiguidade para entravar o processo de tomada de decisões. Grandes campanhas de desinformação, recorrendo aos meios de comunicação social, para controlar o discurso político ou para radicalizar, recrutar e dirigir intervenientes por interposição podem ser vetores de ameaças híbridas.

Na medida em que o combate às ameaças híbridas diz respeito à segurança e à defesa nacionais, bem como à manutenção da lei e da ordem, a principal responsabilidade cabe aos Estados-Membros, porque a maior parte das vulnerabilidades nacionais são específicas de cada país. No entanto, muitos Estados-Membros da UE enfrentam ameaças comuns, que podem visar igualmente redes ou infraestruturas transfronteiras. Tais ameaças podem ser abordadas de forma mais eficaz através de uma resposta coordenada a nível da UE, recorrendo às políticas e instrumentos da UE, para tirar partido da solidariedade europeia, da assistência mútua e de todo o potencial do Tratado de Lisboa.

[1] Conclusões do Conselho sobre a política comum de segurança e defesa (PCSD), maio de 2015 [Consilium 8971/15].
[2] Conclusões do Conselho, junho de 2012 [EUCO 22/15].

As políticas e instrumentos da UE podem, e em grande medida já o fazem, desempenhar um papel fundamental e de inegável valor acrescentado em termos do conhecimento da situação, o que tem vindo a contribuir para melhorar a resiliência dos Estados-Membros na resposta a ameaças comuns. A ação externa da União proposta no âmbito do presente quadro é orientada pelos princípios estabelecidos no artigo 21.º do Tratado da União Europeia (TUE), que incluem a democracia, o Estado de direito, a universalidade e indivisibilidade dos direitos humanos e o respeito pelos princípios da Carta das Nações Unidas e do direito internacional[3].

A presente comunicação conjunta visa facilitar uma abordagem holística que permitirá à UE, em coordenação com os Estados-Membros, combater especificamente as ameaças de natureza híbrida, criando sinergias entre todos os instrumentos relevantes e promovendo uma cooperação mais estreita entre todos os intervenientes[4]. As ações baseiam-se em estratégias e políticas setoriais existentes que contribuem para conseguir uma maior segurança. Em especial, a Agenda Europeia para a Segurança[5], a estratégia global da União Europeia para a política externa e de segurança e o plano de ação europeu no domínio da defesa[6] (em vias de elaboração), a estratégia da UE para a cibersegurança[7], a estratégia de segurança energética[8], a estratégia europeia de segurança marítima[9] são instrumentos que podem igualmente contribuir para fazer face às ameaças híbridas.

Como a NATO também está a trabalhar para fazer face às ameaças híbridas e o Conselho dos Negócios Estrangeiros propôs o reforço da cooperação e da coordenação neste domínio, algumas das propostas têm por objetivo intensificar a cooperação UE-NATO em matéria de luta contra as ameaças híbridas.

A resposta proposta centra-se nos seguintes elementos: aumentar o conhecimento da situação, reforçar a resiliência, prevenir e fazer face às crises, bem como recuperar das mesmas.

2. RECONHECER A NATUREZA HÍBRIDA DE UMA AMEAÇA

As ameaças híbridas visam explorar as vulnerabilidades de um país e, muitas vezes, pretendem minar os valores democráticos e liberdades fundamentais. Como primeiro passo, a Alta Representante e a Comissão trabalharão em conjunto com os Estados-Membros a fim de melhorar o conhecimento da situação através do acompanhamento e avaliação dos riscos suscetíveis de visar as vulnerabilidades da UE. A Comissão está a

[3] A Carta dos Direitos Fundamentais da UE é vinculativa para as instituições da UE e para os Estados-Membros quando aplicam o direito da União.
[4] As eventuais propostas legislativas serão sujeitas aos requisitos da Comissão em matéria de melhoria da regulamentação, em conformidade com as orientações da Comissão «Legislar melhor», SWD(2015) 111.
[5] COM(2015) 185 final.
[6] A apresentar em 2016.
[7] Quadro Estratégico da UE para a Ciberdefesa (Consilium 15585/14] e Comunicação Conjunta intitulada «Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido», fevereiro de 2013 [JOIN (2013) 1].
[8] Comunicação conjunta intitulada «Estratégia europeia de segurança energética», maio de 2014 [SWD(2014) 330].
[9] Comunicação conjunta intitulada «Para um domínio marítimo global aberto e seguro: Elementos para uma estratégia da União Europeia em prol da segurança dos mares», JOIN(2014) 9 final — 06/03/2014.

desenvolver metodologias de avaliação dos riscos para a segurança, a fim de contribuir para informar os responsáveis pela tomada de decisões e promover a elaboração de políticas baseadas nos riscos, em domínios que vão da segurança da aviação ao financiamento do terrorismo e ao branqueamento de capitais. Além disso, seria pertinente que os Estados-Membros realizassem um estudo para identificar domínios vulneráveis a ameaças híbridas. O objetivo seria o de identificar indicadores de ameaças híbridas, a integrar nos mecanismos de alerta precoce e de avaliação dos riscos existentes e, se conveniente, a partilhar.

***Ação 1*: 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.**

3. ORGANIZAR A RESPOSTA DA UE: AUMENTAR O CONHECIMENTO DA SITUAÇÃO

3.1. Célula de fusão da UE contra as ameaças híbridas

É essencial que a UE, em coordenação com os seus Estados-Membros, atinja um nível suficiente de conhecimento da situação para identificar qualquer alteração no contexto de segurança relacionada com uma atividade híbrida provocada por intervenientes estatais e não estatais. A fim de fazer combater eficazmente as ameaças híbridas, é importante melhorar o intercâmbio de informações e promover a partilha de informações pertinentes entre todos os setores e entre a União Europeia, os seus Estados-Membros e os parceiros.

Uma célula de fusão da UE contra as ameaças híbridas constituirá um ponto fulcral único para a análise de ameaças híbridas, estabelecido no âmbito do Centro de Análise de Informações da UE (INTCEN) do Serviço Europeu para a Ação Externa (SEAE). Esta célula de fusão receberá, analisará e partilhará informações classificadas e informações de fonte aberta especificamente relacionadas com os indicadores e alertas relativos a ameaças híbridas provenientes de diferentes partes interessadas no âmbito do SEAE (incluindo as delegações da UE), da Comissão (com as agências da UE[10]) e dos Estados-Membros. Em colaboração com outros organismos semelhantes existentes a nível da UE[11] e a nível nacional, a célula de fusão analisará os aspetos externos das ameaças híbridas, que afetam a UE e os seus vizinhos, a fim de analisar rapidamente os incidentes relevantes neste domínio e disponibilizar informações necessárias aos processos de tomada de decisões estratégicas da UE, nomeadamente facultando contributos que permitam alimentar as avaliações dos riscos para a segurança efetuadas a nível da UE. Os resultados analíticos da célula de fusão serão tratados e utilizados em conformidade com as regras da União Europeia relativas às informações classificadas e à proteção de dados[12]. A célula deverá trabalhar em articulação com os organismos existentes a nível

[10] Em conformidade com os seus mandatos.
[11] Por exemplo, o Centro Europeu da Cibercriminalidade e o Centro Europeu de Luta contra o Terrorismo da Europol, a Frontex e a Equipa de Resposta a Emergências Informáticas (CERT-UE).
[12] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995.

nacional e da UE. Os Estados-Membros devem criar pontos de contacto nacionais ligados à célula de fusão da UE contra as ameaças híbridas. O pessoal dentro e fora da UE (incluindo o destacado junto de delegações da UE, bem como o que participa em missões e operações) e nos Estados-Membros deve igualmente ser formado para detetar os sinais precoces de ameaças híbridas.

<u>Ação 2</u>: Criação de uma célula de fusão da UE contras as ameaças híbridas no âmbito da estrutura existente INTCEN, capaz de receber e de analisar informações classificadas e provenientes de fontes abertas sobre ameaças híbridas. Os Estados-Membros são convidados a criar pontos de contacto nacionais sobre ameaças híbridas para assegurar a cooperação e uma comunicação segura com a célula de fusão da UE contra as ameaças híbridas.

3.2. Comunicação estratégica

Os autores de ameaças híbridas podem realizar campanhas sistemáticas de desinformação, nomeadamente através dos meios de comunicação social, procurando desse modo radicalizar indivíduos, desestabilizar a sociedade e o discurso político. A capacidade de resposta a ameaças híbridas através de uma sólida **política de comunicação** estratégica é essencial. Fornecer respostas factuais rápidas e sensibilizar a opinião pública para as ameaças híbridas são fatores importantes para reforçar a resiliência da sociedade.

A comunicação estratégica deveria explorar plenamente as redes sociais, bem como os meios de comunicação social visuais, áudio e em linha tradicionais. O SEAE, com base nas atividades das task-forces East Stratcom e Arab Stratcom, deverá otimizar o recurso a linguistas fluentes em línguas importantes de países terceiros e a especialistas dos meios de comunicação social, que possam acompanhar a informação proveniente de fora da UE e garantir uma comunicação específica para reagir à desinformação. Além disso, os Estados-Membros devem desenvolver mecanismos coordenados de comunicação estratégica para apoiar a indicação das fontes e combater a desinformação, a fim de expor as ameaças híbridas.

<u>Ação 3</u>: A Alta Representante estudará com os Estados-Membros as formas de atualizar e coordenar as capacidades em matéria de comunicações estratégicas proativas e de otimizar o recurso a especialistas no domínio do acompanhamento dos meios de comunicação social e a linguistas.

3.3. Centro de Excelência para a «luta contra as ameaças híbridas»

Com base na experiência de alguns Estados-Membros e certas organizações parceiras[13], uma instituição multinacional ou uma rede de instituições multinacionais poderá atuar como centro de excelência para as ameaças híbridas. Um centro deste tipo poderá dedicar-se a investigar a forma como as estratégias híbridas foram aplicadas e incentivar

[13] Centros de Excelência da Nato.

o desenvolvimento de novos conceitos e de novas tecnologias no setor privado e na indústria para ajudar os Estados-Membros a aumentar a resiliência. A investigação poderá contribuir para harmonizar as políticas, doutrinas e conceitos nacionais e da UE e garantir que os processos de tomada de decisões tenham em conta a complexidade e as ambiguidades associadas às ameaças híbridas. O centro deverá conceber programas para fazer avançar a investigação e exercícios destinados a encontrar soluções práticas para os problemas atuais colocados pelas ameaças híbridas. A força de um centro deste tipo assentará nas competências desenvolvidas pelos seus participantes intersetoriais e multinacionais, civis e militares, pertencentes ao setor privado e ao meio académico.

Um centro com estas características poderá cooperar estreitamente com os centros de excelência existentes da UE[14] e da NATO[15], com vista a beneficiar dos conhecimentos sobre ameaças híbridas adquiridos no âmbito da ciberdefesa, da comunicação estratégica, da cooperação civil e militar, da resposta energética e da reação às crises.

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

4. ORGANIZAR A RESPOSTA DA UE: REFORÇAR A RESILIÊNCIA

A resiliência é a capacidade de resistir ao desgaste e de recuperar, saindo reforçado dos desafios. Para combater eficazmente as ameaças híbridas, é necessário abordar as potenciais vulnerabilidades das infraestruturas essenciais, das cadeias de abastecimento e da sociedade em geral. As infraestruturas a nível da UE podem tornar-se mais resilientes se assentarem nos instrumentos e políticas da UE.

4.1. Proteção das infraestruturas críticas

É importante proteger as infraestruturas críticas (por exemplo, as cadeias de aprovisionamento energético e os transportes), uma vez que um ataque não convencional, por autores de ameaças híbridas, a qualquer «alvo vulnerável» poderá conduzir a graves perturbações económicas ou sociais. A fim de assegurar a proteção de infraestruturas críticas, o Programa Europeu para a Proteção das Infraestruturas Críticas[16] (EPCIP) prevê uma abordagem sistémica e transetorial, que tenha em conta «todos os riscos», analise as interdependências e se baseie na execução de atividades no quadro dos eixos prevenção, preparação e resposta. A Diretiva relativa às infraestruturas críticas europeias[17] estabelece um procedimento de identificação e designação das infraestruturas críticas europeias (ICE) e uma abordagem comum para avaliar a necessidade de melhorar a sua proteção. Em particular, seria conveniente relançar os trabalhos no contexto da diretiva,

[14] Por exemplo, o Instituto de Estudos de Segurança da UE (IESUE) e os centros de excelência temáticos da UE no domínio das questões QBRN.
[15] http://www.nato.int/cps/en/natohq/topics_68372.htm.
[16] Comunicação da Comissão relativa a um Programa Europeu de Proteção das Infraestruturas Críticas, 12.12.2006, COM (2006) 786 final.
[17] Diretiva 2008/114/CE do Conselho, de 8 de dezembro de 2008, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção, JO L 345, de 23.12.2008.

de modo a reforçar a resiliência das infraestruturas críticas no domínio dos transportes (por exemplo, os principais aeroportos e portos comerciais da UE). A Comissão irá avaliar a possibilidade de desenvolver instrumentos comuns, nomeadamente indicadores, para melhorar a resiliência das infraestruturas críticas contra as ameaças híbridas em todos os setores relevantes.

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

4.1.1. Redes de energia

A produção e distribuição de energia sem perturbações revestem-se de importância vital para a UE; as falhas de energia podem ser muito prejudiciais. Um elemento essencial da luta contra as ameaças híbridas consiste em diversificar as fontes energéticas, os fornecedores e os itinerários de aprovisionamento, a fim de garantir um aprovisionamento energético mais seguro e mais resiliente. A Comissão está também a realizar avaliações dos riscos e da segurança («testes de resistência») nas centrais elétricas da UE. No intuito de garantir a diversificação energética, intensificaram-se os trabalhos no contexto da estratégia para uma União da Energia: por exemplo, o Corredor Meridional de Gás, que pode permitir encaminhar para a Europa o gás proveniente da região do Mar Cáspio e, no Norte da Europa, a criação de plataformas de gás líquido com múltiplos fornecedores. Este exemplo deveria ser seguido na Europa Central e de Leste, bem como no Mediterrâneo, onde está a ser criada uma plataforma de gás[18]. O desenvolvimento do mercado de gás natural liquefeito contribui também positivamente para este objetivo.

No que diz respeito aos materiais e instalações nucleares, a Comissão apoia o desenvolvimento e a adoção das mais rigorosas normas em matéria de segurança, reforçando assim a resiliência. A Comissão está a incentivar a transposição e a aplicação coerentes da Diretiva Segurança Nuclear[19], que estabelece regras para a prevenção de acidentes e a minoração das suas consequências, bem como das disposições da Diretiva Normas de Segurança de Base[20] relativa à cooperação internacional em matéria de preparação e intervenção em situações de emergência, especialmente entre Estados-Membros limítrofes e com os países vizinhos.

[18] Sobre os progressos alcançados até à data, ver o Estado da União da Energia - 2015 (COM(2015) 572 final.

[19] Diretiva 2009/71/Euratom do Conselho, de 25 de junho de 2009, que estabelece um quadro comunitário para a segurança nuclear das instalações nucleares, tal como alterada pela Diretiva 2014/87/Euratom do Conselho, de 8 de julho de 2014.

[20] Diretiva 2013/59/Euratom do Conselho, de 5 de dezembro de 2013, que fixa as normas de segurança de base relativas à proteção contra os perigos resultantes da exposição a radiações ionizantes, e que revoga as Diretivas 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom e 2003/122/Euratom.

<u>Ação 6</u>: A Comissão, em cooperação com os Estados-Membros, apoiará os esforços no sentido de diversificar as fontes de energia e promover normas de segurança e proteção para aumentar a capacidade de resiliência das infraestruturas nucleares

4.1.2 Transportes e segurança da cadeia de abastecimento

O setor dos transportes é essencial para o funcionamento da União. Os ataques híbridos a infraestruturas de transporte (tais como, aeroportos, infraestruturas rodoviárias, portos e caminhos de ferro) podem ter consequências graves, conducentes a perturbações das deslocações e das cadeias de abastecimento. No âmbito da aplicação da legislação em matéria de segurança aérea e marítima[21], a Comissão efetua inspeções periódicas[22] e, através do seu trabalho sobre a segurança do transporte terrestre, procura dar resposta a ameaças híbridas emergentes. Neste contexto, está a ser discutido um enquadramento da UE no âmbito da revisão do Regulamento relativo à segurança da aviação[23], como elemento da Estratégia para o setor da aviação na Europa[24]. Além disso, as ameaças à segurança marítima estão a ser abordadas no âmbito da estratégia da União Europeia em prol da segurança dos mares e do respetivo plano de ação[25]. Este último permite à UE e aos Estados-Membros responder de forma global aos desafios que se colocam em matéria de segurança marítima, incluindo a luta contra as ameaças híbridas, no quadro de uma cooperação intersetorial entre intervenientes civis e militares que visa proteger as infraestruturas marítimas críticas, a cadeia de abastecimento global, o comércio marítimo e os recursos naturais e energéticos. A segurança da cadeia de abastecimento internacional é igualmente abordada na estratégia e no plano de ação da União Europeia sobre gestão dos riscos aduaneiros[26].

<u>Ação 7</u>: A Comissão acompanhará as ameaças emergentes em todo o setor dos transportes e atualizará a legislação, sempre que adequado. Na execução da estratégia de segurança marítima da UE e da estratégia e plano de ação sobre gestão dos riscos aduaneiros na UE, a Comissão e a Alta Representante (no âmbito das respetivas

---

[21] Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho, de 11 de março de 2008, relativo ao estabelecimento de regras comuns no domínio da segurança da aviação civil e que revoga o Regulamento (CE) n.º 2320/2002; Regulamento de Execução (UE) n.º 2015/1998 da Comissão, de 5 de novembro de 2015, que estabelece as medidas de execução das normas de base comuns sobre a segurança da aviação; Diretiva 2005/65/CE do Parlamento Europeu e do Conselho, de 26 de outubro de 2005, relativa ao reforço da segurança nos portos; Regulamento (CE) n.º 725/2004 do Parlamento Europeu e do Conselho, de 31 de março de 2004, relativo ao reforço da proteção dos navios e das instalações portuárias.

[22] Ao abrigo da legislação da UE, a Comissão é obrigada proceder a inspeções nos Estados-Membros para garantir a correta aplicação dos requisitos de segurança aérea e marítima. Tal inclui as inspeções junto da autoridade competente do Estado-Membro, bem como as inspeções nos aeroportos, portos, transportadoras aéreas, navios e junto das autoridades que aplicam as medidas de segurança. As inspeções da Comissão visam garantir que as normas da UE são plenamente aplicadas pelos Estados-Membros.

[23] Regulamento (UE) 2016/4 da Comissão, de 5 de janeiro de 2016, que altera o Regulamento (CE) n.º 216/2008 do Parlamento Europeu e do Conselho no que diz respeito aos requisitos essenciais de proteção ambiental; Regulamento (CE) n.º 216/2008, de 20 de fevereiro de 2008, relativo a regras comuns no domínio da aviação civil e que cria a Agência Europeia para a Segurança da Aviação.

[24] Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Uma estratégia da aviação para a Europa, COM/2015/0598 final, 7.12.2015

[25] Em dezembro de 2014, o Conselho adotou um plano de ação para a implementação da estratégia de segurança marítima da União Europeia; http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf

[26] Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social Europeu relativa à estratégia e ao plano de ação da UE sobre gestão dos riscos aduaneiros: enfrentar os riscos, reforçar a segurança da cadeia de abastecimento e facilitar o comércio, COM (2014) 527 final.

competências), em coordenação com os Estados-Membros, estudarão a forma de dar resposta às ameaças híbridas, em especial no domínio das infraestruturas críticas dos transportes.

4.1.3 Espaço

As ameaças híbridas poderiam visar infraestruturas espaciais com consequências multissetoriais. A UE concebeu o quadro de apoio à vigilância e ao rastreio de objetos no espaço[27], destinado a colocar em rede os meios detidos pelos Estados-Membros, a fim de fornecer serviços de vigilância e rastreio de objetos no espaço[28] a utilizadores identificados (Estados-Membros, instituições da UE, proprietários e operadores de veículos espaciais e autoridades de proteção civil). No contexto da estratégia espacial para a Europa, em vias de elaboração, a Comissão analisará as possibilidades de desenvolver este quadro, a fim de controlar as ameaças híbridas a infraestruturas espaciais.

As comunicações por satélite são ativos fundamentais para a gestão das crises, a resposta a situações de catástrofe, bem como para a vigilância policial, das fronteiras e das costas. Constituem a espinha dorsal de infraestruturas em grande escala, como os transportes, o espaço ou os sistemas de aeronaves pilotadas à distância. Em consonância com o apelo lançado pelo Conselho Europeu a favor da preparação da próxima geração de telecomunicações governamentais por satélite, a Comissão, em cooperação com a Agência Europeia de Defesa, está a avaliar as possibilidades de centralizar a procura, no contexto da próxima estratégia espacial e do futuro plano de ação europeu de defesa.

Muitas infraestruturas críticas dependem de uma informação de tempo exata para sincronizar as suas redes (por exemplo, energia e telecomunicações) ou indicar a hora das operações (por exemplo, mercados financeiros). A dependência em relação a um único sinal de sincronização temporal do sistema mundial de navegação por satélite não oferece a resiliência necessária para fazer face às ameaças híbridas. Galileo, o sistema mundial de navegação por satélite europeu, proporcionaria uma segunda fonte temporal fiável.

<u>Ação 8</u>: No contexto da futura estratégia espacial e do futuro plano de ação europeu de defesa, a Comissão proporá aumentar a resiliência das infraestruturas espaciais contra ameaças híbridas, nomeadamente através de uma eventual extensão do âmbito da vigilância e 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.

[27] Ver Decisão n.º 541/2014/UE do Parlamento Europeu e do Conselho.
[28] Tais como alertas anticolisão de objetos em órbita ou alertas relativos a destruições ou colisões, bem com as reentradas arriscadas de objetos espaciais na atmosfera terrestre.

4.2. Capacidades de defesa

As capacidades de defesa devem ser reforçadas a fim de melhorar a resiliência da UE face às ameaças híbridas. É importante identificar os principais domínios pertinentes em termos de capacidades, tais como a vigilância e o reconhecimento. A Agência Europeia de Defesa poderia agir como um catalisador para o desenvolvimento das capacidades militares relacionadas com as ameaças híbridas (reduzindo os ciclos de desenvolvimento das capacidades de defesa, investindo em tecnologias, sistemas e protótipos ou abrindo as empresas de defesa às tecnologias comerciais inovadoras, por exemplo). As possíveis ações poderiam ser examinadas no quadro do futuro plano de ação europeu no domínio da defesa.

***Ação 9*: A Alta Representante, eventualmente com o apoio dos Estados-Membros, em articulação com a Comissão, proporá a realização de projetos sobre a forma de adaptar as capacidades de defesa e desenvolvimento com interesse para a UE, para fazer face especificamente às ameaças híbridas contra um ou vários Estados-Membros.**

4.3. Proteção da saúde pública e da segurança dos alimentos

O estado de saúde da população pode ser comprometido pela manipulação de doenças transmissíveis ou pela contaminação dos produtos alimentares, dos solos, do ar e da água potável por substâncias químicas, biológicas, radiológicas e nucleares (QBRN). Além disso, a propagação intencional de doenças dos animais ou das plantas pode afetar gravemente a segurança alimentar da União e ter graves efeitos económicos e sociais em setores cruciais da cadeia alimentar na UE. As estruturas existentes da UE em matéria de segurança sanitária, proteção do ambiente e segurança dos alimentos podem ser utilizadas para responder a ameaças híbridas que utilizam estes métodos.

Ao abrigo da legislação da UE sobre as ameaças sanitárias transfronteiriças[29], os mecanismos existentes coordenam a preparação para as ameaças sanitárias transfronteiriças graves, associando os Estados-Membros, as agências da UE e os comités científicos[30], através do sistema de alerta rápido e de resposta. O Comité de Segurança da Saúde, que coordena a resposta dada pelos Estados-Membros às ameaças, pode agir como ponto de contacto no que se refere às vulnerabilidades no domínio da saúde pública[31] para inscrever as ameaças híbridas (nomeadamente o bioterrorismo) nas orientações sobre comunicação em situações de crise e nos exercícios de reforço das capacidades (simulação de crises) realizados com os Estados-Membros. No domínio da segurança dos alimentos, através do sistema de alerta rápido para os géneros alimentícios

[29] Decisão n.º 1082/2013/UE do Parlamento Europeu e do Conselho, de 22 de outubro de 2013, relativa às ameaças sanitárias transfronteiriças graves e que revoga a Decisão n.º 2119/98/CE, JO L 293 de 5.11.2013, p. 1.
[30] Decisão C(2015) 5383 da Comissão, de 7 de agosto de 2015, relativa ao estabelecimento de comités científicos no domínio da saúde pública, da segurança dos consumidores e do ambiente.
[31] em linha com a Decisão n.º 1082/2013/UE do Parlamento Europeu e do Conselho, de 22 de outubro de 2013, relativa às ameaças sanitárias transfronteiriças graves e que revoga a Decisão n.º 2119/98/CE, JO L 293, p. 1.

e alimentos para animais (RASFF) e do sistema comum de gestão dos riscos aduaneiros (CRMS), as autoridades competentes procedem a uma troca de informações relativas à análise dos riscos, a fim de controlar os riscos para a saúde decorrentes de alimentos contaminados. Relativamente à saúde animal e à fitossanidade, a revisão do quadro jurídico da UE[32] acrescentará novos elementos à atual «caixa de ferramentas» [33], tendo em vista uma melhor preparação face às ameaças híbridas.

Ação 10: 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.

4.4. Cibersegurança

A UE beneficia em grande medida da sua sociedade interconectada e digitalizada. Os ciberataques, que podem perturbar os serviços digitais em toda a UE, podem ser utilizados por autores de ameaças híbridas. Melhorar a resiliência dos sistemas de comunicação e informação na Europa é importante para apoiar o mercado único digital. A estratégia da UE para a cibersegurança e a Agenda Europeia para a Segurança proporcionam o quadro estratégico global para as iniciativas da UE sobre cibersegurança e cibercriminalidade. A UE contribui ativamente para o reforço do conhecimento da situação, dos mecanismos de cooperação e das respostas a dar no âmbito dos resultados esperados da estratégia em matéria de cibersegurança. Em especial, a proposta de diretiva relativa à segurança das redes e da informação (SRI)[34], contempla os riscos em matéria de cibersegurança enfrentados por um amplo leque de prestadores de serviços cruciais nos domínios da energia, dos transportes, das finanças e da saúde. Esses fornecedores, bem como os prestadores de serviços digitais essenciais (por exemplo, a computação em nuvem) devem tomar medidas adequadas de segurança e comunicar os incidentes graves às autoridades nacionais, salientando eventuais características de ameaça híbrida. Após a sua adoção pelos colegisladores, a transposição e aplicação efetivas da diretiva reforçarão as capacidades de cibersegurança nos Estados-Membros, estreitando a sua cooperação em matéria de cibersegurança através do intercâmbio de informações e de boas práticas na luta contra as ameaças híbridas. Em especial, a diretiva prevê a constituição de uma rede de 28 equipas de resposta a incidentes de segurança informática (Computer Security

[32] Regulamento n.º 2016/429 do Parlamento Europeu e do Conselho relativo às doenças animais transmissíveis e que altera e revoga determinados atos no domínio da saúde animal («Lei da Saúde Animal»), Relativamente ao Regulamento do Parlamento Europeu e do Conselho relativo a medidas de proteção contra pragas vegetais («legislação fitossanitária»), o Parlamento Europeu e o Conselho alcançaram um acordo político sobre o texto em 16 de dezembro de 2015.

[33] Por exemplo, bancos de vacinas da UE, um sistema eletrónico sofisticado de informação sobre doenças dos animais, obrigações mais rigorosas no que se refere às medidas adotadas pelos laboratórios e outras entidades que lidam com agentes patogénicos.

[34] Proposta da Comissão de Diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, COM(2013) 48 final - 7/2/2013. O Conselho da UE e o Parlamento Europeu alcançaram um acordo político sobre esta proposta de diretiva, que deverá ser formalmente adotada dentro em breve.

Incidents Response Teams - CSIRT) nacionais e de uma CERT-UE[35] para efeitos de uma cooperação operacional numa base voluntária.

A fim de incentivar a cooperação entre os setores público e privado e as abordagens à escala da UE relativamente à cibersegurança, a Comissão criou a Plataforma SRI, que propões orientações relativas às boas práticas em matéria de gestão dos riscos. Embora sejam os Estados-Membros a determinar os requisitos de segurança e as modalidades para notificar os incidentes de caráter nacional, a Comissão incentiva um elevado grau de convergência das abordagens de gestão dos riscos, com base, em especial, na rede de cooperação da Agência da União Europeia para a Segurança das Redes e da Informação (ENISA).

***Ação 11**: A Comissão incentiva os Estados-Membros a criar e a explorar plenamente, com caráter prioritário, uma rede que agrupe as 28 CSIRT e a CERT-UE, bem como um quadro para a cooperação estratégica. A Comissão, em colaboração com os Estados-Membros, deverá assegurar que as iniciativas setoriais sobre ciberameaças (por exemplo, nos setores da aviação, da energia e marítimo) sejam coerentes com as capacidades intersetoriais cobertas pela Diretiva SRI, de modo a congregar informações, conhecimentos especializados e respostas rápidas.*

4.4.1. Indústria

A dependência crescente da computação em nuvem e os grandes volumes de dados aumentaram a vulnerabilidade às ameaças híbridas. A estratégia do mercado único digital prevê uma parceria público-privada contratual em matéria de cibersegurança[36], que se concentrará na investigação e inovação e contribuirá para que a União mantenha um elevado grau de capacidade tecnológica neste domínio. A parceria público-privada contratual irá reforçar a confiança entre os diferentes intervenientes no mercado e desenvolver sinergias entre a procura e a oferta. Embora a parceria público-privada contratual e as medidas de acompanhamento incidam principalmente nos produtos e serviços de cibersegurança civil, o resultado destas iniciativas deverá permitir que os utilizadores de tecnologia estejam igualmente mais bem protegidos contra as ameaças híbridas.

***Ação 12**: A Comissão, em coordenação com os Estados-Membros, colaborará 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 relacionados com ameaças híbridas.*

4.4.2. Energia

O aparecimento de casas e equipamentos inteligentes e o desenvolvimento da rede inteligente, bem como a digitalização crescente do sistema energético, implicam

[35] Equipa de resposta a emergências informáticas (CERT-UE) para as instituições da UE
[36] A lançar em meados de 2016.

igualmente uma maior vulnerabilidade a ciberataques. A estratégia europeia de segurança energética[37] e a estratégia para a União da Energia[38] apoiam uma abordagem «todos os riscos», em que a resiliência às ameaças híbridas está integrada. A rede temática sobre a proteção das infraestruturas críticas de energia favorece a colaboração entre os operadores do setor da energia (petróleo, gás, eletricidade). A Comissão lançou uma plataforma na Internet para analisar e partilhar informações sobre as ameaças e os incidentes[39], estando igualmente a desenvolver, em conjunto com as partes interessadas[40], uma estratégia global para o setor da energia relativa à cibersegurança das operações ligadas às redes inteligentes para reduzir as vulnerabilidades. Embora os mercados da eletricidade estejam cada vez mais integrados, as regras e procedimentos para lidar com situações de crise são ainda de âmbito nacional. Devemos garantir que os governos cooperem uns com os outros na preparação para os riscos, assim como na sua prevenção e atenuação, e que todas as partes interessadas atuem com base num conjunto de regras comuns.

<u>Ação 13</u>: A Comissão publicará 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.

4.4.3. Garantir a solidez dos sistemas financeiros

A economia da UE necessita de um sistema financeiro e de pagamento seguro para funcionar. Proteger o sistema financeiro e as suas infraestruturas de ciberataques, independentemente do motivo ou natureza do agressor, é essencial. Para lidar com as ameaças híbridas contra os serviços financeiros da UE, o setor tem de compreender a ameaça, ter testado as suas defesas e dispor da tecnologia necessária para se proteger contra os ataques. Por conseguinte, a partilha de informações sobre ameaças entre participantes no mercado financeiro e com as autoridades competentes e os prestadores de serviços ou clientes é fundamental, mas também tem de ser segura e cumprir os requisitos em matéria de proteção dos dados. Em consonância com os trabalhos nas instâncias internacionais, incluindo os trabalhos do G7 neste setor, a Comissão procurará identificar os fatores que dificultam a partilha adequada de informações sobre ameaças e propor soluções. É importante assegurar controlos regulares e um aperfeiçoamento dos protocolos para proteger as empresas e infraestruturas pertinentes, incluindo a atualização constante das tecnologias que permitem reforçar segurança.

[37] Comunicação da Comissão ao Parlamento Europeu e ao Conselho: Estratégia europeia de segurança energética» - COM/2014/0330 final.
[38] Comunicação intitulada «Uma estratégia-quadro para uma União da Energia resiliente dotada de uma política em matéria de alterações climáticas virada para o futuro - COM(2015) 080 final.
[39] Incident and Threat Information Sharing EU Centre – ITIS.
[40] No quadro da plataforma «Energy Expert CyberSecurity Platform (EECSP)».

<u>Ação 14</u>: A Comissão, em cooperação com a ENISA[41], os Estados-Membros, as autoridades nacionais, europeias e internacionais competentes e as instituições financeiras, promoverá e facilitará a criação de plataformas e redes de partilha de informações sobre ameaças e estudará os fatores que dificultam o intercâmbio de tais informações.

4.4.4. Transportes

Os sistemas de transportes modernos (ferroviário, rodoviário, aéreo e marítimo) dependem de sistemas de informação que são vulneráveis aos ciberataques. Tendo em conta a dimensão transfronteiras, a UE tem um papel específico a desempenhar neste domínio. A Comissão, em coordenação com os Estados-Membros, continuará a analisar as ciberameaças e os riscos relacionados com interferências ilegais nos sistemas de transporte. A Comissão está a desenvolver um roteiro sobre a cibersegurança no domínio da aviação, em cooperação com a Agência Europeia para a Segurança da Aviação (AESA) [42]. As ciberameaças à segurança marítima são igualmente abordadas no âmbito da estratégia da União Europeia em prol da segurança dos mares e do respetivo plano de ação.

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

4.5. Focalização no financiamento das ameaças híbridas

Os autores de ameaças híbridas necessitam de financiamento para realizar as suas atividades. O financiamento pode ser utilizado para apoiar grupos terroristas ou formas mais subtis de desestabilização, tais como o apoio a grupos de pressão e de partidos políticos marginais. A UE intensificou os seus esforços contra o financiamento da criminalidade e do terrorismo, tal como indicado na Agenda Europeia para a Segurança, designadamente no seu plano de ação[43]. Neste contexto, o novo quadro europeu de luta contra o branqueamento de capitais, nomeadamente, reforça a luta contra o financiamento do terrorismo e o branqueamento de capitais, facilita o trabalho das unidades de informação financeira (UIF) nacionais com vista à identificação e ao seguimento de transferências de dinheiro suspeitas e permite o intercâmbio de informações, assegurando simultaneamente a rastreabilidade das transferências de fundos

[41] Agência da União Europeia para a Segurança das Redes e da Informação

[42] O novo Regulamento AESA é atualmente objeto de discussão entre o Parlamento Europeu e o Conselho na sequência da proposta da Comissão de dezembro de 2015. Proposta de Regulamento do Parlamento Europeu e do Conselho relativo a regras comuns no domínio da aviação civil e que cria a Agência da União Europeia para a Segurança da Aviação, e que revoga o Regulamento (CE) n.º 216/2008 do Parlamento Europeu e do Conselho - COM(2015) 613 final, 2015/0277 (COD).

[43] Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre um Plano de Ação para reforçar a luta contra o financiamento do terrorismo - COM(2016) 50 final.

na União Europeia, pelo que poderia contribuir igualmente para fazer face às ameaças híbridas. No contexto dos instrumentos da PESC, poderiam ser estudadas medidas restritivas adaptadas e eficazes para fazer face às ameaças híbridas.

<u>Ação 16</u>: A Comissão aproveitará a execução do Plano de Ação sobre o financiamento do terrorismo para contribuir igualmente para fazer face às ameaças híbridas.

4.6. Reforço da resiliência contra a radicalização e o extremismo violento

Embora os atos terroristas e o extremismo violento não sejam, por si só, de natureza híbrida, os autores de ameaças híbridas podem visar e recrutar os membros mais vulneráveis da sociedade, radicalizando-os através dos canais de comunicação modernos (incluindo as redes sociais na Internet e grupos que agem por interposição) e através da propaganda.

A fim de combater os conteúdos extremistas na Internet, a Comissão - no âmbito da estratégia para o mercado único digital - está a analisar a necessidade de eventuais novas medidas, tendo devidamente em conta o seu impacto sobre os direitos fundamentais de liberdade de expressão e de informação. Tal poderá incluir procedimentos rigorosos para a remoção de conteúdos ilegais, evitando simultaneamente a retirada de conteúdos legais («notificação e ação») e uma maior responsabilidade e controlo por parte dos intermediários na gestão das suas redes e sistemas. Estas medidas completariam a abordagem voluntária existente, segundo a qual as empresas ativas na internet e nos meios de comunicação social (em especial sob a égide do Fórum Internet da UE) e em cooperação com a Unidade de Sinalização de Conteúdos na Internet da Europol, retiram rapidamente a propaganda terrorista.

No contexto da Agenda de Segurança Europeia, a radicalização está a ser combatida através da troca de experiências e do desenvolvimento de melhores práticas, incluindo a cooperação em países terceiros. A Equipa Consultiva de Comunicação Estratégica para a Síria visa reforçar o desenvolvimento e a divulgação de mensagens alternativas para lutar contra a propaganda terrorista. A Rede de Sensibilização para a Radicalização apoia os Estados-Membros e os profissionais que necessitam de interagir com as pessoas radicalizadas (incluindo os combatentes terroristas estrangeiros) ou consideradas vulneráveis à radicalização. A rede de sensibilização para a radicalização disponibiliza atividades de formação e aconselhamento e prestará apoio a países terceiros prioritários, quando existir vontade de participar no processo. Além disso, a Comissão está a promover a cooperação judicial entre os intervenientes da justiça penal, incluindo a Eurojust, para combater o terrorismo e a radicalização nos Estados-Membros, incluindo o tratamento a reservar aos combatentes terroristas estrangeiros e aos retornados.

Em complemento das abordagens acima referidas a nível da **ação externa**, a UE contribui para a luta contra o extremismo violento, nomeadamente através de um empenhamento e um trabalho de sensibilização a nível externo, da prevenção (combate à radicalização e ao financiamento do terrorismo), bem como através de medidas para atacar os fatores económicos, políticos e sociais que dão aos grupos terroristas oportunidade para prosperar.

<u>Ação 17:</u> 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 assegurem o controlo devido na gestão das redes e sistemas.

4.7. Cooperação mais estreita com os países terceiros

Tal como sublinhado na Agenda Europeia para a Segurança, a UE reforçou a sua tónica na consolidação das capacidades no setor da segurança nos ***países parceiros***, nomeadamente explorando a ligação entre segurança e desenvolvimento e reforçando a dimensão de segurança da Política Europeia de Vizinhança revista[44]. Estas ações também podem incentivar a resiliência dos parceiros face às ameaças híbridas.

A Comissão tenciona intensificar o intercâmbio de informações operacionais e estratégicas com os países do alargamento e no âmbito da Parceria Oriental e da Vizinhança Meridional, na medida necessária para lutar contra a criminalidade organizada, o terrorismo, a migração ilegal e o tráfico de armas ligeiras. Em matéria de luta contra o terrorismo, a UE está a reforçar a cooperação com os países terceiros, através do estabelecimento de diálogos e planos de ação melhorados em matéria de segurança.

Os instrumentos de financiamento da ação externa da UE têm por objetivo a criação de instituições eficientes e responsáveis em países terceiros[45] que constituem um requisito prévio para responder eficazmente às ameaças à segurança e para aumentar a resiliência. Neste contexto, a reforma do setor da segurança e o reforço das capacidades em matéria de segurança e de desenvolvimento[46] constituem instrumentos essenciais. Ao abrigo do Instrumento para a Estabilidade e a Paz[47], a Comissão desenvolveu ações para reforçar a ciberresiliência e as capacidades dos seus parceiros de detetar e de se defender dos ciberataques e da cibercriminalidade, o que pode ser útil na luta contra as ameaças híbridas em países terceiros. A UE está a financiar as atividades de reforço das capacidades nos países parceiros para atenuar os riscos de segurança associados às questões QBRN[48].

---

[44] Comunicação conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões intitulada «Revisão da Política Europeia de Vizinhança», de 18 de novembro de 2015, JOIN(2015) 50 final.

[45] Idem; Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões intitulada «Estratégia de alargamento da UE», 10.11.2015, COM(2015) 611 final; Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões intitulada «Aumentar o impacto da política de desenvolvimento da UE: uma Agenda para a Mudança», 13.10.2011, COM(2011) 637 final.

[46] Comunicação conjunta intitulada «Desenvolver as capacidades para promover a segurança e o desenvolvimento - Capacitar os parceiros para a prevenção e a gestão das crises», JOIN(2015)17 final.

[47] Regulamento (UE) n.º 230/2014 do Parlamento Europeu e do Conselho, de 11 de março de 2014, que cria um instrumento para a estabilidade e a paz, JO L 77 de 15.3.2014, p. 1.

[48] As áreas abrangidas incluem o controlo de fronteiras, a gestão de crises, a primeira resposta, o tráfico ilícito, o controlo das exportações de produtos de dupla utilização, a vigilância e o controlo das doenças, a investigação forense no âmbito nuclear, a recuperação pós-incidente e a proteção das instalações de alto risco. As melhores práticas adquiridas graças aos instrumentos desenvolvidos no âmbito do Plano de Ação

Por último, num espírito de abordagem global da gestão de crises, os Estados-Membros poderão utilizar os instrumentos e as missões da política comum de segurança e defesa (PCSD), independentemente ou em complemento dos instrumentos da UE, a fim de ajudar os parceiros a reforçar as suas capacidades. Poderiam ser consideradas as seguintes medidas: (i) apoio à comunicação estratégica, (ii) apoio sob a forma de aconselhamento para os principais ministérios expostos a ameaças híbridas; (iii) apoio adicional para a gestão das fronteiras em caso de emergência. Poderão ser exploradas outras sinergias entre os instrumentos da PCSD e os intervenientes nos domínios da segurança, das alfândegas e da justiça, nomeadamente as agências competentes da UE[49], a Interpol e a Força de Gendarmerie Europeia, em conformidade com os respetivos mandatos.

<u>Ação 18</u>: 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 sua resiliência 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.

5. PREVENIR E RESPONDER A SITUAÇÕES DE CRISE E RECUPERAR

Tal como indicado no ponto 3.1, a célula de fusão da UE contra as ameaças híbridas proposta pela União tem por objetivo analisar os indicadores relevantes, a fim de prevenir e reagir a ameaças híbridas e informar os decisores políticos da UE. Embora as insuficiências 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, reagir e recuperar de ameaças híbridas de uma forma rápida e coordenada.

Uma reação rápida aos eventos desencadeados pelas ameaças híbridas é fundamental. A este respeito, a facilitação de ações e das capacidades de proteção civil por parte do Centro de Coordenação de Resposta de Emergência[50] poderia constituir um mecanismo eficaz de resposta a aspetos de ameaças híbridas que exijam uma intervenção da proteção civil. Este objetivo poderia ser alcançado em coordenação com outros mecanismos de resposta e sistemas de alerta rápido da UE, em especial a sala de situação do SEAE, no que se refere aos aspetos relativos à segurança externa e a unidade «Análise Estratégica e Resposta», no que se refere à segurança interna.

A cláusula de solidariedade (artigo 222.º do TFUE) permite uma ação da União e dos seus Estados-Membros, se um Estado-Membro for alvo de um ataque terrorista ou vítima

---

QBRN da UE, tais como o Centro Europeu de Formação em Segurança Nuclear e a participação da UE no grupo de trabalho internacional sobre a vigilância das fronteiras internacionais, podem ser partilhadas com países terceiros.

[49] EUROPOL, FRONTEX, CEPOL, EUROJUST

[50] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en.

de uma catástrofe natural ou de origem humana. A ação da União para assistir o Estado-Membro é implementada mediante a aplicação da Decisão 2014/415/UE do Conselho[51]. As modalidades de coordenação no âmbito do Conselho deverão basear-se no Mecanismo Integrado da UE de Resposta Política a Situações de Crise[52]. Estas modalidades preveem que a Comissão e a Alta Representante, nos respetivos domínios de competência, identifiquem os instrumentos pertinentes da União e apresentem ao Conselho propostas de decisões sobre medidas excecionais.

O artigo 222.º do TFUE também aborda situações que envolvam assistência direta por um ou vários Estados-Membros a um Estado-Membro que seja alvo de um ataque terrorista ou vítima de uma catástrofe. A este respeito, a Decisão 2014/415/UE do Conselho não é aplicável. Tendo em conta a ambiguidade associada a atividades híbridas, a aplicabilidade possível em última instância da cláusula de solidariedade deve ser avaliada pela Comissão e pela Alta Representante (nas respetivas áreas de competência), no caso de um Estado-Membro da UE ser alvo de importantes ameaças híbridas.

Contrariamente ao artigo 222.º do TFUE, se várias ameaças híbridas graves constituírem uma agressão armada contra um Estado-Membro da UE, o artigo 42.º, n.º 7, do TUE poderia ser invocado, a fim de dar uma resposta adequada e atempada. A manifestação de ameaças híbridas graves e de grande amplitude pode igualmente exigir uma cooperação e uma coordenação reforçadas com a NATO.

Ao preparar as suas forças, os Estados-Membros são incentivados a ter em conta potenciais ameaças híbridas. Para estarem em condições de tomar decisões de forma rápida e eficaz em caso de ataque híbrido, os Estados-Membros devem organizar exercícios regulares, a nível operacional e a nível político, a fim de testar as capacidades de decisão aos níveis nacional e multinacional. O objetivo seria o de dispor de um protocolo operacional comum entre os Estados-Membros, a Comissão e a Alta Representante, definindo procedimentos eficazes a seguir em caso de ameaça híbrida, desde a fase inicial de identificação até à fase final de ataque, e de precisar o papel de cada instituição da União e de cada interveniente no processo.

Como componente importante do envolvimento da PCSD, poderia prever-se a organização de: (a) uma formação civil e militar, (b) missões de enquadramento e de aconselhamento para melhorar as capacidades em matéria de segurança e de defesa de um Estado ameaçado, (c) o planeamento de medidas de emergência, a fim de identificar sinais de ameaças híbridas e reforçar as capacidades de alerta rápido, (d) apoio à gestão do controlo das fronteiras, em caso de emergência, (e) apoio em domínios especializados, como a atenuação dos riscos QBRN e a evacuação dos não combatentes.

<u>Ação 19</u>: A Alta Representante e a Comissão, em coordenação com os Estados-Membros, estabelecerão um protocolo operacional comum e procederão a exercícios

[51] Decisão 2014/415/UE do Conselho, de 24 de junho de 2014, relativa às regras de execução da cláusula de solidariedade pela União (JO L 192 de 1.7.2014, p. 53).
[52] http://www.consilium.europa.eu/en/documents-publications/publications/2014/eu-ipcr/

regulares para melhorar a capacidade de tomada de decisões estratégicas em resposta a ameaças híbridas complexas com base nos procedimentos de gestão das crises e do mecanismo integrado de resposta política a situações de crise.

<u>Ação 20</u>: A Comissão e a Alta Representante, nos respetivos domínios de competência, analisarão a aplicabilidade e as implicações práticas dos artigos 222.º do TFUE e artigo 42.º, n.º 7, do TUE, no caso da ocorrência de ameaças híbridas graves e de grande amplitude.

<u>Ação 21</u>: A Alta Representante, em coordenação com os Estados-Membros, integrará, explorará e coordenará as capacidades de ação militar na luta contra as ameaças híbridas no âmbito da política comum de segurança e defesa.

6. INTENSIFICAR A COOPERAÇÃO COM A NATO

As ameaças híbridas representam um desafio não só para a UE, mas também para outras grandes organizações parceiras, nomeadamente a Organização das Nações Unidas (ONU), a Organização para a Segurança e a Cooperação na Europa (OSCE) e, em especial, a NATO. Uma resposta efetiva exige diálogo e coordenação, tanto a nível político como a nível operacional, entre organizações. Uma interação mais estreita entre a UE e a NATO colocaria ambas as organizações em melhores condições para se prepararem e responderem eficazmente a ameaças híbridas, de uma forma complementar e através de apoio mútuo, com base no princípio da inclusividade, respeitando simultaneamente a autonomia decisória e as regras de proteção de dados de cada organização.

As duas organizações partilham valores e enfrentam desafios semelhantes. Os Estados-Membros da UE e os aliados da NATO esperam que as respetivas organizações os apoiem, agindo rapidamente, com determinação e de forma coordenada em caso de crise ou, de preferência, para evitar o desencadear-se de uma crise. Os domínios identificados com vista a uma cooperação e coordenação mais estreitas entre a UE e a NATO incluem o conhecimento da situação, a comunicação estratégica, a cibersegurança e a prevenção e resposta a situações de crise. O diálogo informal em curso entre a UE e a NATO sobre ameaças híbridas deve ser reforçado, a fim de conduzir à sincronização das atividades das duas organizações neste domínio.

Para que as respostas da UE/NATO possam ser complementares, é importante que ambas partilhem o mesmo conhecimento da situação geral antes e durante a crise. Tal poderá ser conseguido mediante um intercâmbio periódico das análises e dos ensinamentos adquiridos, mas também através de uma ligação direta entre a célula de fusão da UE contra as ameaças híbridas e a célula da NATO para as ameaças híbridas. É igualmente importante reforçar o conhecimento mútuo dos respetivos procedimentos de gestão de crises, a fim de assegurar reações rápidas e eficazes. A resiliência pode ser reforçada assegurando uma complementaridade entre as normas fixadas para os elementos críticos das respetivas infraestruturas, bem como uma colaboração estreita em matéria de comunicação estratégica e de ciberdefesa. Exercícios conjuntos plenamente inclusivos, tanto a nível político como a nível técnico, contribuiriam para reforçar a eficácia da

capacidade de tomada de decisão das duas organizações. A procura de novas possibilidades de atividades de formação contribuiria para atingir um nível comparável de conhecimentos especializados em áreas críticas.

<u>Ação 22</u>: A Alta Representante, em coordenação com a Comissão, a prosseguirá o diálogo informal e reforçará 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 de decisão de cada organização.

7. CONCLUSÕES

A presente comunicação conjunta apresenta ações destinadas a contribuir para a luta contra as ameaças híbridas e para reforçar a resiliência a nível nacional, da UE e dos parceiros. Dado que a tónica é colocada no **aumento do conhecimento da situação**, propõe-se criar mecanismos específicos para o intercâmbio de informações com os Estados-Membros e coordenar a capacidade da UE em matéria de comunicações estratégicas. São propostas ações para **aumentar a resiliência** em áreas 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. Em cada um destes domínios, a aplicação das estratégias acordadas pela UE e pelos Estados-Membros, assim como a aplicação integral por estes da legislação em vigor, constituirão um importante primeiro passo. Outras ações mais concretas foram propostas igualmente para reforçar ainda mais este empenho.

No que respeita à **prevenção, à resposta e à recuperação no que respeita às ameaças híbridas**, é proposto examinar a possibilidade de aplicar a cláusula de solidariedade prevista no artigo 222.º do TFUE (tal como especificado na decisão correspondente) e o artigo 42.º, n.º 7, do TUE, no caso da ocorrência de ataques híbridos graves e de grande amplitude. A capacidade de tomada de decisões estratégicas poderia ser reforçada mediante a criação de um protocolo operacional comum.

Por último, é proposto **reforçar a cooperação** e a **coordenação entre a UE e a NATO** num esforço comum para fazer face a ameaças híbridas.

Na aplicação do presente quadro comum, a Alta Representante e a Comissão comprometem-se a mobilizar os instrumentos da UE relevantes ao seu dispor. É importante que a UE, juntamente com os Estados-Membros, trabalhem no sentido de reduzir os riscos associados à exposição a potenciais ameaças híbridas por parte de intervenientes estatais e não-estatais.