Conselho da
União Europeia

Bruxelas, 18 de outubro de 2023
(OR. en)

14394/23

COSI 181
CRIMORG 139
ENFOPOL 433
CT 156
COTER 186
AVIATION 194
JAI 1334

NOTA DE ENVIO

de:	Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora
data de receção:	18 de outubro de 2023
para:	Thérèse BLANCHET, secretária-geral do Conselho da União Europeia
n.° doc. Com.:	COM(2023) 659 final
Assunto:	COMUNICAÇÃO DA COMISSÃO AO CONSELHO E AO PARLAMENTO EUROPEU sobre o combate às potenciais ameaças resultantes dos drones

Envia-se em anexo, à atenção das delegações, o documento COM(2023) 659 final.

Anexo: COM(2023) 659 final

COMISSÃO
EUROPEIA

Bruxelas, 18.10.2023
COM(2023) 659 final

COMUNICAÇÃO DA COMISSÃO AO CONSELHO E AO PARLAMENTO EUROPEU

sobre o combate às potenciais ameaças resultantes dos drones

I. INTRODUÇÃO

A presente comunicação define a política da UE para combater as potenciais ameaças dos sistemas de aeronaves não tripuladas (UAS) não cooperantes, comummente conhecidos como «drones». Faz parte de um pacote de combate aos drones mais vasto que inclui igualmente dois manuais com orientações práticas sobre os principais aspetos técnicos desta política. Este pacote foi anunciado como uma ação emblemática no âmbito da Comunicação da Comissão intitulada «Estratégia Drone 2.0 para um ecossistema de aeronaves não tripuladas inteligente e sustentável na Europa»[1]. A presente comunicação dá resposta à necessidade de: i) proporcionar um quadro estratégico abrangente e harmonizado; ii) criar um entendimento comum dos procedimentos aplicáveis para fazer face às ameaças em constante evolução que os drones podem representar; e iii) ter em conta a rápida evolução tecnológica.

A. Complementar o quadro da UE em matéria de drones

A utilização legítima de drones é um elemento fundamental do caminho para a dupla transição ecológica e digital, tal como estabelecido na Estratégia Drone 2.0 da UE. Os drones desempenham um papel importante, nomeadamente nos domínios dos transportes, da defesa, do comércio e dos serviços. Nos próximos anos, o número de drones utilizados na UE deverá aumentar significativamente e estes serão consideravelmente melhores em termos de velocidade, agilidade, autonomia máxima, capacidade de carga útil, precisão dos sensores e utilização da inteligência artificial. Esta evolução conduzirá a um leque mais vasto de utilizações legítimas e lícitas dos drones. No entanto, para que este potencial seja alcançado, é necessário fazer face à potencial ameaça que os drones não cooperantes podem representar. Um drone não cooperante deve ser definido de acordo com a natureza da não cooperação, que pode ser criminosa, ilegal (violação regulamentar intencional) ou amadora (ignorante, negligente).

A presente comunicação aborda as ameaças resultantes dos drones concebidos para utilização civil e procura combater as ameaças destes drones num ambiente civil. Embora os drones concebidos para fins de defesa não sejam o cerne da presente comunicação, subsistem várias interligações com o domínio da defesa. Tais ligações incluem a potencial utilização de drones de menor dimensão concebidos para fins de defesa por criminosos ou terroristas, bem como as sinergias entre tecnologias de combate aos drones. Os drones concebidos para fins de defesa poderão ocupar o mesmo espaço aéreo que os drones civis, caso em que têm de ser identificáveis pelas autoridades competentes para fins de conhecimento situacional.

O âmbito da presente comunicação incide especificamente no *combate* às potenciais ameaças resultantes dos drones. Por conseguinte, não visa abranger a dimensão mais ampla do papel dos drones no domínio da segurança interna, nomeadamente a sua utilização para fins de aplicação da lei, ordem pública ou segurança pública.

As autoridades dos Estados-Membros são as principais responsáveis pelo combate às ameaças resultantes dos drones não cooperantes. No entanto, os Estados-Membros também beneficiam de uma ação a nível da UE, permitindo uma cooperação e coordenação mais estreitas nos diferentes meios e instrumentos utilizados para o efeito. Por conseguinte, a presente comunicação promove várias ações relacionadas com a criação de comunidades e a partilha de informações. Apoia igualmente os Estados-Membros através da disponibilização de orientações, formação, financiamento e procedimentos operacionais.

[1] Estratégia Drone 2.0 para um ecossistema de aeronaves não tripuladas inteligente e sustentável na Europa, COM(2022) 652 final de 29 de novembro de 2022.

Os incidentes potencialmente perigosos que envolvem drones tornaram-se mais frequentes, dentro e fora da UE. Por conseguinte, é importante facilitar a adoção de soluções físicas ou digitais de combate aos drones pelas autoridades responsáveis pela aplicação da lei e por outras autoridades públicas na UE e pelos operadores das infraestruturas críticas. A elaboração de uma política da UE de combate aos drones contribuirá para reforçar os procedimentos de ensaio da eficiência das novas soluções disponíveis e para facilitar a utilização orientada da investigação e inovação nesse domínio. Ao elaborar esta política de combate aos drones, a Comissão está a contribuir para o reforço de um mercado da UE de soluções de combate aos drones. Tal abrirá caminho a uma maior autonomia estratégica e soberania tecnológica da UE, nomeadamente nos domínios das tecnologias críticas, promoverá as capacidades europeias para desenvolver soluções de ponta nos domínios da defesa, aeroespacial e da segurança civil e reduzirá a dependência de fornecedores de países terceiros. Tal basear-se-á nos resultados da avaliação das dependências tecnológicas críticas[2] e fornecerá dados adicionais e uma nova análise. Irá ainda: i) ajudar a Comissão a compreender a utilização de tecnologias críticas e a dependência de fornecedores de países terceiros; e ii) fornecer uma panorâmica sólida do nível de dependência.

Além disso, a fim de combater as ameaças resultantes dos drones não cooperantes do ponto de vista das autoridades públicas, é igualmente importante: i) dispor de quadros e procedimentos claros e harmonizados; ii) autorizar claramente as partes interessadas públicas e privadas responsáveis a intervir contra drones não cooperantes; e iii) facilitar a colaboração entre as partes interessadas que nem sempre estão habituadas a trabalhar em conjunto (autoridades responsáveis pela aplicação da lei, autoridades da aviação civil, operadores, fabricantes, operadores de redes móveis). A presente comunicação propõe ações para: i) criar um entendimento comum dos procedimentos aplicáveis ao lidar com ameaças resultantes dos drones; e ii) identificar eventuais necessidades de harmonização das medidas regulamentares.

B. Fazer face a uma ameaça atual e em rápida evolução

Tanto a Estratégia da UE para a União da Segurança[3] como a Agenda da UE em matéria de Luta contra o Terrorismo[4] sublinham que a ameaça dos drones não cooperantes é uma grave preocupação na Europa.

A rápida evolução das capacidades dos drones representa um risco crescente para a segurança. Nos últimos anos, foram descobertos planos de testagem e utilização de drones para cometer ataques terroristas[5]. Também foram avistados drones suspeitos em torno de infraestruturas críticas, como instalações energéticas, aeroportos e portos, o que indica a potencial utilização abusiva de drones para recolha hostil de informações. Os drones são utilizados por criminosos envolvidos no contrabando transfronteiras ou para facilitar outras operações ilícitas, incluindo o tráfico de estupefacientes. Além disso, os drones podem ser uma fonte de riscos cibernéticos, por exemplo, se forem utilizados para efeitos de reconhecimento digital. As ameaças resultantes dos drones não são um mero problema técnico. Atualmente, a maior parte dos drones concebidos para fins civis pode ser detetada e identificada, mas continua a ser muito difícil combatê-los ou neutralizá-los (ou seja, assumir o controlo dos mesmos, aterrá-los em segurança ou abatê-los),

---

2 Uma avaliação aprofundada interna da Comissão sobre sistemas autónomos realizada em 2022.

3 Estratégia da UE para a União da Segurança, COM(2020) 605 final de 24 de julho de 2020.

4 Uma Agenda da UE em matéria de Luta contra o Terrorismo: Antecipar, Prevenir, Proteger, Responder, COM(2020) 795 final de 9 de dezembro de 2020.

5 Exemplos disso são: i) o plano de um jiadista inspirado, condenado por um tribunal espanhol em outubro de 2022 por planear atacar um estádio durante um importante jogo de futebol recorrendo a um drone carregado de explosivos; e ii) um cidadão belga, condenado por tentativa de atentado à bomba com recurso a drones contra uma prisão.

frequentemente devido à falta de autorização legal para o efeito. Tal aplica-se especialmente aos operadores privados das infraestruturas críticas. Por conseguinte, o combate às ameaças resultantes dos drones deve ser tido em consideração nas futuras avaliações de riscos ao abrigo da Diretiva relativa à resiliência das entidades críticas[6].

A situação de ameaça torna-se ainda mais clara quando se analisam incidentes em países próximos da UE e noutras partes do mundo. Os drones provaram ser uma plataforma de dupla utilização eficaz e eficiente em termos de custos que impulsionou a inovação no domínio da defesa na guerra russa contra a Ucrânia. A utilização de drones concebidos para fins civis para lançar ataques destrutivos, mesmo noutros conflitos armados (por exemplo, no Iémen ou na Síria), é um fenómeno suscetível de ter implicações na segurança interna da UE. O *modus operandi* dos grupos terroristas e a melhoria das competências na pilotagem de drones «prontos a utilizar» (*off the shelf*) podem chegar às nossas fronteiras e representar uma ameaça. O mesmo se aplica à utilização de drones para tentativas de assassinatos seletivos[7].

No entanto, as soluções de combate aos drones não são unicamente necessárias contra uma utilização mal-intencionada orientada. São igualmente necessárias para prevenir incidentes causados por negligência ou imprudência. A maioria dos utilizadores de drones na UE (nomeadamente os pilotos remotos profissionais detentores de licenças ou os pilotos de recreio organizados) cumpre as regras, os regulamentos e as limitações técnicas em vigor. Não obstante, os utilizadores de drones ignorantes, negligentes e criminosos são responsáveis pelos inúmeros incidentes perigosos que envolvem drones em toda a UE. Os eventos públicos de grande escala são particularmente vulneráveis a tais perturbações, tal como alguns setores críticos, como o dos transportes aéreos. Além disso, a utilização ilícita de drones pode igualmente afetar a segurança pessoal e o direito à privacidade dos cidadãos, nomeadamente quando os drones são operados em zonas residenciais.

C. Acompanhar a evolução tecnológica

A proteção das nossas sociedades contra drones malévolos e não cooperantes exige o acesso a contramedidas fiáveis e a preços acessíveis que permitam soluções flexíveis. Geralmente, as soluções abordam três aspetos — deteção, seguimento e identificação —, estando as autoridades públicas igualmente interessadas em dois aspetos adicionais: neutralização e investigação forense.

Tanto no domínio da defesa como no da segurança civil, já estão a ser desenvolvidas e testadas soluções inovadoras de combate aos drones. A sua introdução no mercado e a sua adoção pelos utilizadores finais podem ser facilitadas por um quadro global da UE em matéria de combate aos drones, tal como promovido na presente comunicação. No entanto, não é possível adotar uma abordagem única normalizada para a aplicação de medidas de combate aos drones devido à grande variedade de cenários e ambientes operacionais possíveis.

Por conseguinte, as medidas de combate aos drones têm de ser adaptadas a diferentes necessidades e ambientes operacionais. Do ponto de vista das autoridades responsáveis pela segurança interna, pode haver situações em que a destruição física total de um drone seja a opção preferida e única, por exemplo, para evitar um ataque iminente a pessoas ou infraestruturas. Noutros casos, como a utilização criminosa ou a recolha hostil de informações, existe um grande interesse em garantir o controlo do drone para o fazer

---

[6] Diretiva (UE) 2022/2557 relativa à resiliência das entidades críticas, de 14 de dezembro de 2022 (JO L 333 de 27.12.2022, p. 164).

[7] Exemplos disso são uma tentativa infrutífera de assassinar o Presidente da Venezuela e a utilização de drones pelos cartéis da droga mexicanos contra representantes de outras organizações criminosas.

aterrar, mantendo-o o mais intacto possível, de modo a permitir uma investigação forense otimizada. Tal inclui a necessidade de soluções cibernéticas sofisticadas para assumir o controlo do sistema operativo de um drone.

Uma das tendências tecnológicas que devem ser monitorizadas e utilizadas ativamente é o desenvolvimento de sensores para a deteção mais precisa de drones. As capacidades de sensores existentes podem ser aperfeiçoadas não só para detetar um drone, mas também para avaliar a ameaça que o mesmo representa através da análise da trajetória de voo, da deteção da carga útil e da deteção de equipamento. Os sensores e os sistemas de deteção têm de ser capazes de lidar com a evolução das formas e capacidades dos drones (velocidade, agilidade, capacidade de implantar engodos, etc.). A capacidade das autoridades públicas e dos operadores privados das infraestruturas críticas para analisar os dados desses sensores será cada vez mais importante. A inteligência artificial também desempenhará um papel importante, por exemplo, ao gerar automaticamente alertas, calcular os riscos, prever rotas ou locais de aterragem. Assim, é necessário acompanhar de forma contínua as novas tendências nos mercados de drones e incorporá-las em soluções de combate aos drones. O acompanhamento desta evolução tecnológica deverá permitir às autoridades da UE identificar prioridades de investimento e apoiar a evolução mais adequada para satisfazer as necessidades operacionais expressas pelas autoridades responsáveis pela aplicação da lei e pelos operadores privados dos Estados-Membros.

No que diz respeito à interação e à neutralização, são necessários mais ensaios de tecnologias que sejam adequadas em diferentes ambientes e cenários. No domínio da defesa, foram identificadas soluções para destruir fisicamente ou capturar totalmente um drone enquanto este se encontra no ar, reduzindo assim a produção de detritos que podem causar ferimentos em pessoas ou danos em objetos. Tal inclui a energia dirigida sob a forma de lasers de alta energia, bem como a utilização de sistemas de radiofrequência e de captação de redes de alta potência, para além de ferramentas digitais para obter controlo sobre drones não cooperantes.

Para efeitos de aplicação da lei e de investigação, seria particularmente útil poder neutralizar uma ameaça de um drone ao assumir o controlo do seu sistema de comando e fazê-lo aterrar em segurança, proporcionando às autoridades e aos investigadores o melhor acesso possível a potenciais provas físicas e digitais. Por conseguinte, deve ser disponibilizado e validado um vasto leque de soluções diferentes para diferentes fins, de forma a servir o domínio da segurança interna. Assim, é necessário promover um verdadeiro mercado e ambiente de inovação para soluções de combate aos drones que deem resposta às necessidades do domínio da segurança civil. Caso contrário, é pouco provável que a evolução das soluções de combate aos drones acompanhe o aumento do número e das capacidades dos próprios drones. É igualmente essencial estruturar e segmentar este mercado para ajudar as autoridades competentes a identificar as soluções que melhor respondem às suas necessidades.

Além disso, é importante monitorizar os denominados sistemas de resposta ao combate aos drones utilizados pelos criminosos. Os sistemas de resposta ao combate aos drones são dispositivos transportados pelo drone ou implantados a partir do solo e concebidos para obstruir medidas específicas de combate aos drones.

Por último, muitos sistemas de combate aos drones são igualmente desenvolvidos para fins de defesa. Embora diferentes em termos de requisitos, partilham frequentemente características e tecnologias comuns com sistemas destinados a fins civis, o que torna necessária uma estreita cooperação com o domínio da defesa.

Este panorama tecnológico em evolução exige igualmente um quadro regulamentar coerente e continuamente atualizado para a utilização de sistemas de combate aos drones.

II. FORMULAÇÃO DE UMA POLÍTICA DA UE DE COMBATE AOS DRONES

Desde 2016, altura em que teve lugar o primeiro seminário da UE sobre o combate aos drones, a Comissão tem trabalhado com os Estados-Membros e outras partes interessadas no que se refere às potenciais ameaças resultantes dos drones. Desde então, foi introduzido um vasto leque de iniciativas para facilitar a criação de comunidades, a partilha de informações, o desenvolvimento de boas práticas e o financiamento específico de projetos. Na sequência dos debates com peritos dos Estados-Membros, a Comissão continuará a apoiar estas iniciativas em curso, desenvolvendo e integrando simultaneamente novas vertentes de trabalho para elaborar uma verdadeira política da UE de combate aos drones. Este trabalho consistirá nas seguintes seis atividades principais:

Criação de comunidades e partilha de informações	**Ensaio de sistemas de combate aos drones**	**Orientações práticas e apoio operacional**	**Investigação e inovação**	**Apoio financeiro**	**Medidas regulamentares**

A. Criação de comunidades e partilha de informações

Um vasto leque de diferentes redes e intervenientes está atualmente a trabalhar a nível da UE em soluções de combate aos drones. Por conseguinte, é necessário simplificar e orientar as suas atividades futuras em termos políticos, técnicos e operacionais, a fim de: i) criar comunidades de partes interessadas funcionais; ii) assegurar a partilha eficaz de informações e boas práticas; e iii) evitar a duplicação de esforços.

A Comissão promoverá as iniciativas existentes a nível técnico, criando simultaneamente um **grupo de peritos da Comissão para o combate aos drones** para prestar aconselhamento a nível político. Este grupo de peritos será capaz de contribuir estrategicamente para várias políticas a nível da UE com pertinência para as atividades de combate aos drones, nomeadamente nos domínios da segurança interna, da gestão das fronteiras ou da resiliência das infraestruturas críticas. Para o efeito, o grupo de peritos cooperará com outros grupos de peritos e, se adequado, com os grupos de trabalho competentes do Conselho.

Regularmente, realizam-se seminários e reuniões de peritos sobre soluções e políticas de combate aos drones que reúnem decisores políticos, peritos técnicos e investigadores da Comissão, dos Estados-Membros, de outras instituições da UE, de agências da UE, de projetos financiados pela UE, de organizações internacionais e de países parceiros. Estas atividades conduziram à participação contínua de todas as partes interessadas, facilitando significativamente a sua cooperação operacional e prática. Para o efeito, a Comissão criou o **Polo de Informação Anti-UAS**[8], que conta atualmente com mais de 300 membros. Esta plataforma em linha é atualizada regularmente e aloja diferentes fontes de informação, como resultados de projetos pertinentes financiados pela UE, apresentações, relatórios e um boletim informativo semestral.

Outra parte importante da criação de comunidades e da partilha de informações, nomeadamente para as necessidades operacionais das autoridades responsáveis pela aplicação da lei, tem lugar no âmbito das **redes europeias de serviços responsáveis pela aplicação da lei** financiadas pela UE. Por exemplo, as redes a seguir indicadas iniciaram as suas próprias atividades de combate às ameaças resultantes dos drones: a Rede Europeia de Serviços de Tecnologia das Autoridades de Aplicação da Lei (ENLETS); a Rede Europeia de Forças de Polícia Aeroportuárias (AIRPOL); a Rede de Unidades Especiais de Intervenção da UE (ATLAS); e a Rede de Risco Elevado para a Segurança da UE. O recém-criado grupo de trabalho da rede de serviços responsáveis pela aplicação da lei, uma iniciativa da DG Migração e Assuntos Internos destinada a promover a cooperação entre redes de forças de polícia e financiada pela Comissão[9], simplificará as vertentes de trabalho em curso no domínio do combate aos drones num subgrupo de trabalho específico.

A **Agência Europeia para a Segurança da Aviação (AESA)** elaborou orientações não vinculativas para ajudar as autoridades e os aeroportos a prepararem-se, darem resposta e recuperarem de incidentes com drones[10]. A fim de promover atividades de apoio informadas e a elaboração de políticas a nível da UE, é essencial dispor de intercâmbios de informações fiáveis e pormenorizados sobre incidentes que envolvam drones na UE para além dos intercâmbios já realizados em zonas críticas específicas, como os aeroportos.

---

[8] Utilizando a plataforma CIRCABC da UE, apoiada pelo Programa ISA² da Comissão Europeia, que promove soluções de interoperabilidade para as administrações públicas europeias.

[9] O grupo de trabalho (informal) da rede de serviços responsáveis pela aplicação da lei (LENWG) é presidido pela Comissão e reuniu-se pela primeira vez em 20 de março de 2023 para promover uma melhor cooperação entre as redes financiadas pela DG Migração e Assuntos Internos. Após um período de avaliação de 12 meses, o LENWG poderá tornar-se um grupo de peritos da Comissão propriamente dito.

[10] A Agência da União Europeia para a Segurança da Aviação (AESA) publicou, em março de 2021, um conjunto de orientações para a gestão de incidentes com drones em aeroportos: *Drone Incident Management at Aerodromes* (não traduzido para português).

Embora respeitando plenamente a confidencialidade das investigações, existe uma margem significativa para melhorar a partilha de informações sobre: i) os métodos utilizados pelos operadores de drones não cooperantes; ii) padrões específicos de ameaça; e iii) potenciais riscos identificados. A fim de facilitar e harmonizar a partilha dessas informações sobre incidentes, a Comissão partilhou com os Estados-Membros um modelo para a comunicação de incidentes com drones. Com o intuito de aumentar ainda mais a qualidade e a frequência da partilha de informações, a Comissão explorará a possibilidade de criar uma **plataforma digital que contenha informações sobre incidentes com drones,** para utilização pelas autoridades públicas competentes, que poderia servir para identificar adequadamente e relacionar informações sobre os incidentes graves de segurança que envolvem drones na UE. Tal pode incluir também a dimensão cibernética, uma vez que os drones são utilizados não só para efeitos de reconhecimento visual, mas também para efeitos de reconhecimento digital. Esta plataforma seria coerente com as obrigações de comunicação de informações em vigor ao abrigo do Regulamento (UE) n.º 376/2014[11] e não duplicaria os esforços envidados.

A Comissão organizará igualmente reuniões periódicas classificadas para promover o intercâmbio de ensinamentos retirados de incidentes num formato adequado.

Ações-chave para a criação de comunidades e a partilha de informações

- **A Comissão criará um grupo de peritos, composto por peritos dos Estados-Membros e outras partes interessadas, sobre atividades de combate aos drones.**
- **A Comissão explorará a possibilidade de desenvolver uma plataforma digital que contenha informações sobre incidentes com drones.**
- **A Comissão organizará reuniões periódicas para facilitar o intercâmbio de informações classificadas entre os Estados-Membros sobre incidentes graves de segurança que envolvam a utilização de drones.**

B. Ensaio de sistemas de combate aos drones: identificação e ensaio de soluções

Os Estados-Membros e as autoridades locais podem escolher entre um vasto leque de soluções comerciais, cibernéticas e não cibernéticas, de combate aos drones disponíveis no mercado. Fazer esta escolha constitui um desafio, especialmente para as entidades locais que não dispõem de capacidades técnicas suficientes. A Comissão ajudará as autoridades dos Estados-Membros a fazerem a escolha certa para dar resposta às suas necessidades operacionais, prestando aconselhamento e fornecendo orientações através do grupo de peritos específico para o combate aos drones e do trabalho desenvolvido pelo Centro Comum de Investigação (JRC) da Comissão.

Em 2019, foram lançadas atividades a nível da UE para ensaiar sistemas de combate aos drones que visam desenvolver uma metodologia comum para avaliar sistemas que podem ser utilizados pelas autoridades responsáveis pela aplicação da lei e por outras autoridades públicas para detetar, seguir e identificar drones potencialmente malévolos. Um pilar central destas atividades é o projeto «Courageous»[12] (2021-2024), financiado pelo Fundo para a Segurança Interna - Polícia (FSI-Polícia) da UE e liderado pela Academia Militar Real da Bélgica, incumbida de: i) identificar cenários normalizados adequados ao ensaio de sistemas

[11] Regulamento (UE) n.º 376/2014 do Parlamento Europeu e do Conselho, de 3 de abril de 2014, relativo à comunicação, à análise e ao seguimento de ocorrências na aviação civil.

[12] https://courageous-isf.eu/.

de combate aos drones; ii) desenvolver requisitos funcionais e de desempenho; e iii) desenvolver uma metodologia de ensaio. O projeto está igualmente a ensaiar o desempenho de sensores e sistemas integrados. Os resultados do projeto são partilhados continuamente com os Estados-Membros, bem como com determinados países parceiros e organizações internacionais. Após a conclusão do projeto, a Comissão e o consórcio Courageous apresentarão aos Estados-Membros opções para assegurar a sustentabilidade do projeto e recomendarão uma **metodologia para as instalações de ensaio de combate aos drones** nos Estados-Membros.

A evolução tecnológica dos sistemas de combate aos drones está a progredir rapidamente. Por conseguinte, as atividades de ensaio têm de ser complementadas por um acompanhamento constante das tendências, a fim de identificar tanto as soluções mais promissoras como quaisquer novos potenciais desafios para o desenvolvimento de sistemas de combate aos drones. O JRC desenvolveu capacidades para realizar este acompanhamento e identificar estes novos desafios, o que beneficia os Estados-Membros e dá um contributo valioso para as iniciativas de ensaio a nível da UE. As informações serão partilhadas através dos canais adequados, nomeadamente do grupo de peritos.

A normalização é um instrumento para harmonizar as soluções tecnológicas. O projeto «Courageous» elaborou aconselhamento específico sobre a pré-normalização, com base no qual é possível avaliar mais aprofundadamente a viabilidade e a necessidade de lançar processos de normalização. A nível da UE, registaram-se progressos significativos no desenvolvimento de requisitos de desempenho voluntários para o equipamento de deteção fora do setor da aviação (por exemplo, máquinas de raios X e detetores de metais[13]). Juntamente com peritos dos Estados-Membros e da indústria, a Comissão desenvolverá agora também **requisitos de desempenho voluntários** para os sistemas de combate aos drones, se for caso disso, em consonância com as disposições do Regulamento Cibersegurança[14]. A criação de um processo de certificação dos sistemas de combate aos drones deve continuar a ser um objetivo a médio prazo. Quando adequado, serão igualmente tidas em consideração normas híbridas civis/de defesa.

A normalização e a certificação da cibersegurança dos sistemas de combate aos drones, especialmente quando fornecidos por fornecedores de países terceiros, constitui outro elemento fundamental. Nesta fase, subsiste incerteza quanto ao grau de proteção dos dados recolhidos por determinados sistemas de deteção. Além disso, é importante prevenir, tanto quanto possível, a pirataria informática e a utilização abusiva de sistemas de combate aos drones, assegurando a ciber-resiliência dos seus componentes.

Em setembro de 2022, a Comissão adotou uma proposta de regulamento relativo à ciber-resiliência[15], com o objetivo de elaborar regras gerais em matéria de cibersegurança para os produtos com componentes digitais, tanto no que se refere ao *hardware* como ao *software*, que têm acesso ao mercado único. O novo regulamento proposto visa introduzir requisitos de cibersegurança obrigatórios para estes produtos. Estes requisitos incluirão a cibersegurança desde a conceção e por defeito, bem como requisitos para combater a vulnerabilidade. Tal como proposto pela Comissão, os sistemas de drones que não sejam desenvolvidos exclusivamente para fins militares ou de segurança nacional e que ainda não estejam certificados em conformidade com o Regulamento (UE) 2018/1139 seriam abrangidos por estas novas regras enquanto

[13] Recomendação da Comissão relativa aos requisitos de desempenho voluntários dos equipamentos de raios X utilizados em espaços públicos, C(2022) 4179 final.

[14] Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA e à certificação da cibersegurança das tecnologias da informação e comunicação.

[15] Proposta de Regulamento do Parlamento Europeu e do Conselho relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera o Regulamento (UE) 2019/1020, COM(2022) 454 final.

produtos com elementos digitais, com exceção dos desenvolvidos exclusivamente para fins de segurança nacional ou de defesa.

Ações-chave para ensaiar sistemas de combate aos drones

- **A Comissão trabalhará na aplicação de uma metodologia de ensaio harmonizada para os sistemas de combate aos drones com base nos resultados do projeto «Courageous».**
- **O JRC elaborará um relatório anual sobre a evolução técnica da tecnologia de combate aos drones.**
- **A Comissão, em cooperação com os grupos de peritos competentes, como as redes de serviços responsáveis pela aplicação da lei ENLETS, HRSN e AIRPOL, desenvolverá um conjunto de requisitos de desempenho voluntários para os sistemas de combate aos drones.**

C. Orientações práticas e apoio operacional

O combate às ameaças resultantes dos drones não cooperantes já foi identificado como uma prioridade em várias publicações do JRC, por exemplo, em orientações centradas na proteção do perímetro dos edifícios[16] e no estudo específico sobre cargas explosivas transportadas por drones[17]. Além disso, a recente publicação[18] sobre o conceito de segurança desde a conceção salienta a importância de integrar medidas de proteção proporcionadas, adequadas e multifuncionais numa abordagem ponderada desde o início da fase de planeamento e conceção de um projeto, incluindo medidas para combater quaisquer ataques que utilizem drones.

Além disso, o manual da AESA intitulado *Drone Incident Management at Aerodromes* (Gestão de Incidentes com Drones em Aeródromos) fornece orientações sobre a forma de desenvolver mecanismos e procedimentos adequados que apoiem um sistema de resposta a incidentes em aeroportos que seja rápido, eficaz e proporcionado. Desta forma, as suspensões do tráfego aéreo, ou o encerramento do espaço aéreo ou das pistas, podem ser evitadas ou reduzidas ao mínimo e o encerramento de aeroportos continuaria a ser uma medida de último recurso. O trabalho desenvolvido pela AESA tem em conta as orientações da Organização da Aviação Civil Internacional (OACI) em matéria de segurança da aviação[19].

---

[16] Karlos, V., e Larcher, M., *Guideline - Building Perimeter Protection* (não traduzido para português), EUR 30346 EN, Serviço das Publicações da União Europeia, Luxemburgo, 2020.

[17] A ameaça da utilização de explosivos por UAS foi investigada pelo JRC em: Larcher, M., Karlos, V., Valsamos, G., e Solomos, G.: *Scenario study: drones carrying explosives* (não traduzido para português), JRC107683, 2018.

[18] Comissão Europeia, *Security by Design: Protection of public spaces from terrorist attacks* (não traduzido para português), JRC131172, 2022.

[19] O Manual de Segurança da Aviação da OACI (doc. 8973 – confidencial) presta assistência aos Estados-Membros na aplicação do anexo 17 da Convenção de Chicago, fornecendo orientações sobre a forma de aplicar as suas normas e práticas recomendadas (SARP) – Manual de Segurança da Aviação.

O JRC elaborou dois novos manuais:

- ***Proteção contra sistemas de aeronaves não tripuladas:*** *Handbook on UAS protection of Critical Infrastructure and Public Space - A five Phase approach for C-UAS stakeholders* (Manual sobre a proteção das infraestruturas críticas e do espaço público contra UAS – Uma abordagem em cinco fases para as partes interessadas no combate aos UAS),

- ***Proteção contra sistemas de aeronaves não tripuladas:*** *Handbook on UAS Risk Assessment and Principles for Physical Hardening of Buildings and Sites* (Manual sobre a avaliação dos riscos inerentes aos UAS e Manual sobre os princípios para o reforço da proteção física de edifícios e instalações).

No domínio da **formação**, o projeto «DroneWISE»[20], financiado pela UE, criou um pacote de estratégias de comando, controlo e coordenação de combate aos drones para as equipas de primeira intervenção. O projeto produziu igualmente dez módulos de formação, um manual e um portal de formação em linha. Estes módulos de formação foram integrados no currículo de formação da CEPOL, a Agência da União Europeia para a Formação Policial. Outro projeto do FSI dedicado à formação para efeitos de combate aos drones foi o projeto «Skyfall». É necessário alargar a formação disponibilizada aos prestadores de serviços de segurança privados, especificamente aos responsáveis pela proteção das infraestruturas críticas.

O **programa da Comissão relativo aos consultores da UE em matéria de segurança (PSA da UE)**[21] tem uma secção dedicada às atividades de combate aos drones, que disponibiliza: i) uma avaliação específica da vulnerabilidade das instalações e infraestruturas de alto risco; ii) conselhos práticos sobre a forma de lidar com a ameaça dos drones; e iii) conselhos práticos sobre a forma de lidar com a utilização de equipamento de deteção de drones durante eventos de alto risco. A Comissão explorará a necessidade de criar uma reserva da UE de equipamentos de combate aos drones à disposição dos Estados-Membros para os apoiar em eventos de grande escala.

Exercícios como os organizados com a rede de serviços responsáveis pela aplicação da lei a nível da UE contribuem para a preparação operacional em diferentes domínios da segurança interna. Se for caso disso, a Comissão colaborará com as redes pertinentes para incluir elementos de combate aos drones em futuros exercícios. Tal contribuirá para aumentar ainda mais os conhecimentos e o intercâmbio de boas práticas, recorrendo a diferentes soluções. Para reagir eficazmente às ameaças resultantes dos drones, é necessário assegurar uma comunicação segura e fiável entre as diferentes autoridades. Por conseguinte, o combate às ameaças resultantes dos drones fará parte do futuro planeamento de exercícios a realizar no âmbito do projeto de preparação BroadEU.Net financiado pela UE, que testará a base do futuro sistema de comunicações críticas da UE[22]. Além disso, poderão ser realizados exercícios conjuntos que incluam peritos em cibersegurança e segurança de drones que abordem os riscos cibernéticos colocados pelos drones, bem como soluções digitais para neutralizar os drones.

---

[20] https://dronewise-project.eu/

[21] https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en.

[22] O sistema de comunicações críticas da UE proporcionará uma infraestrutura segura e de banda larga para assegurar a interoperabilidade transfronteiriça dos sistemas de comunicação utilizados pelas autoridades responsáveis pela aplicação da lei e pelos serviços responsáveis pela resposta a emergências no espaço Schengen.

Ações-chave para orientações práticas e apoio operacional

- **O JRC publicará dois manuais no âmbito do pacote de combate aos drones.**
- **A Comissão, em cooperação com as agências competentes, apoiará o alargamento da formação existente em matéria de combate aos drones ao setor da segurança privada.**
- **A Comissão integrará as componentes de combate aos drones no planeamento de exercícios, em cooperação com as redes de serviços responsáveis pela aplicação da lei.**

D. Investigação e inovação

A UE continua a financiar o seu programa de investigação em matéria de segurança no âmbito do **Horizonte Europa (2021-2027)**[23]. Este programa de investigação representa cerca de 50 % do financiamento público total investido na UE e nos seus Estados-Membros no domínio da segurança. Enquanto contributo estratégico para várias prioridades da política de segurança da UE, esta investigação em matéria de segurança já começou a abordar as ameaças resultantes dos drones. Exemplos notáveis incluem o ALADDIN, que fornece soluções para detetar e neutralizar drones em zonas restritas[24] ou o 7SHIELD, que investigou o desenvolvimento de soluções de combate aos drones para segmentos terrestres de infraestruturas espaciais críticas. O projeto ALFA também foi bem-sucedido no desenvolvimento de um sistema para detetar e seguir drones utilizados para efeitos de contrabando[25]. Estas iniciativas de investigação e inovação podem ser prosseguidas no âmbito do Horizonte Europa, validadas ou complementadas por ações realizadas no âmbito do FSI-Polícia.

No futuro, a Comissão facilitará o intercâmbio mais sistemático dos resultados relevantes dos projetos com as partes interessadas, nomeadamente através da Comunidade Europeia de Investigação e Inovação para a Segurança[26]. Tal reforçaria ainda mais o intercâmbio de dados específicos e permitiria igualmente recolher de forma mais eficiente informações sobre as necessidades dos utilizadores e comunicá-las à indústria, a fim de orientar a inovação. Além disso, o intercâmbio sistemático dos resultados dos projetos permitirá um diálogo estruturado com os Estados-Membros e as partes interessadas para identificar tecnologias, ferramentas e soluções promissoras que possam ser adotadas por um grupo de autoridades dos Estados-Membros. Neste contexto, a Comissão avaliará com os Estados-Membros[27] a possibilidade de: i) criar um tema de investigação independente sobre soluções de combate aos drones nos futuros programas de trabalho

[23] Até ao final de 2020, a investigação e a inovação em matéria de segurança eram financiadas ao abrigo do Horizonte 2020 e do Sétimo Programa-Quadro.

[24] https://cordis.europa.eu/project/id/740859.

[25] O ALFA constitui igualmente a base para o projeto «Courageous» do FSI e as suas atividades de ensaio.

[26] A Comunidade Europeia de Investigação e Inovação para a Segurança (CERIS) reúne partes interessadas na investigação em matéria de segurança, desde decisores políticos, utilizadores finais, universidades e indústria à segurança civil: https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en.

[27] No formato do comité do programa Horizonte Europa «Segurança Civil para a Sociedade».

do Horizonte Europa; e ii) apoiar sistemas inovadores específicos através de contratos pré-comerciais[28]. Tal está em plena consonância com a abordagem centrada nas capacidades descrita no documento de trabalho dos serviços da Comissão intitulado «Melhorar a segurança através da investigação e inovação»[29].

É fundamental reforçar as sinergias em soluções de combate aos drones entre as indústrias europeias da segurança civil, da defesa e do espaço, com o objetivo de promover sinergias entre os três setores[30] no domínio das tecnologias de drones e de combate aos drones. Na prática, o reforço destas sinergias significa que os projetos de defesa podem beneficiar de desenvolvimentos inovadores no domínio civil, podendo a aeronáutica civil beneficiar de progressos em matéria de defesa.

O **Fundo Europeu de Defesa (FED)** e os respetivos programas precursores incentivam e apoiam a investigação e o desenvolvimento colaborativos e transfronteiriços no domínio da defesa. Complementando e ampliando os esforços dos Estados-Membros, o FED promove a cooperação entre empresas e investigadores de todas as dimensões e de todos os Estados-Membros na UE. Os programas precursores do FED já financiaram projetos de combate aos drones no âmbito da investigação e desenvolvimento no domínio da defesa.

O programa de trabalho do FED para 2023 inclui uma ação de desenvolvimento de combate aos drones[31], com um orçamento indicativo de 43 milhões de EUR. A ação visa desenvolver módulos de *hardware* ou *software* para uma solução móvel abrangente de combate a um vasto leque de drones, incluindo «enxames».

O principal resultado esperado do apoio do FED no domínio do combate aos drones em 2021-2027 é o desenvolvimento de um protótipo de solução de combate aos drones conducente a uma eventual futura contratação conjunta a nível da UE. Os desafios tecnológicos no domínio dos sistemas de combate aos drones são abordados através do Programa Europeu de Inovação no domínio da Defesa da UE (EUDIS). Além disso, o EUDIS inclui uma vertente para incubadoras de dupla utilização, a fim de promover uma melhor colaboração entre os domínios civil e da defesa e estimular a maturação e a adaptação tecnológicas.

O trabalho desenvolvido pelo JRC é outro pilar fundamental para a inovação e, especificamente, para a investigação aplicada sobre a forma de combater as ameaças resultantes dos drones. No âmbito do projeto «Drone C-UAS» do JRC, este último analisará as tecnologias ativas e passivas para aplicar contramedidas e a forma como estas tecnologias podem ser utilizadas para garantir a segurança de espaços públicos e infraestruturas críticas.

Para o efeito, e como primeiro passo, o JRC criará um **laboratório vivo** para estudar tecnologias de combate aos drones e a forma como estas tecnologias podem ser aplicadas em condições reais. A configuração do laboratório abrangerá o planeamento, a preparação e a aplicação de uma solução, bem como a deteção, o seguimento, a identificação, a neutralização e a integração das partes interessadas e dos processos. O âmbito de aplicação do laboratório vivo incluirá a integração com sistemas de gestão do tráfego tripulados e não

---

[28] Os contratos pré-comerciais (CPC) são uma forma de abordar a contratação pública de serviços de investigação e desenvolvimento (I&D) que foi delineada na Comunicação relativa aos contratos pré-comerciais, C(2007) 799 final de 14 de dezembro de 2007. Trata-se de um instrumento importante para estimular a inovação, uma vez que permite ao setor público orientar o desenvolvimento de novas soluções para dar resposta às suas necessidades.

[29] Documento de trabalho dos serviços da Comissão intitulado «Melhorar a segurança através da investigação e inovação», SWD(2021) 422 final de 15 de dezembro de 2021.

[30] SWD(2022) 362 de 10 de novembro de 2022. Conforme descrito no relatório intercalar sobre a execução do plano de ação sobre as sinergias entre as indústrias civis, da defesa e do espaço no âmbito da ação 9.

[31] Decisão de Execução C(2023) 2296 da Comissão, de 29 de março de 2023, relativa ao financiamento do Fundo Europeu de Defesa criado pelo Regulamento (UE) 2021/697 do Parlamento Europeu e do Conselho e à adoção do programa de trabalho para 2023 - Parte II.

tripulados, nomeadamente o espaço «U»[32]. O laboratório vivo estudará também a forma como a aprendizagem automática e a inteligência artificial podem ser integradas a fim de melhorar o desempenho global de uma solução de combate aos drones.

A médio prazo, este laboratório vivo do JRC será transformado num **centro de excelência de combate aos drones.**

Ações prioritárias para tirar o máximo partido da investigação e inovação

- **A Comissão e os Estados-Membros decidirão sobre as necessidades futuras de novas soluções de combate aos drones a abordar nos programas europeus de investigação e inovação pertinentes, nomeadamente o Horizonte Europa.**
- **A Comissão e os Estados-Membros identificarão uma lista de soluções promissoras de combate aos drones e avaliarão a viabilidade de algumas destas soluções para efeitos de contratos pré-comerciais.**
- **A Comissão identificará ideias, tecnologias e soluções a integrar no desenvolvimento das capacidades de defesa e apoiará projetos que procurem difundir estas ideias, tecnologias e soluções junto dos setores civis.**
- **O JRC transformará um laboratório vivo num centro de excelência de combate aos drones.**

E. Apoio financeiro

A Comissão continuará a prestar apoio financeiro a atividades relevantes de combate aos drones, principalmente através do FSI, mas também ao abrigo do Instrumento de Apoio Financeiro à Gestão das Fronteiras e à Política de Vistos (IGFV) e do programa Horizonte Europa (para ações relacionadas com a investigação e inovação).

O instrumento temático do FSI apoiará: i) as redes europeias de serviços responsáveis pela aplicação da lei; ii) o trabalho conexo desenvolvido pelo JRC; iii) o novo grupo de peritos para o combate aos drones; e iv) a criação de uma plataforma de intercâmbio de informações. A Comissão já está a financiar projetos para desenvolver e validar sistemas para detetar e localizar drones que atravessam ilegalmente as fronteiras externas da UE. Esses projetos baseiam-se nos resultados de projetos de investigação anteriores financiados pela UE[33].

[32] Regulamento de Execução (UE) 2021/664 da Comissão relativo a um quadro normativo do espaço «U». O termo «espaço U» foi adotado para descrever a gestão do tráfego de aeronaves não tripuladas, a fim de garantir a interação segura com outras entidades que utilizam o mesmo espaço em zonas urbanas e quaisquer outros locais.

[33] São exemplos disso os projetos financiados ao abrigo de ações específicas do IGFV no que se refere à: i) inovação nas fronteiras marítimas/costeiras e/ou terrestres; e à ii) Frontex. Alguns projetos financiados no âmbito da ação específica em matéria de inovação nas fronteiras marítimas/costeiras e/ou terrestres centram-se no desenvolvimento de tecnologias de vigilância inovadoras. Existe também uma ação específica para a aquisição e disponibilização às autoridades europeias responsáveis pelas fronteiras de equipamento para detetar e localizar drones que atravessam as fronteiras no contexto de atividades ilegais ou criminosas. Esta ação específica permitirá aos Estados-Membros adquirir dois sistemas de combate aos drones. Enquanto valor acrescentado para a UE, a pedido da Frontex no âmbito das negociações bilaterais anuais, o equipamento técnico adquirido no contexto das

No âmbito do instrumento temático do FSI, a Comissão lançará, no primeiro semestre de 2024, um **convite à apresentação de propostas** destinado especificamente a apoiar a implantação de soluções de combate aos drones com elevado potencial de adoção.

Os Estados-Membros serão incentivados a aplicar a presente comunicação e a tomar em consideração os resultados da investigação financiada pela UE no que se refere a soluções de combate aos drones através dos seus programas do FSI.

Ações-chave para o apoio financeiro

- **A Comissão lançará um convite à apresentação de propostas sobre soluções de combate aos drones no âmbito dos programas de trabalho do instrumento temático do FSI para 2026-2027.**
- **Os Estados-Membros serão incentivados a utilizar plenamente os seus programas do FSI para 2021-2027 para identificar e aplicar soluções eficazes de combate aos drones.**

F. Explorar medidas regulamentares

Embora a UE tenha regulamentado a utilização legítima de drones, não existem atualmente regulamentos específicos de combate aos drones a nível da UE que estabeleçam um quadro harmonizado comum para as autoridades, os operadores e os fabricantes dos Estados-Membros. Ainda que as orientações não vinculativas da AESA relativas aos incidentes com drones em aeroportos (referidas anteriormente na presente comunicação) tenham sido acolhidas favoravelmente pelo setor, a sua natureza consultiva e o seu âmbito de aplicação limitado tornam-nas insuficientes para atenuar a ameaça resultante dos drones não cooperantes. Uma vez que a necessidade de prevenir eficazmente a utilização não autorizada de drones está constantemente a aumentar, a Comissão, em estreita colaboração com peritos dos Estados-Membros, continuará a analisar a necessidade de medidas legislativas ou não legislativas no futuro. Para o efeito, a Comissão iniciará um **estudo de levantamento** específico para determinar o atual panorama regulamentar. Este estudo de levantamento também deve ter em conta o quadro e a evolução da OACI, bem como ter em consideração que as regras para combater as potenciais ameaças resultantes dos drones não devem impedir indevidamente operações legítimas, incluindo as atividades de pilotos de recreio organizados.

Os aeroportos da UE beneficiam de regras de segurança pormenorizadas e abrangentes que também incluem as ameaças resultantes dos drones. A fim de assegurar que as autoridades da aviação e os aeroportos sejam mais resilientes quando confrontados com os riscos colocados pelos drones, e em consonância com uma abordagem baseada em dados concretos, a Comissão, em cooperação com os Estados-Membros, **identificará potenciais vulnerabilidades adicionais na proteção contra drones não cooperantes que possam exigir alterações regulamentares numa avaliação dos riscos para a segurança**.

Neste contexto, é necessário encetar um diálogo estruturado com a indústria e os fabricantes de drones sobre as medidas de segurança desde a conceção (por exemplo, sistemas sólidos contra a mistificação da entidade, limitações de capacidades, partilha de protocolos de comunicação e atualizações de bases de dados relativas ao combate aos drones).

ações específicas tem de ser colocado à disposição da Frontex por um período máximo de quatro meses por ano, para utilização nas suas operações conjuntas.

Ações-chave para explorar medidas regulamentares

- **A Comissão iniciará um estudo de levantamento para identificar as necessidades regulamentares e o potencial de harmonização da legislação e dos procedimentos dos Estados-Membros.**
- **Em consonância com uma abordagem baseada em dados concretos, a Comissão realizará uma avaliação dos riscos para a segurança da aviação no que diz respeito aos drones a fim de identificar potenciais vulnerabilidades adicionais dos aeroportos que possam exigir alterações regulamentares.**
- **A Comissão encetará um diálogo estruturado com a indústria sobre a necessidade e a natureza de eventuais medidas específicas adicionais relacionadas com a segurança dos drones.**

III. O CAMINHO A SEGUIR

A fim de assegurar que a rápida evolução tecnológica e o número crescente de drones não conduzem a um aumento descontrolado das ameaças resultantes dos drones não cooperantes, é necessário intensificar a cooperação a nível da UE, com base na política global da UE de combate aos drones definida na presente comunicação. Para o efeito, as atuais atividades a nível da UE serão prosseguidas e complementadas pelo conjunto de ações-chave enumeradas na presente comunicação, que serão executadas nos próximos anos.

As atividades descritas na presente comunicação abrangerão o período até 2030. Até 2027, proceder-se-á a uma avaliação intercalar através do grupo de peritos, estando prevista uma revisão completa do programa da UE de combate aos drones, o mais tardar, até 2030.