COMISSÃO
EUROPEIA

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

Bruxelas, 13.6.2018
JOIN(2018) 16 final

COMUNICAÇÃO CONJUNTA AO PARLAMENTO EUROPEU, AO CONSELHO EUROPEU E AO CONSELHO

Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas

1. INTRODUÇÃO

As atividades híbridas de intervenientes estatais e não estatais continuam a representar uma ameaça grave e premente para a UE e os Estados-Membros. Multiplicam-se as tentativas de desestabilização dos países por meio da erosão da confiança pública nas instituições governamentais e do ataque aos valores fundamentais das sociedades. As nossas sociedades enfrentam um importante desafio colocado por aqueles que pretendem prejudicar a UE e os Estados-Membros através de ciberataques que perturbam a economia e os serviços públicos, campanhas de desinformação específicas e ações militares hostis.

As campanhas híbridas são multidimensionais, combinando medidas coercivas e subversivas, ao utilizarem táticas e instrumentos (diplomáticos, militares, económicos e tecnológicos) convencionais e não convencionais para desestabilizar a parte contrária. Essas campanhas são concebidas de forma a serem difíceis de detetar ou de atribuir e podem ser utilizadas por intervenientes estatais e não estatais. O atentado com um agente neurotóxico em Salisbury, em março último[1], sublinhou ainda mais a versatilidade das ameaças híbridas e a multiplicidade das táticas atualmente disponíveis. Em resposta, o Conselho Europeu[2] realçou a necessidade de reforçar a capacidade da UE e dos Estados-Membros de deteção, prevenção e resposta a ameaças híbridas em áreas como a cibernética, a comunicação estratégica e a contrainformação. Além disso, chamou especialmente a atenção para a necessidade de uma capacidade de resiliência face a ameaças químicas, biológicas, radiológicas e nucleares.

As ameaças colocadas por armas não convencionais pertencem a uma categoria própria devido à potencial amplitude dos danos que podem causar. Além de ser difícil detetá-las e saber a quem pertencem, é também complicado fazer-lhes face. As ameaças químicas, biológicas, radiológicas e nucleares, que vão além das ameaças híbridas e incluem também as ameaças terroristas, constituem também uma preocupação geral da comunidade internacional[3], em especial no que diz respeito ao risco crescente de proliferação, tanto a nível geográfico como para intervenientes não estatais.

O reforço da resiliência a essas ameaças e o reforço das capacidades são principalmente da competência dos Estados-Membros. No entanto, as instituições da UE já tomaram várias medidas para ajudar a reforçar os esforços nacionais. Neste âmbito incluem-se os trabalhos em estreita colaboração com outros intervenientes internacionais, nomeadamente a Organização do Tratado do Atlântico Norte (OTAN)[4], os quais poderão aprofundar o apoio aos Estados-Membros em domínios como a resposta rápida[5].

A presente comunicação conjunta responde ao convite do Conselho Europeu no sentido de fazer avançar esses trabalhos. Por conseguinte, faz parte de um pacote mais amplo que

---

1 No referente ao atentado de Salisbury, o Conselho Europeu concordou, em 22 de março de 2018, com a avaliação do governo do Reino Unido segunda a qual é muito provável que a Federação da Rússia seja responsável e não exista nenhuma outra explicação plausível.

2 Conclusões do Conselho Europeu de março de 2018.

3 Incluindo pelo Conselho de Segurança das Nações Unidas, Resolução S/RES/2325 (2016), de 14 de dezembro de 2016.

4 A luta contra as ameaças híbridas é um dos sete domínios de cooperação com a Organização do Tratado do Atlântico Norte previstos na declaração conjunta assinada em Varsóvia em julho de 2016 pelo Presidente do Conselho Europeu, pelo Presidente da Comissão Europeia e pelo Secretário-Geral da Organização do Tratado do Atlântico Norte.

5 Na cimeira de Charlevoix, em junho de 2018, o G7 acordou também em desenvolver um Mecanismo de Resposta Rápida do G7 para enfrentar as ameaças à democracia: https://g7.gc.ca/en/official-documents/charlevoix-commitment-defending-democracy-from-foreign-threats/

inclui igualmente o mais recente relatório de progresso da União da Segurança[6], que faz um balanço e apresenta as próximas etapas da aplicação do plano de ação de outubro de 2017[7] em matéria de ameaças químicas, biológicas, radiológicas e nucleares, bem como o segundo relatório de progresso[8] sobre a execução das 22 ações do quadro comum em matéria de luta contra as ameaças híbridas: uma resposta da União Europeia[9].

2. A RESPOSTA DA UNIÃO EUROPEIA

A Comissão e a Alta Representante envidaram esforços contínuos para reforçar as capacidades da UE e apoiar eficazmente os Estados-Membros na luta contra as ameaças híbridas e as ameaças químicas, biológicas, radiológicas e nucleares. São já visíveis resultados concretos em domínios como as comunicações estratégicas, o conhecimento da situação, o reforço da preparação e da resiliência e o reforço da capacidade de resposta às crises.

O grupo de trabalho «East StratCom», criado após o Conselho Europeu de março de 2015, liderou os trabalhos em matéria de previsão, seguimento e combate da desinformação proveniente de fontes estrangeiras. As análises especializadas e os resultados públicos[10] aumentaram significativamente a sensibilização para o impacto da desinformação russa. Ao longo dos últimos dois anos, foram revelados mais de 4000 casos individuais de desinformação, muitos dos quais deliberadamente dirigidos contra a Europa. Os trabalhos do grupo de trabalho «East StratCom» também se centraram na melhoria da prestação de comunicações positivas, com uma maior sensibilização nos países da vizinhança oriental. Na sequência deste êxito, foram criados mais dois grupos de trabalho com uma incidência geográfica distinta: um grupo de trabalho para os Balcãs Ocidentais e um grupo de trabalho Sul específico para o mundo árabe.

Foram tomadas medidas importantes para reforçar as estruturas necessárias, com vista a melhorar o conhecimento da situação e a apoiar a tomada de decisões. A Célula de Fusão contra as Ameaças Híbridas foi criada, em 2016, no âmbito do Centro de Situação e de Informações do Serviço Europeu para a Ação Externa em 2016. A Célula de Fusão da UE recebe e analisa informações classificadas e de fontes abertas sobre ameaças híbridas provenientes de diferentes partes interessadas. Até à data, mais de 100 avaliações e documentos de informação, partilhados a nível da UE e entre os Estados-Membros, apoiam a tomada de decisões da UE. A Célula de Fusão da UE contra as Ameaças Híbridas mantém uma relação de trabalho estreita com o Centro de Excelência Europeu de Luta contra as Ameaças Híbridas em Helsínquia. Criado em abril de 2017 para promover o diálogo estratégico e desenvolver atividades de investigação e análise sobre ameaças híbridas, o Centro de Excelência aumentou o número de membros para 16 países[11] e beneficia de apoio contínuo por parte da UE.

---

6 Décimo quinto relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz, COM(2018) 470 final.

7 COM(2017) 610 final.

8 Relatório Conjunto sobre a execução do quadro comum em matéria de luta contra as ameaças híbridas (julho de 2017 - julho de 2018), JOIN(2018) 14.

9 JOIN(2016) 18 final.

10 Ver www.euvsdisinfo.eu

11 Dos atuais 16 membros, 14 são Estados-Membros da UE: Alemanha, Dinamarca, Espanha, Estónia, Finlândia, França, Itália, Letónia, Lituânia, Países Baixos, Polónia, Reino Unido, República Checa e Suécia. A iniciativa para a sua criação deriva do quadro comum em matéria de luta contra as ameaças híbridas. Além disso, o Centro tem sido ativamente apoiado pela UE e pela Organização do Tratado do Atlântico Norte no âmbito da sua cooperação.

Foram igualmente dados passos importantes para o reforço da preparação e da resiliência, em especial contra as ameaças químicas, biológicas, radiológicas e nucleares. Nos últimos seis meses, foram tomadas medidas importantes para a identificação de lacunas na preparação para incidentes de segurança químicos, biológicos, radiológicos ou nucleares, nomeadamente em termos de capacidade de deteção para ajudar a prevenir ataques químicos, biológicos, radiológicos e nucleares. Por iniciativa da Comissão, um consórcio de peritos nacionais realizou uma análise das lacunas no equipamento de deteção para diferentes tipos de cenários de ameaças químicas, biológicas, radiológicas e nucleares. O relatório de análise das lacunas foi partilhado com os Estados-Membros, permitindo-lhes tomar decisões fundamentadas sobre estratégias de deteção e tomar medidas operacionais para resolver as lacunas identificadas.

Este trabalho foi apoiado através de exercícios que testam o grau de progresso. O Exercício Coordenado e Paralelo para 2017 (PACE17) com a Organização do Tratado do Atlântico Norte permitiu uma verificação pormenorizada das capacidades de resposta da UE a crises híbridas em grande escala. Sem precedentes em termos de âmbito de aplicação, o exercício colocou à prova não só o «protocolo de atuação conjunta da UE para a luta contra as ameaças híbridas», os diferentes mecanismos de resposta da UE e a respetiva capacidade de interagir eficazmente entre si, mas também a forma como a resposta da UE às ameaças híbridas interagiu com a ação da Organização do Tratado do Atlântico Norte. Está também a ser planeado um exercício para 2018, com a ambição não só de este tipo de exercícios passarem a ser uma prática anual como também de ajudar os Estados-Membros a reforçar a capacidade de resposta a crises híbridas.

Estas medidas concretas ilustram a forma como os quadros estratégicos estabelecidos pela UE estão a produzir resultados. Com efeito, nos últimos dois anos, foram criados vários quadros para orientar e a centrar os trabalhos da UE.

O *quadro comum em matéria de luta contra as ameaças híbridas: uma resposta da União Europeia*[12] de abril de 2016 incentivou uma abordagem ao nível de todas as administrações, com 22 áreas de atuação, para ajudar na luta contra as **ameaças híbridas** e reforçar a resiliência da UE e dos Estados-Membros, bem como a resiliência dos parceiros internacionais. A maioria das ações definidas no quadro comum centram-se na melhoria do conhecimento da situação e no reforço da resiliência, com uma melhor capacidade de resposta. As ações incluem o reforço, a nível da UE, da capacidade de análise das informações a fim de reforçar a proteção de infraestruturas críticas e a cibersegurança, assim como a luta contra a radicalização e o extremismo violento. As ciberameaças e os ciberataques encontram-se também no âmago do quadro comum. O segundo relatório de progresso sobre a execução do quadro comum, adotado em paralelo à presente comunicação conjunta, demonstra progressos concretos nestas ações e confirma o reforço e o aprofundamento dos esforços da UE para lutar contra as ameaças híbridas[13].

No que diz respeito à **cibersegurança**, um marco importante foi o dia 9 de maio de 2018, prazo para a transposição, por todos os Estados-Membros, do primeiro conjunto de regras juridicamente vinculativas em toda a UE no domínio da cibersegurança, definidas na diretiva relativa à segurança das redes e dos sistemas de informação. Trata-se de uma componente importante da abordagem mais ampla estabelecida na *comunicação conjunta sobre a resiliência, a dissuasão e a defesa*: *criação de uma cibersegurança sólida na Europa*[14] de setembro de 2017, com amplas medidas concretas para dar um forte impulso às capacidades e estruturas de cibersegurança da UE. Estas medidas têm por principal objetivo o reforço da resiliência da UE aos ciberataques e o reforço da capacidade de

[13] Em relação ao primeiro relatório de execução (julho de 2017): JOIN(2017) 30 final.
[14] JOIN(2017) 450 final.

cibersegurança da UE; uma resposta eficaz do direito penal; e o reforço da estabilidade global através da cooperação internacional. A comunicação foi também acompanhada por uma proposta legislativa em matéria de cibersegurança, cujo objetivo é reforçar o apoio a nível da UE[15], e completada por um conjunto de propostas que devem ainda ser objeto de execução (ver infra).

A **desinformação** prejudica as nossas democracias, uma vez que impede os cidadãos de tomar decisões fundamentadas e de participar no processo democrático. A Internet aumentou de modo significativo a quantidade e variedade de notícias à disposição dos cidadãos. Porém, as novas tecnologias podem ser utilizadas para divulgar desinformações a uma escala e um ritmo sem precedentes, com um direcionamento específico, de modo a semear a desconfiança e criar tensões sociais. A *comunicação sobre a luta contra a desinformação em linha: uma abordagem europeia*[16] da Comissão estabeleceu uma abordagem europeia em resposta ao problema da desinformação, exortando as diferentes partes interessadas, em particular as plataformas em linha, mas também as empresas de meios de comunicação, a tomar medidas. Estas ações abrangem uma vasta gama de domínios pertinentes, incluindo uma maior transparência; credibilidade e responsabilidade das plataformas em linha; processos eleitorais mais seguros e resilientes; promoção da educação e da literacia mediática; apoio ao jornalismo de qualidade; e luta contra a desinformação através de uma comunicação estratégica. As primeiras medidas concretas incluem um código de boas práticas em matéria de desinformação, a ser elaborado por um Fórum Multilateral Europeu sobre a Desinformação e uma rede de verificadores de factos a estabelecer antes do verão. A primeira reunião do Fórum Multilateral Europeu sobre a Desinformação realizou-se em 29 de maio de 2018, tendo sido aprovadas as medidas necessárias para adotar o código em julho de 2018. A Comissão avaliará, até ao final de 2018, os progressos realizados na resolução do problema e decidirá se é necessária uma intervenção suplementar neste domínio. As atividades previstas serão coerentes com as atividades do grupo de trabalho «East StratCom» e complementares.

No que se refere aos riscos **químicos, biológicos, radiológicos e nucleares**, o *plano de ação*[17] da Comissão, de outubro de 2017, propôs 23 ações práticas e medidas destinadas a melhorar a proteção dos cidadãos e das infraestruturas contra essas ameaças, nomeadamente através de uma cooperação mais estreita entre a UE e os Estados-Membros, bem como com a Organização do Tratado do Atlântico Norte. Como parte das medidas da União da Segurança para melhorar a proteção e a resiliência contra o terrorismo, o plano de ação seguiu uma abordagem preventiva baseada no princípio segundo o qual os riscos químicos, biológicos, radiológicos e nucleares apresentam um reduzido grau de probabilidade, mas, em caso de ataque, têm um impacto elevado e duradouro. Entretanto, o atentado de Salisbury e a crescente preocupação quanto ao interesse e à capacidade dos terroristas no referente à utilização de materiais químicos, biológicos, radiológicos e nucleares, tanto na UE como fora da UE[18], demonstraram que a ameaça representada por substâncias nucleares, biológicas, radiológicas e químicas é real. Torna-se, portanto, mais do que nunca, urgente aplicar integralmente o plano de ação, que contempla «todos os riscos» e se centra em quatro objetivos: redução do acesso a materiais químicos, biológicos, radiológicos e nucleares; garantia de uma preparação e resposta mais sólida a incidentes de segurança químicos, biológicos, radiológicos e nucleares; estabelecimento de relações internas/externas mais fortes em termos de segurança química, biológica, radiológica e nuclear com os principais parceiros da UE a

15 COM (2017) 477, ver infra.
16 COM(2018) 236 final.
17 COM(2017) 610 final.
18 Europol, Relatório sobre a situação e as tendências do terrorismo na UE (TE-SAT) 2017, p. 16, disponível em: www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf. Ver também as declarações do diretor-geral da OPAQ: www.globaltimes.cn/content/1044644.shtml.

nível regional e internacional; e melhoria dos conhecimentos sobre os riscos químicos, biológicos, radiológicos e nucleares. No mais recente relatório sobre os progressos da União da Segurança, adotado em paralelo à presente comunicação conjunta, são fornecidas informações pormenorizadas sobre os progressos concretos realizados na aplicação do plano de ação.

Por último, com vista a aumentar a eficácia dos esforços no sentido de lutar contra as ameaças híbridas e reforçar a mensagem de unidade entre os Estados-Membros da UE e os Aliados da Organização do Tratado do Atlântico Norte (OTAN), a cooperação contra as ameaças híbridas foi definida como um dos principais domínios de **cooperação entre a UE e a OTAN**, tal como previsto na *declaração conjunta de Varsóvia*[19] de julho de 2016. Cerca de um terço de todas as atuais propostas comuns de cooperação incide nas ameaças híbridas[20]. Os exercícios e o «protocolo de atuação conjunta da UE»[21] acima descritos estão a ser desenvolvidos com uma cooperação aprofundada este ano.

3. REFORÇO DA RESPOSTA ÀS AMEAÇAS CRESCENTES

3.1. Conhecimento da situação: maior capacidade de deteção das ameaças híbridas

Os esforços para combater e responder às ameaças híbridas devem ser apoiados por uma capacidade de deteção precoce de fontes e atividades híbridas maliciosas, internas e externas, e de conhecimento das eventuais ligações entre acontecimentos muitas vezes aparentemente não relacionados. Para o efeito, é essencial utilizar todos os fluxos de dados disponíveis, incluindo informações de fontes abertas.

A Célula de Fusão da UE contra as Ameaças Híbridas, criada no Serviço Europeu para a Ação Externa como um ponto de convergência único a nível da UE para a análise de ameaças híbridas, é um recurso importante, mas é necessário que possua os conhecimentos especializados necessários para contemplar todo o espetro das ameaças híbridas, incluindo nos domínios químico, biológico, radiológico e nuclear, bem como da contrainformação. O alargamento dos conhecimentos especializados aumentaria o apoio a qualquer futura resposta em situação de crise na UE, oferecendo resultados da análise de informações civis e militares mais completos nestes domínios específicos. Tal poderá ser apoiado por medidas dos Estados-Membros destinadas a aumentar as contribuições dos seus serviços nacionais de informações para a Célula de Fusão contra as Ameaças Híbridas e a reforçar ainda mais a capacidade da rede estabelecida de pontos de contacto nacionais para a Célula de Fusão contra as Ameaças Híbridas de fornecimento e tratamento de informações urgentes. Outra medida seria a análise, por parte dos Estados-Membros, do aumento das contribuições dos seus serviços nacionais de informações para o Centro de Situação e de Informações da UE (INTCEN), de modo a permitir uma análise mais aprofundada das potenciais ameaças.

---

19 A declaração assinada pelo Presidente Jean-Claude Juncker, pelo Presidente Donald Tusk e pelo Secretário-Geral da OTAN, Jens Stoltenberg, constitui a base atual para a cooperação entre a UE e a OTAN.

20 15283/16 e 14802/17.

21 Documento de trabalho SWD(2016) 227 final.

Próximas etapas

- A Alta Representante alargará a Célula de Fusão da UE contra as Ameaças Híbridas com componentes analíticos cibernéticos especializados nos domínios químico, biológico, radiológico e nuclear, bem como da contrainformação. Os Estados-Membros são convidados a intensificar as contribuições de informações para a Célula de Fusão da UE contra as Ameaças Híbridas para a análise das ameaças híbridas existentes e emergentes.

- A Comissão, em coordenação com a Alta Representante, concluirá os trabalhos sobre indicadores de vulnerabilidade para permitir aos Estados-Membros avaliarem melhor o potencial das ameaças híbridas em diferentes setores. Além disso, esses trabalhos apoiarão a análise de tendências híbridas da UE.

3.2. **Ações reforçadas contra as ameaças químicas, biológicas, radiológicas e nucleares**

O plano de ação de outubro de 2017 contra riscos de segurança química, biológica, radiológica e nuclear estabelece o quadro de ação para reforçar a preparação, a resiliência e a coordenação a nível da UE. As ações aí definidas abrangem um leque de medidas destinadas a apoiar os Estados-Membros através da partilha de conhecimentos especializados e do desenvolvimento de capacidades conjuntas, do intercâmbio de conhecimentos e melhores práticas e do reforço da cooperação operacional. Os Estados-Membros e a Comissão têm de trabalhar em conjunto para implementar plenamente o plano de ação com caráter de urgência. Além disso, com base nos progressos já alcançados em termos de análise das lacunas existentes nas capacidades de deteção e no intercâmbio de melhores práticas no recém-criado Grupo Consultivo de Segurança em matéria de ameaças químicas, biológicas, radiológicas e nucleares, a União deverá agora tomar medidas suplementares para resolver a questão do desenvolvimento e da evolução das ameaças. Tal aplica-se, em especial, às ameaças químicas. Seguindo o exemplo dos trabalhos para limitar o acesso a precursores de explosivos[22], a UE necessita de tomar rapidamente medidas operacionais para melhor controlar o acesso a materiais químicos de elevado risco e otimizar a capacidade de deteção desses materiais o mais rapidamente possível. Além disso, os Estados-Membros deverão considerar a realização de novos exercícios de mapeamento e análises das lacunas a nível da UE, por exemplo, no que se refere aos recursos e às abordagens de descontaminação e resiliência a ameaças químicas, biológicas, radiológicas e nucleares. Para gerir as consequências de um eventual ataque químico, biológico, radiológico ou nuclear e estar preparados, é necessário reforçar a cooperação e coordenação entre os Estados-Membros, nomeadamente entre as autoridades de proteção civil. O Mecanismo de Proteção Civil da União pode desempenhar um papel essencial neste processo de reforço da capacidade coletiva de preparação e resposta.

A cooperação internacional é também um elemento importante nesses trabalhos e a UE pode desenvolver relações com os Centros de Excelência regionais em matéria de ameaças

[22] Como parte dos trabalhos na União da Segurança para encerrar o espaço em que os terroristas e os criminosos operam, a Comissão tomou medidas firmes para reduzir o acesso a precursores de explosivos que podem ser utilizados indevidamente para fabricar explosivos «caseiros». Em outubro de 2017, a Comissão apresentou uma recomendação que estabelece medidas imediatas para prevenir a utilização indevida de precursores de explosivos com base nas regras existentes (Recomendação C(2017) 6950 final). Neste contexto, a Comissão adotou, em abril de 2018, uma proposta de revisão e reforço do atual Regulamento n.º 98/2013 relativo à comercialização e utilização de precursores de explosivos (COM(2018) 209 final).

químicas, biológicas, radiológicas e nucleares, nomeadamente no que diz respeito à procura de sinergias com a Organização do Tratado do Atlântico Norte, e programas de prevenção, preparação e resposta a catástrofes naturais ou provocadas pelo homem para o sul e o leste[23].

Próximas etapas

- A UE deverá estudar a adoção de medidas para respeitar regras e normas internacionais contra a utilização de armas químicas, nomeadamente através de um eventual regime de sanções específicas da UE para armas químicas.
- De modo a fazer avançar o plano de ação em matéria de ameaças químicas, biológicas, radiológicas e nucleares, a Comissão trabalhará com os Estados-Membros no sentido de concluir as medidas seguintes até ao final de 2018:
  - elaborar uma lista de substâncias químicas que representam uma ameaça específica, como base para ações operacionais para reduzir a respetiva acessibilidade;
  - estabelecer um diálogo com intervenientes privados da cadeia de abastecimento com vista a um trabalho conjunto para responder a ameaças em evolução de substâncias químicas que podem ser utilizadas como precursores;
  - acelerar uma revisão dos cenários de ameaça e uma análise dos métodos de deteção existentes, a fim de melhorar a deteção de ameaças químicas, com vista ao desenvolvimento de orientações operacionais para que os Estados-Membros reforcem as suas capacidades de deteção.
- Os Estados-Membros devem estabelecer inventários das existências em termos de contramedidas médicas essenciais, incluindo das capacidades em termos de laboratórios, tratamentos, etc. A Comissão colaborará com os Estados-Membros para verificar regularmente em que medida estas existências estão disponíveis em toda a UE, a fim de permitir um acesso e utilização rápida em caso de ataque.

3.3. **Comunicação estratégica: divulgação coerente de informações**

Um importante desafio no que respeita às ameaças híbridas consiste na sensibilização e educação do público em geral para distinguir entre informação e desinformação. Com base na experiência do grupo de trabalho «East StratCom», da Célula de Fusão da UE contra as Ameaças Híbridas e do Centro de Excelência Europeu de Luta contra as Ameaças Híbridas, bem como noutros esforços envidados pela Comissão[24], a Comissão e a Alta Representante irão desenvolver e profissionalizar ainda mais as capacidades da UE em matéria de comunicações estratégicas, assegurando uma interação e uma coerência sistemática entre as estruturas existentes. Este aspeto será ainda alargado a outras

[23] Nos países da vizinhança oriental e meridional, organizam-se exercícios e formações de proteção civil no âmbito dos programas regionais de prevenção, preparação e resposta a catástrofes naturais ou provocadas pelo homem.

[24] As Representações da Comissão, por exemplo, estão também ativas no domínio da verificação de factos e da desmistificação. Várias Representações desenvolveram instrumentos adaptados às condições locais como, por exemplo, *Les Décodeurs de l'Europe* em França, *UE Vero Falso* em Itália, um concurso público de desenhos animados de desmistificadores da UE na Áustria, uma série de desenhos animados semelhante na Roménia e *Euromyths A-Z* da Representação do Reino Unido. Estão já na forja mais projetos semelhantes aos anteriormente referidos.

instituições da UE e dos Estados-Membros, nomeadamente mediante a utilização da anunciada plataforma em linha segura relativa à desinformação.

Uma melhor coordenação e cooperação em matéria de comunicação estratégica em todas as instituições da UE, com os Estados-Membros e com os parceiros e organizações internacionais, é essencial e exige preparação e prática antes da reação a crises em tempo real.

Os períodos eleitorais revelaram-se um alvo particularmente estratégico e sensível para os ataques cibernéticos e a evasão em linha de proteções e regras convencionais («fora de linha»), tais como períodos de silêncio, regras de financiamento transparente e igualdade de tratamento dos candidatos. Tal incluiu ataques contra infraestruturas e sistemas informáticos de campanha eleitoral, bem como campanhas de desinformação em linha e em massa por motivos políticos e ciberataques por países terceiros com o objetivo de desacreditar e retirar a legitimidade de eleições democráticas. Várias vertentes de trabalho estão a ser desenvolvidas a nível da UE para aumentar a sensibilização nos Estados-Membros na preparação e na resposta a estas ameaças em evolução. No Conselho, as autoridades de cibersegurança dos Estados-Membros[25] emitirão orientações voluntárias e definirão boas práticas comuns para abordar a cibersegurança da tecnologia eleitoral ao longo do ciclo de vida das eleições. Tal inclui sistemas de informação e soluções de TIC utilizados para registar os eleitores e os candidatos, reunir e contar os votos e divulgar os resultados, bem como sistemas auxiliares diretamente relacionados com a legitimidade dos resultados das eleições.

É igualmente necessário assegurar informações rápidas, fiáveis e coerentes para o público em geral em caso de ataques híbridos. Qualquer incidente químico, biológico, radiológico ou nuclear ou evento com impacto semelhante provoca protestos públicos, uma vez que os cidadãos exigem respostas rápidas. As mensagens estratégicas desempenham um papel fundamental, nomeadamente entre as organizações internacionais que podem adotar separadamente os seus planos de resposta.

Próximas etapas

- O Serviço Europeu para a Ação Externa e a Comissão irão trabalhar em conjunto no âmbito das respetivas competências para estabelecer uma cooperação mais estruturada em matéria de comunicações estratégicas, com vista a combater a desinformação proveniente de dentro e de fora da UE e a desencorajar a produção de desinformação hostil e interferências híbridas por parte de governos estrangeiros.

- A Comissão organizará eventos de alto nível no outono com os Estados-Membros e as partes interessadas, incluindo um colóquio sobre os direitos fundamentais dedicado à democracia, a fim de promover melhores práticas e orientações quanto ao modo de prevenção, atenuação e resposta a ciberameaças, assim como às ameaças da desinformação no quadro de eleições.

- A Alta Representante e a Comissão examinarão em que medida é possível dar um maior apoio, em termos de ferramentas e recursos, ao trabalho efetuado pelos três Grupos de Trabalho «StratCom», de modo a assegurar que os esforços da UE são suficientemente ajustados para abordar a complexidade das campanhas de desinformação realizadas por intervenientes hostis.

[25] No âmbito do Grupo de Cooperação instituído ao abrigo da diretiva relativa à segurança das redes e dos sistemas de informação.

3.4. **Reforço da resiliência e da dissuasão no setor da cibersegurança**

A cibersegurança é essencial tanto para a nossa prosperidade como para a nossa segurança. Atendendo a que a vida quotidiana e as nossas economias dependem cada vez mais de tecnologias digitais, vamos ficando gradualmente mais expostos.

A cibersegurança eficaz na atual UE é prejudicada pela falta de investimento e pela falta de coordenação. A UE está agora a tentar resolver esta questão mediante o desenvolvimento de capacidades através de medidas de apoio, maior coordenação e novas estruturas para o avanço da tecnologia e da implementação em matéria de cibersegurança[26]. A diretiva relativa à segurança das redes e dos sistemas de informação[27] estabeleceu um nível mínimo de segurança das redes e dos sistemas de informação em toda a União. A sua aplicação integral por todos os Estados-Membros é essencial para reforçar a ciber-resiliência: tal constitui uma primeira etapa fundamental. O Regulamento Geral sobre a Proteção de Dados introduz uma obrigação de notificação de uma violação dos dados pessoais à autoridade de controlo competente. Outras medidas importantes incluem o reforço e a modernização da Agência da União Europeia para a Cibersegurança e um quadro de certificação da UE para os produtos e serviços de TIC[28], de modo a reforçar a confiança dos consumidores. Encontram-se igualmente em curso trabalhos de apoio à rede de centros de competência dos Estados-Membros para estimular o desenvolvimento e a implementação de soluções de cibersegurança e completar os esforços de desenvolvimento de capacidades neste domínio a nível da UE e a nível nacional. Tal terá em conta os trabalhos do Programa para a Europa Digital, apresentado pela Comissão em 6 de junho[29], que confere uma nova prioridade ao investimento da UE em matéria de cibersegurança.

Simultaneamente, uma recomendação para uma resposta coordenada a crises e incidentes de cibersegurança em larga escala (o «plano»)[30] define a forma como a cooperação deverá funcionar entre os Estados-Membros e vários intervenientes da UE na resposta a ciberataques transfronteiriços em grande escala. A recomendação sublinhou o papel fundamental do conhecimento da situação para uma coordenação eficaz a nível técnico, operacional e estratégico/político. O Grupo de Cooperação instituído ao abrigo da diretiva relativa à segurança das redes e dos sistemas de informação está também a trabalhar no sentido de melhorar o intercâmbio e a partilha de informações entre as partes relevantes, desenvolvendo uma taxonomia comum para descrever um incidente. Esta abordagem será testada nos próximos exercícios. A análise estratégica de ciberameaças atuais e emergentes, com base nas contribuições dos serviços de informações dos Estados-Membros, é assegurada pela Célula de Fusão da UE contra as Ameaças Híbridas.

O quadro para uma resposta diplomática conjunta da UE às ciberatividades maliciosas («instrumentos de ciberdiplomacia») constituiu um importante passo em frente em termos operacionais, estabelecendo as medidas no âmbito da política externa e de segurança comum, incluindo medidas restritivas, que podem ser utilizadas para reforçar a resposta da UE a atividades que lesem os seus interesses políticos, económicos e de segurança. Quanto mais aquele for plenamente utilizado pelos Estados-Membros, mais funcionará

---

[26] No âmbito do reforço da inovação nas regiões da Europa, foi lançada, em dezembro de 2017, uma nova ação-piloto inter-regional, que reúne várias regiões da UE, com vista a intensificar os trabalhos no domínio da cibersegurança .

[27] 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.

[28] COM (2017) 477.

[29] Proposta de regulamento que cria o programa Europa Digital para o período 2021-2027, COM(2018) 434.

[30] C(2017) 6100.

como um dissuasor eficaz. Em abril, o Conselho dos Negócios Estrangeiros adotou conclusões sobre as ciberatividades maliciosas que condenaram firmemente a utilização maliciosa das tecnologias de informação e comunicação, incluindo os ataques NotPetya e WannaCry, que causaram danos e prejuízos económicos importantes na UE e não só.

A UE e os seus Estados-Membros têm de melhorar a capacidade de atribuição dos ciberataques, sobretudo através de uma maior partilha de informações. A atribuição dissuadiria potenciais agressores e aumentaria a possibilidade de os autores serem devidamente responsabilizados. O aumento da dissuasão é um objetivo-chave da abordagem estratégica da Comissão para o reforço da cibersegurança. As recentes propostas da Comissão destinadas a melhorar a recolha transfronteiras de elementos de prova eletrónicos em processos penais também aumentariam significativamente a capacidade de aplicação da lei para investigar e intentar ações penais contra a cibercriminalidade.

Uma ciber-resiliência forte requer uma abordagem coletiva e global. Para tal, são precisas estruturas mais robustas e eficazes para promover a cibersegurança e responder aos ciberataques nos Estados-Membros, mas também nas próprias instituições, agências, delegações, missões e atividades da UE: a ausência de uma rede de comunicações segura e conjunta a nível das instituições europeias constitui uma lacuna importante. É necessário sensibilizar mais as instituições da UE e o pessoal destas instituições para as questões de cibersegurança por meio de uma maior cultura da segurança e do reforço das formações neste domínio.

Próximas etapas

- O Parlamento Europeu e o Conselho deverão acelerar os trabalhos para concluir as negociações sobre as propostas em matéria de cibersegurança, mediante acordo até ao final do presente ano, e aprovar rapidamente a legislação proposta em matéria de recolha de elementos de provas eletrónicos.

- A Comissão e a Alta Representante colaborarão estreitamente com os Estados-Membros para promover os aspetos cibernéticos, à escala da UE, dos mecanismos de resposta e gestão de crises. Os Estados-Membros são convidados a continuar os seus trabalhos relativos à atribuição das responsabilidades por ciberataques e à utilização prática dos instrumentos de ciberdiplomacia com vista a reforçar a resposta política aos ciberataques.

- Em resposta à necessidade de reforçar as nossas capacidades de ciberdefesa, está a ser criada uma plataforma de ensino e formação específica para ajudar a coordenar as oportunidades de formação em ciberdefesa oferecidas pelos Estados-Membros. Além disso, serão procuradas sinergias com esforços semelhantes da Organização do Tratado do Atlântico Norte.

3.5. **Reforço da resiliência a atividades de informações hostis**

A luta contra as atividades de informações hostis exige, em primeiro lugar, uma coordenação reforçada e eficaz entre os Estados-Membros, em conformidade com as regras e os acordos nacionais e da UE pertinentes. Contudo, é também imperativo reforçar as capacidades das instituições da UE para lutar contra a ameaça crescente dessas atividades especificamente orientadas para as instituições e criar uma cultura de sensibilização para a segurança, apoiada por uma melhor formação e segurança física.

Além disso, as instituições poderão trabalhar com os Estados-Membros no sentido de desenvolver um sistema de acreditação da UE mais sólido. Esse sistema basear-se-ia numa comunicação proativa, que permita uma melhor sensibilização dos possíveis intervenientes hostis, nomeadamente aqueles já identificados pelos Estados-Membros, entre os Estados-Membros e as instituições.

A coordenação entre os Estados-Membros e entre os Estados-Membros e outras organizações internacionais pertinentes, em particular a Organização do Tratado do Atlântico Norte, ajudaria a conseguir uma situação de vantagem para a contrainformação que permita combater as atividades hostis na UE. Um domínio que beneficiaria de uma maior coordenação entre os Estados-Membros seria, por exemplo, o escrutínio dos investimentos, com base numa proposta de regulamento[31] apresentada pela Comissão em setembro de 2017 relativa ao escrutínio, pelos Estados-Membros, dos investimentos estrangeiros diretos por motivos de segurança ou de ordem pública. O reforço da coordenação entre os Estados-Membros afigura-se também muito importante para escrutinar as transações financeiras, uma vez que os serviços de informações hostis financiam cada vez mais as medidas ativas contra a UE por meio de planos financeiros elaborados.

Próximas etapas

- O Serviço Europeu para a Ação Externa e a Comissão irão implementar melhores medidas práticas para manter e desenvolver a capacidade da UE de interação com os Estados-Membros, com vista a combater atividades de informações hostis especificamente orientadas para as instituições.
- A Célula de Fusão da UE contra as Ameaças Híbridas reforçada será complementada por conhecimentos especializados de contrainformação para análises pormenorizadas e reuniões de informação sobre a natureza das atividades de informações hostis provavelmente contra as pessoas e as instituições.
- O Parlamento Europeu e o Conselho devem acelerar os trabalhos para concluir os debates sobre a proposta relativa ao escrutínio dos investimentos até ao final do ano.

4. CONCLUSÃO

As ameaças híbridas e as ameaças químicas, biológicas, radiológicas e nucleares fazem parte das principais preocupações da UE. O incidente em março no Reino Unido sublinhou o amplo espetro da guerra híbrida e a necessidade específica de resiliência perante as ameaças químicas, biológicas, radiológicas e nucleares.

A Comissão e a Alta Representante adotaram e propuseram um conjunto de iniciativas para responder aos desafios colocados pelas ameaças híbridas. A Comissão está também a acelerar a aplicação do plano de ação de 2017 a fim de reforçar a preparação contra riscos de segurança químicos, biológicos, radiológicos e nucleares.

A presente comunicação conjunta tem por objetivo informar o Conselho Europeu dos trabalhos já em curso e identificar domínios em que a ação deve ser intensificada, a fim de

[31] Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece um quadro para a análise de investimentos diretos estrangeiros na União Europeia, COM(2017) 487.

aprofundar e reforçar ainda mais a contribuição fundamental da UE para a resposta a estas ameaças. Por conseguinte, cabe agora aos Estados-Membros, à Comissão e à Alta Representante garantir que é dado um seguimento rápido.