Conseil de
l'Union européenne

Bruxelles, le 18 octobre 2023
(OR. en)

14394/23

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

NOTE DE TRANSMISSION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	18 octobre 2023
Destinataire:	Madame Thérèse BLANCHET, secrétaire générale du Conseil de l'Union européenne
N° doc. Cion:	COM(2023) 659 final
Objet:	COMMUNICATION DE LA COMMISSION AU CONSEIL ET AU PARLEMENT EUROPÉEN relative à la lutte contre les menaces potentielles posées par les drones

Les délégations trouveront ci-joint le document COM(2023) 659 final.

p.j.: COM(2023) 659 final

COMMISSION
EUROPÉENNE

Bruxelles, le 18.10.2023
COM(2023) 659 final

COMMUNICATION DE LA COMMISSION AU CONSEIL ET AU PARLEMENT EUROPÉEN

relative à la lutte contre les menaces potentielles posées par les drones

I. INTRODUCTION

La présente communication expose la politique de l'UE en matière de lutte contre les menaces potentielles que posent les systèmes d'aéronefs sans équipage à bord (UAS) non coopératifs, communément appelés «drones». Elle s'inscrit dans un paquet antidrone plus large, qui comprend également deux manuels fournissant des explications pratiques sur les principaux aspects techniques de cette politique. Ce train de mesures avait été annoncé comme une action phare dans la communication de la Commission intitulée «*Une stratégie Drone 2.0 pour favoriser un écosystème intelligent et durable d'aéronefs sans équipage à bord en Europe*[1]». La présente communication répond au besoin: i) de fournir un cadre d'action global et harmonisé; ii) de forger une compréhension commune des procédures applicables pour faire face aux menaces en constante évolution que peuvent représenter les drones; et iii) de tenir compte de l'évolution rapide de la technologie.

A. Compléter le cadre de l'UE sur les drones

L'utilisation légitime de drones est un élément essentiel pour réaliser la double transition écologique et numérique, comme l'évoque la stratégie «Drone 2.0» de l'UE. Ces appareils jouent un rôle important dans les domaines des transports, de la défense, du commerce et des services, pour n'en citer que quelques-uns. Le nombre de drones en circulation dans l'UE devrait considérablement augmenter dans les années à venir, et ils connaîtront des améliorations considérables du point de la vitesse, de l'agilité, de la portée maximale, des capacités de charge utile, de la précision des capteurs et de l'utilisation de l'intelligence artificielle. Ces évolutions conduiront à de plus larges possibilités d'utilisation légitime et licite des drones. Mais pour réaliser ce potentiel, il faut s'attaquer à la menace que peuvent représenter les drones non coopératifs. Un drone non coopératif doit être défini en fonction de la nature de la non-coopération, qui peut être criminelle, illégale (violation intentionnelle de la réglementation) ou amateur (ignorance, négligence).

La présente communication traite des menaces que posent les drones conçus pour un usage civil et vise à lutter contre les menaces qu'ils créent dans un environnement civil. Bien que les drones conçus à des fins de défense ne soient pas l'objet de la présente communication, il n'en existe pas moins plusieurs liens avec le domaine de la défense. Il s'agit notamment de l'utilisation potentielle, par des criminels ou des terroristes, de drones de petite taille conçus à des fins de défense, ainsi que des synergies entre les technologies antidrones. Les drones conçus à des fins de défense sont susceptibles d'occuper le même espace aérien que les drones civils, auquel cas les autorités compétentes doivent pouvoir les identifier pour apprécier la situation.

La présente communication porte spécifiquement sur la *lutte* contre les menaces potentielles posées par les drones. Elle ne vise donc pas à inclure la dimension plus large du rôle des drones dans le domaine de la sécurité intérieure, à savoir leur utilisation à des fins répressives, de sécurité publique ou de sûreté publique.

Les autorités des États membres sont responsables au premier chef de la lutte contre les menaces posées par les drones non coopératifs. Les États membres bénéficient toutefois également de l'action au niveau de l'UE, qui permet une coopération plus étroite et une meilleure coordination des différents moyens et outils utilisés à cette fin. Par conséquent, la présente communication promeut diverses actions relatives à la

[1] Une stratégie Drone 2.0 pour favoriser un écosystème intelligent et durable d'aéronefs sans équipage à bord en Europe, COM(2022) 652 final du 29 novembre 2022.

création de communautés et au partage d'informations. Elle soutient également les États membres en leur apportant des orientations, des formations, des financements et des procédures opérationnelles.

Les incidents potentiellement dangereux impliquant des drones sont devenus plus fréquents, tant au sein de l'UE qu'au-delà de ses frontières. Il importe donc de faciliter l'adoption de solutions antidrones physiques ou numériques par les services répressifs et autres autorités publiques de l'UE et par les opérateurs d'infrastructures essentielles. L'adoption d'une politique antidrone de l'UE permettra de renforcer les procédures servant à tester l'efficacité des nouvelles solutions disponibles et de faciliter l'utilisation ciblée de la recherche et de l'innovation dans ce domaine. En élaborant cette politique, la Commission contribue au renforcement d'un marché européen des solutions antidrones. L'autonomie stratégique et la souveraineté technologique de l'UE en seront accrues, y compris dans le domaine des technologies critiques. L'Europe sera ainsi plus à même de mettre au point des solutions de pointe dans les domaines de la défense, de l'aérospatial et de la sécurité civile, et de réduire sa dépendance à l'égard des fournisseurs non européens. Elle s'appuiera sur les résultats de l'évaluation des dépendances dans le domaine des technologies critiques[2] et obtiendra des données et analyses supplémentaires. En outre, cette politique i) fournira à la Commission des informations permettant de mieux comprendre l'utilisation des technologies critiques et les dépendances à l'égard de fournisseurs non européens, et ii) donnera une bonne vue d'ensemble du degré de dépendance.

De surcroît, pour lutter contre les menaces que représentent les drones non coopératifs du point de vue de l'autorité publique, il importe également i) de disposer de cadres et de procédures clairs et harmonisés; ii) de conférer sans ambiguïté aux acteurs publics et privés responsables le pouvoir d'intervenir contre les drones non coopératifs; et iii) faciliter la collaboration entre les parties prenantes qui ne sont pas toujours habituées à travailler ensemble (services répressifs, autorités de l'aviation civile, exploitants, constructeurs, exploitants de réseaux mobiles). La présente communication propose des actions visant à i) forger une compréhension commune des procédures applicables pour faire face aux menaces posées par les drones; et ii) recenser les éventuels besoins d'harmonisation des mesures réglementaires.

B. Faire face à une menace actuelle, en rapide évolution

La stratégie de l'UE pour l'union de la sécurité[3] et le programme de lutte antiterroriste[4] soulignent tous les deux que la menace que représentent les drones non coopératifs est un problème de taille en Europe.

Le développement rapide des capacités des drones crée un risque croissant pour la sécurité. Ces dernières années, des plans prévoyant d'essayer de perpétrer des attentats terroristes au moyen de drones ont été découverts[5]. Des drones suspects ont en outre été observés autour d'infrastructures critiques, telles que des installations énergétiques, des aéroports et des ports, ce qui indique leur potentielle utilisation malveillante à des fins de collecte hostile d'informations. Les drones sont utilisés par des criminels qui se livrent à la contrebande transfrontière ou pour faciliter d'autres opérations illicites, notamment le trafic de drogue. Ils peuvent en outre être une source de risques cybernétiques, par exemple s'ils servent à la reconnaissance

[2] Évaluation interne approfondie des systèmes autonomes, réalisée par la Commission en 2022.

[3] Stratégie de l'UE pour l'union de la sécurité, COM(2020) 605 du 24 juillet 2020.

[4] Programme de lutte antiterroriste pour l'UE: anticiper, prévenir, protéger et réagir, COM(2020) 795 final du 9 décembre 2020.

[5] On peut citer à titre d'exemple: i) le projet d'un djihadiste inspiré, qui a été condamné par un tribunal espagnol en octobre 2022 pour avoir planifié d'attaquer un stade lors d'un grand match de football, au moyen d'un drone chargé d'explosifs; et ii) un citoyen belge, condamné pour une tentative d'attentat à la bombe, à l'aide de drones, contre une prison.

numérique. Les menaces qu'ils posent ne sont pas simplement un problème technique. À l'heure actuelle, la plupart des drones conçus à des fins civiles peuvent être détectés et identifiés, mais il reste très difficile d'interagir avec eux ou de les neutraliser (c'est-à-dire d'en prendre le contrôle, de les faire atterrir en toute sécurité, ou de les abattre), souvent en raison de l'absence d'autorisation légale pour le faire. C'est particulièrement le cas pour les opérateurs privés d'infrastructures critiques. La lutte contre les menaces posées par les drones devrait donc être prise en considération dans les futures évaluations de risques prévues par la directive sur la résilience des entités critiques[6].

L'état de la menace devient encore plus clair lorsque l'on examine les incidents survenus dans des pays proches de l'UE et dans d'autres parties du monde. Les drones se sont révélés être une plateforme à double usage rentable et efficace, qui a stimulé l'innovation en matière de défense dans la guerre menée par la Russie contre l'Ukraine. L'utilisation de drones conçus à des fins civiles dans des attaques destructrices, même dans d'autres conflits armés (comme au Yémen ou en Syrie), est un phénomène susceptible d'avoir des répercussions directes sur la sécurité intérieure de l'UE. Le mode opératoire des groupes terroristes et les compétences avancées en matière d'utilisation des drones «prêts à l'emploi» pourraient atteindre nos frontières et représenter une menace. Il en va de même de l'utilisation de drones pour des tentatives d'assassinats ciblés[7].

Cependant, les solutions antidrones ne sont pas nécessaires uniquement pour lutter contre des utilisations malveillantes ciblées. Elles le sont également pour prévenir des incidents dus à la négligence ou à l'imprudence. La plupart des utilisateurs de drones dans l'UE (notamment les pilotes à distance professionnels titulaires d'une licence ou les pilotes de loisirs organisés) respectent les règles, réglementations et limitations techniques existantes. Mais des utilisateurs de drones ignorants, négligents ou criminels sont responsables des nombreux incidents dangereux impliquant ces appareils dans toute l'UE. Les manifestations publiques de grande ampleur sont particulièrement exposées à de telles perturbations, de même que certains secteurs critiques comme le transport aérien. En outre, l'utilisation illicite de drones peut également porter atteinte à la sécurité personnelle des particuliers et à leur droit au respect de la vie privée, notamment lorsque des drones survolent des zones résidentielles.

C. Rester en phase avec l'évolution technologique

Pour protéger nos sociétés contre les drones malveillants et non coopératifs, des contre-mesures abordables et fiables qui offrent des solutions flexibles sont nécessaires. Les solutions portent généralement sur les trois aspects que sont la détection, le suivi et l'identification, tandis que les pouvoirs publics s'intéressent également à deux aspects supplémentaires, la neutralisation et la criminalistique.

Dans les domaines de la défense et de la sécurité civile, des solutions antidrones innovantes sont déjà en cours de mise au point et testées. Leur mise sur le marché et leur adoption par les utilisateurs finaux pourraient être facilitées par un cadre global de l'UE en matière de lutte antidrone, tel que préconisé dans la présente communication. Il n'est toutefois pas possible d'adopter une approche uniforme pour la mise en œuvre de mesures antidrones, en raison de la grande variété des scénarios et des environnements opérationnels possibles.

[6] Directive (UE) 2022/2557 du 14 décembre 2022 sur la résilience des entités critiques (JO L 333 du 27.12.2022, p. 164).

[7] On peut citer, à titre d'exemple, une tentative infructueuse d'assassinat du président du Venezuela et l'usage de drones par les cartels mexicains de la drogue contre des membres d'autres organisations criminelles.

Les mesures antidrones doivent donc être adaptées aux différents besoins et aux divers environnements. Du point de vue des autorités chargées de la sécurité intérieure, il peut y avoir des situations dans lesquelles la destruction physique complète d'un drone est la solution privilégiée et unique, par exemple pour prévenir une attaque imminente contre des personnes ou des infrastructures. Dans d'autres cas, tels qu'une utilisation à des fins criminelles ou la collecte hostile d'informations, il y a un grand intérêt à prendre le contrôle du drone pour le faire atterrir tout en le gardant aussi intact que possible, afin de permettre une enquête criminalistique optimale. Il faut dès lors disposer de cybersolutions complexes pour prendre le contrôle du système d'exploitation des drones.

L'une des tendances technologiques à suivre et à utiliser activement est la mise au point de capteurs permettant une détection plus précise des drones. Les capacités existantes des capteurs peuvent être davantage développées pour non seulement détecter un drone, mais aussi évaluer la menace qu'il représente, par l'analyse du profil de vol, la détection de la charge utile et la détection des équipements. Les capteurs et les systèmes de détection doivent pouvoir s'adapter à l'évolution des formes et des capacités des drones (vitesse, agilité, capacité à déployer des leurres, etc.). La faculté des pouvoirs publics et des opérateurs privés d'infrastructures critiques d'analyser les données provenant de ces capteurs revêtira une importance croissante. L'intelligence artificielle jouera également un rôle, par exemple en déclenchant automatiquement des alertes, en calculant les risques et en prédisant les itinéraires ou les sites d'atterrissage. Par conséquent, les nouvelles tendances apparaissant sur les marchés des drones doivent faire l'objet d'une veille permanente et être intégrées dans les solutions antidrones. Le suivi de ces évolutions technologiques devrait permettre aux autorités de l'UE de déterminer les priorités d'investissement et de soutenir les développements qui sont les mieux à même de répondre aux besoins opérationnels exprimés par les services répressifs des États membres et par les opérateurs privés.

En ce qui concerne l'interaction avec les drones et leur neutralisation, des essais supplémentaires sont nécessaires sur des technologies qui sont adaptées à différents environnements et scénarios. Dans le domaine de la défense, des solutions ont été trouvées pour détruire physiquement ou capturer entièrement un drone en vol, ce qui permet de réduire la production de débris susceptibles de blesser des personnes ou d'endommager des objets. Il s'agit notamment d'énergie dirigée sous la forme de lasers à haute énergie, ainsi que du recours à des systèmes de radiofréquence à haute puissance et à des filets de capture, ainsi que d'outils numériques permettant de prendre le contrôle des drones non coopératifs.

Pour les services répressifs et les enquêteurs, il serait particulièrement utile de pouvoir neutraliser une menace par drone en prenant le contrôle de son système de contrôle et en le faisant atterrir en toute sécurité, ce qui donnerait aux autorités et aux enquêteurs le meilleur accès possible aux éléments de preuve physiques et numériques potentiels. Par conséquent, un large éventail de solutions variées devrait être disponible et validé à diverses fins, pour servir la sécurité intérieure. Il convient donc de favoriser un véritable environnement de marché et d'innovation permettant de créer des solutions antidrones qui répondent aux besoins de la sécurité civile. Faute de quoi, l'évolution des solutions antidrones ne pourra pas suivre le rythme d'augmentation des drones eux-mêmes et de leurs capacités. Il est également essentiel de structurer et de segmenter ce marché, afin d'aider les autorités compétentes à trouver les solutions qui répondent le mieux à leurs besoins.

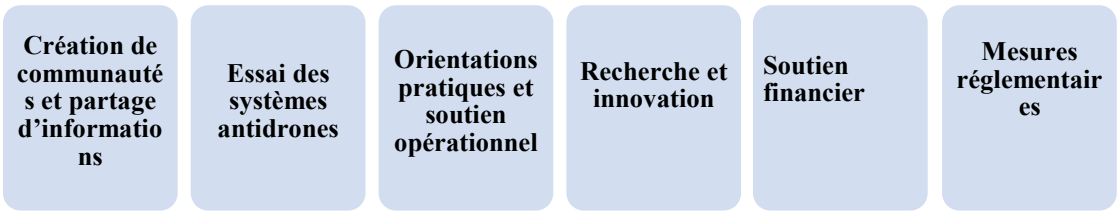
En outre, il importe de surveiller les systèmes utilisés par les criminels pour contrer les mesures antidrones. Ces systèmes sont des dispositifs transportés par le drone ou déployés depuis le sol, qui sont conçus pour faire obstacle à des mesures antidrones spécifiques.

Enfin, de nombreux systèmes antidrones sont également mis au point à des fins de défense. Bien que les exigences diffèrent, ils ont souvent des caractéristiques et des technologies communes aux systèmes destinés à des fins civiles, ce qui rend nécessaire une coopération étroite avec le domaine de la défense.

Ce paysage technologique en évolution nécessite, lui aussi, un cadre réglementaire cohérent et constamment actualisé pour l'utilisation des systèmes antidrones.

II. ÉLABORER UNE POLITIQUE ANTIDRONE DE L'UE

La Commission a commencé à collaborer avec les États membres et d'autres parties prenantes au sujet de la menace potentielle posée par les drones en 2016, date à laquelle a eu lieu le premier atelier de l'UE sur la lutte antidrone. Depuis lors, un large éventail d'initiatives a été mis en place pour faciliter la création de communautés, le partage d'informations, l'élaboration de bonnes pratiques et le financement spécifique de projets. À la suite des discussions avec les experts des États membres, la Commission continuera de soutenir ces initiatives en cours, tout en poursuivant le développement et l'intégration de nouveaux axes de travail en vue d'élaborer une véritable politique antidrone de l'UE. Ces travaux comprendront les six activités clés suivantes:



A. Création de communautés et partage d'informations

De nombreux réseaux et acteurs très divers travaillent actuellement au niveau de l'UE sur des solutions antidrones. Il est donc nécessaire de rationaliser et d'orienter leurs futures activités sur les plans stratégique, technique et opérationnel afin: i) de mettre en place des communautés de parties prenantes qui puissent fonctionner; ii) d'assurer le partage efficace d'informations et de bonnes pratiques; et iii) d'éviter la duplication des efforts.

La Commission encouragera les initiatives existantes, au niveau technique, et créera un **groupe d'experts antidrones de la Commission** chargé de fournir des conseils, au niveau stratégique. Ce groupe d'experts sera en mesure d'apporter une contribution stratégique à diverses politiques menées au niveau de l'UE qui présentent un intérêt pour les activités de lutte antidrone, par exemple dans les domaines de la sécurité intérieure, de la gestion des frontières ou de la résilience des infrastructures critiques. À cette fin, le groupe d'experts coopérera avec d'autres groupes d'experts et, s'il y a lieu, avec les groupes de travail compétents du Conseil.

Des ateliers et des réunions d'experts sur les solutions et les politiques antidrones ont lieu régulièrement. Ils réunissent des décideurs politiques, des experts techniques et des chercheurs de la Commission, des États membres, d'autres institutions de l'UE, des agences de l'UE, des projets financés par l'UE, des organisations internationales et des pays partenaires. Ces activités ont permis un dialogue continu entre toutes les parties prenantes, qui a considérablement facilité leur coopération opérationnelle et pratique. À cette fin, la Commission a mis en place la **plateforme d'information antidrone**[8], qui compte actuellement plus de 300 membres. Cette plateforme en ligne est régulièrement mise à jour et héberge différentes sources d'information, telles que les résultats de projets en la matière financés par l'UE, des présentations, des rapports et une lettre d'information semestrielle.

Un autre volet important de la création de communautés et du partage d'informations, notamment pour les besoins opérationnels des services répressifs, se trouve dans le cadre des **réseaux européens de services répressifs** financés par l'UE. À titre d'exemple, les réseaux suivants ont tous lancé leurs propres activités de lutte contre les menaces posées par les drones: le réseau européen des services technologiques de police (ENLETS); le réseau de l'UE pour les unités de police et de garde-frontières aéroportuaires (AIRPOL); le réseau d'unités spéciales d'intervention de l'UE (ATLAS); et le réseau de sécurité de l'UE pour la protection des espaces publics à haut risque. Le nouveau groupe de travail du réseau de services répressifs, une initiative de la DG HOME visant à favoriser la coopération entre les réseaux de police et financée par la Commission[9], rationalisera les axes de travail en cours dans le domaine de la lutte antidrone, au sein d'un sous-groupe de travail spécifique.

L'**Agence européenne de la sécurité aérienne (AESA)** a établi des lignes directrices non contraignantes pour aider les autorités et les aéroports à se préparer, à réagir et à remédier aux incidents liés aux drones[10]. Afin de favoriser des activités d'appui et des politiques éclairées au niveau de l'UE, il est essentiel de procéder à des échanges d'informations fiables et détaillés sur les incidents impliquant des drones dans

[8] En utilisant la plateforme EU CIRCABC, financée par le programme ISA² de la Commission européenne, qui promeut des solutions d'interopérabilité pour les administrations publiques européennes.

[9] Le groupe de travail (informel) du réseau de services répressifs (LENWG) est présidé par la Commission et s'est réuni pour la première fois le 20 mars 2023, afin de favoriser une meilleure coopération entre les réseaux financés par la DG HOME. Après une période d'évaluation de douze mois, le LENWG pourrait devenir un véritable groupe d'experts de la Commission.

[10] L'Agence de l'Union européenne pour la sécurité aérienne (AESA) a publié, en mars 2021, un ensemble de lignes directrices pour la gestion des incidents liés aux drones dans les aéroports: Drone Incident Management at Aerodromes.

l'UE, en plus des échanges qui ont déjà lieu dans des zones critiques spécifiques telles que les aéroports. Même en respectant pleinement la confidentialité des enquêtes, il est tout à fait possible d'améliorer le partage d'informations sur: i) les méthodes utilisées par les exploitants de drones non coopératifs; ii) les schémas de menace spécifiques; et iii) les risques potentiels recensés. Pour faciliter et harmoniser le partage de ces informations sur les incidents, la Commission a transmis aux États membres un modèle de notification des incidents liés aux drones. Afin d'accroître encore la qualité et la fréquence du partage d'informations, la Commission étudiera la possibilité de mettre en place une **plateforme numérique contenant des informations sur les incidents liés aux drones**, à l'usage des autorités publiques compétentes. Cette plateforme pourrait permettre de recenser et compiler correctement les incidents de sécurité majeurs impliquant des drones dans l'UE. La dimension cyber peut également être concernée, étant donné que les drones servent non seulement à la reconnaissance visuelle, mais aussi à la reconnaissance numérique. Cette plateforme s'inscrirait dans la ligne des obligations de notification existant au titre du règlement (UE) nº 376/2014[11] et ne ferait pas double emploi avec les efforts existants.

La Commission organisera en outre régulièrement des réunions classifiées afin de favoriser l'échange des enseignements tirés des incidents sous une forme appropriée.

Actions clés pour la création de communautés et le partage d'informations

- **La Commission créera un groupe d'experts sur les activités antidrones, composé d'experts des États membres et d'autres parties prenantes.**
- **La Commission étudiera la possibilité de créer une plateforme numérique contenant des informations sur les incidents liés aux drones.**
- **La Commission organisera régulièrement des réunions pour faciliter l'échange d'informations classifiées entre les États membres sur les principaux incidents de sécurité impliquant l'utilisation de drones.**

B. Essai des systèmes antidrones: recenser et tester les solutions

Les États membres et les autorités locales peuvent choisir parmi une large variété de solutions commerciales antidrones, cyber ou non cyber, disponibles sur le marché. Ce choix est difficile, en particulier pour les entités locales qui ne disposent pas de capacités techniques suffisantes. La Commission aidera les autorités des États membres à faire le bon choix pour leurs besoins opérationnels, en fournissant des conseils et des orientations par l'intermédiaire du groupe d'experts consacré aux solutions antidrones et des travaux du Centre commun de recherche (JRC) de la Commission.

Des activités au niveau de l'UE visant à tester les systèmes antidrones ont démarré en 2019. Elles ont pour objectif de mettre au point une méthode commune d'évaluation des systèmes susceptibles d'être utilisés par les services répressifs et d'autres autorités publiques pour détecter, suivre et identifier des drones potentiellement malveillants. Le projet «Courageous»[12] (2021-2024), financé par le Fonds de l'UE pour la sécurité intérieure, Police (FSI-Police), est un pilier central de ces activités. «Courageous» est dirigé par l'École royale militaire de Belgique et a pour missions: i) la définition de scénarios standard pertinents pour tester les systèmes antidrones; ii) la définition d'exigences fonctionnelles et de performances; iii) l'élaboration d'une méthode d'essai. Le projet vise également à évaluer la performance des capteurs et

[11] Règlement (UE) nº 376/2014 du Parlement européen et du Conseil du 3 avril 2014 concernant les comptes rendus, l'analyse et le suivi d'événements dans l'aviation civile, modifiant le règlement (UE).

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

des systèmes intégrés. Les résultats du projet sont partagés en permanence avec les États membres ainsi qu'avec certains pays partenaires et organisations internationales. À la fin du projet, la Commission et le consortium chargé de «Courageous» présenteront des options aux États membres pour garantir la viabilité du projet et recommanderont une **méthodologie pour les installations d'essai des systèmes antidrones** dans les États membres.

Les innovations technologiques utiles aux systèmes antidrones évoluent rapidement. Par conséquent, les essais doivent être complétés par un suivi permanent des tendances, afin de recenser à la fois les solutions les plus prometteuses et tout nouveau défi potentiel pour l'évolution des systèmes antidrones. Le JRC a renforcé ses moyens pour réaliser ce suivi et recenser ces nouveaux défis, ce qui est bénéfique aux États membres et apporte une contribution précieuse aux initiatives de l'UE en matière d'essai. Les informations seront partagées par les canaux appropriés, notamment le groupe d'experts.

La normalisation est l'un des instruments d'harmonisation des solutions technologiques. Le projet «Courageous» a formulé des conseils spécifiques sur la prénormalisation, sur la base desquels la faisabilité, et la nécessité, de lancer des processus de normalisation peuvent être évaluées de manière plus approfondie. Au niveau de l'UE, l'élaboration d'exigences de performance, d'application volontaire, pour les équipements de détection hors aviation (par exemple, pour les appareils d'imagerie radioscopique et les détecteurs de métaux[13]) a bien avancé. En collaboration avec des experts des États membres et de l'industrie, la Commission entend à présent également élaborer des **exigences de performance, d'application volontaire,** pour les systèmes antidrones, en cohérence avec les dispositions du règlement sur la cybersécurité, s'il y a lieu[14]. La mise en place d'un processus de certification des systèmes antidrones devrait rester un objectif à moyen terme. S'il y a lieu, des normes hybrides civil-défense seront également envisagées.

La normalisation et la certification de la cybersécurité des systèmes antidrones, en particulier s'ils sont fournis par des fournisseurs de pays tiers, est un autre élément clé. À ce stade, le degré de protection des données recueillies par certains systèmes de détection demeure incertain. En outre, il importe de prévenir autant que possible le piratage et l'utilisation malveillante des systèmes antidrones, en assurant la cyberrésilience de leurs composants.

En septembre 2022, la Commission a adopté une proposition de règlement sur la cyberrésilience[15], en vue de l'adoption de règles générales en matière de cybersécurité pour les produits comportant des composants numériques, tant matériels que logiciels, qui entrent sur le marché unique. Le nouveau règlement proposé vise à introduire des exigences de cybersécurité obligatoires pour ces produits. Il s'agit notamment de la cybersécurité dès la conception et par défaut, ainsi que d'exigences destinées à remédier à la vulnérabilité. Comme l'a proposé la Commission, les systèmes de drones qui ne sont pas conçus exclusivement à des fins militaires ou de sécurité nationale et qui ne sont pas déjà certifiés conformément au règlement (UE) 2018/1139 seraient soumis à ces nouvelles règles en tant que produits comportant des éléments numériques, à l'exception de ceux conçus exclusivement à des fins de sécurité nationale ou de défense.

[13] Recommandation de la Commission relative à des exigences de performance d'application volontaire pour les équipements d'imagerie radioscopique utilisés dans les espaces publics, C(2022) 4179 final.

[14] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications.

[15] Proposition de règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020, COM(2022) 454 final.

Actions clés pour les essais des systèmes antidrones

- **La Commission s'emploiera à mettre en œuvre une méthode d'essai harmonisée pour les systèmes antidrones, fondée sur les résultats du projet «Courageous».**
- **Le JRC établira un rapport annuel sur les évolutions techniques dans le domaine des technologies antidrones.**
- **La Commission, en coopération avec les groupes d'experts concernés, tels que les réseaux de services répressifs ENLETS, HRSN et AIRPOL, élaborera un ensemble d'exigences de performance, d'application volontaire, pour les systèmes antidrones.**

C. Orientations pratiques et soutien opérationnel

La lutte contre les menaces que représentent les drones non coopératifs a déjà été définie comme une priorité dans plusieurs publications du JRC, notamment dans des lignes directrices axées sur la protection périmétrique des bâtiments[16] et dans l'étude spécifique sur les charges d'explosifs transportées par drones[17]. En outre, la récente publication[18] sur le concept de sécurité dès la conception souligne l'importance d'intégrer des mesures de protection proportionnées, appropriées et multifonctionnelles dans une approche réfléchie dès le début de la phase de planification et de conception d'un projet, y compris des mesures visant à lutter contre toute attaque utilisant des drones.

En outre, le manuel de l'AESA intitulé «*Drone Incident Management at Aerodromes*» explique comment mettre en place des mécanismes et des procédures appropriées pour disposer d'un système rapide, efficace et proportionné de réaction aux incidents dans les aéroports. Les suspensions du trafic aérien, ou la fermeture de l'espace aérien ou des pistes, pourront ainsi être évitées ou réduites au minimum, et les fermetures d'aéroports resteront une solution de dernier recours. Les travaux de l'AESA tiennent compte des orientations de l'Organisation de l'aviation civile internationale en matière de sûreté aérienne[19].

Deux nouveaux manuels ont été élaborés par le JRC:

- ***Protection against Unmanned Aircraft Systems:*** *Handbook on UAS protection of Critical Infrastructure and Public Space - A five Phase approach for C-UAS stakeholders*

- ***Protection against Unmanned Aircraft Systems:*** *Handbook on UAS Risk Assessment and Principles for Physical Hardening of Buildings and Sites.*

Dans le domaine de la **formation**, le projet DroneWISE[20], financé par l'UE, a créé un ensemble de stratégies de commandement, de contrôle et de coordination antidrones à l'intention des premiers intervenants. Il a également produit dix modules de formation, un manuel et un portail de formation en ligne. Ces modules de formation ont été intégrés dans le programme d'études du CEPOL, l'Agence de l'Union européenne

[16] Karlos, V. et Larcher, M., Guideline - Building Perimeter Protection, EUR 30346 EN, Office des publications de l'Union européenne, Luxembourg, 2020.

[17] La menace que représente l'utilisation d'explosifs par des UAS a été analysée par le JRC dans les publications suivantes: Larcher M., Karlos V., Valsamos G., Solomos G.: Scenario study: drones carrying explosives, JRC107683, 2018

[18] Commission européenne, Security by Design: Protection of public spaces from terrorist attacks, JRC131172, 2022.

[19] Le manuel de sûreté de l'aviation de l'OACI (Doc 8973 — diffusion restreinte) aide les États membres à mettre en œuvre l'annexe 17 de la convention de Chicago, en expliquant comment appliquer ses normes et pratiques recommandées (SARP), Manuel de sûreté de l'aviation.

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

pour la formation des services répressifs. Le projet Skyfall est autre projet du FSI consacré à la formation antidrones. Il est nécessaire d'étendre la formation disponible aux entreprises de sécurité privées, en particulier à celles chargées de protéger les infrastructures critiques.

Le **programme des conseillers en matière de sûreté (EU PSA)**[21] de la Commission comporte une section consacrée aux activités de lutte antidrones, qui propose: i) une évaluation spécifique de la vulnérabilité des installations et infrastructures à haut risque, ii) des conseils pratiques pour faire face à la menace des drones, et iii) des conseils pratiques pour gérer le déploiement d'équipements de détection des drones lors d'événements à haut risque. La Commission étudiera la nécessité de créer une réserve européenne d'équipements antidrones à disposition des États membres pour les appuyer lors d'événements de grande ampleur.

Des exercices tels que ceux organisés avec le réseau des services répressifs au niveau de l'UE contribuent à la préparation opérationnelle dans différents domaines de la sécurité intérieure. S'il y a lieu, la Commission collaborera avec les réseaux concernés pour intégrer des éléments antidrones dans les futurs exercices. Cela permettra d'améliorer davantage les connaissances et l'échange de bonnes pratiques, en recourant à diverses solutions. Pour réagir efficacement aux menaces posées par les drones, il est nécessaire de disposer d'une communication fiable et sécurisée entre les différentes autorités. La lutte contre les menaces posées par les drones fera donc partie de la planification future des exercices qui aura lieu dans le cadre du projet de préparation BroadEU.Net financé par l'UE, qui testera la base du futur système de communication critique de l'UE[22]. En outre, des exercices conjoints pourraient être menés avec des experts en cybersécurité et en sécurité des drones, pour aborder les risques cyber posés par les drones, ainsi que les solutions numériques pour les neutraliser.

Actions clés pour les orientations pratiques et le soutien opérationnel

- **Le JRC publiera deux manuels dans le cadre du paquet antidrones.**
- **La Commission, en coopération avec les agences compétentes, soutiendra l'extension de la formation existante en lutte antidrones au secteur de la sécurité privée.**
- **La Commission intégrera les éléments antidrones dans la planification des exercices, en coopération avec les réseaux de services répressifs.**

D. Recherche et innovation

L'UE continue de financer son programme de recherche en matière de sécurité dans le cadre d'**Horizon Europe (2021-2027)**[23]. Ce programme de recherche en matière de sécurité représente environ 50 % des fonds publics investis dans l'UE et ses États membres dans le domaine de la sécurité. Du fait de sa contribution stratégique à diverses priorités de la politique de sécurité de l'UE, cette activité de recherche a déjà commencé à prendre en considération les menaces que représentent les drones. On peut notamment

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

[22] Le système de communication critique de l'UE fournira une infrastructure sécurisée et à large bande pour assurer l'interopérabilité transfrontière des systèmes de communication utilisés par les services répressifs et les services d'urgence dans l'espace Schengen.

[23] Auparavant, jusqu'à la fin de 2020, la recherche et l'innovation dans le domaine de la sécurité étaient financées par Horizon 2020 et par le 7e programme-cadre.

citer ALADDIN, qui fournit des solutions pour détecter et neutraliser les drones dans les zones réglementées[24] ou 7SHIELD, qui a étudié la mise au point de solutions antidrones pour les segments terrestres des infrastructures spatiales critiques. Le projet ALFA a lui aussi permis de mettre au point un système de détection et de suivi des drones utilisés pour la contrebande[25]. Ces initiatives de recherche et d'innovation peuvent être poursuivies dans le cadre d'Horizon Europe, être validées, ou être complétées par des actions entreprises dans le cadre du FSI-Police.

À l'avenir, la Commission facilitera l'échange plus systématique des résultats de projets pertinents avec les parties prenantes concernées, notamment par l'intermédiaire de la Communauté pour la recherche et l'innovation européennes en matière de sécurité[26]. Cela renforcerait encore l'échange de données spécifiques et permettrait de recenser plus efficacement les besoins des utilisateurs et de les communiquer au secteur afin d'orienter l'innovation. En outre, l'échange systématique des résultats des projets permettra d'établir un dialogue structuré avec les États membres et les parties prenantes pour recenser les technologies, outils et solutions prometteurs qui pourraient être adoptés par un groupe d'autorités des États membres. Dans ce contexte, la Commission examinera avec les États membres[27] la possibilité: (i) de créer un thème de recherche indépendant sur les solutions antidrones dans les futurs programmes de travail d'«Horizon Europe» et; et ii) de soutenir des systèmes innovants particuliers au moyen d'achats publics avant commercialisation[28]. Cette démarche est pleinement conforme à l'approche axée sur les capacités, exposée dans le document de travail des services de la Commission intitulé «Enhancing security through research and innovation» (renforcer la sécurité par la recherche et l'innovation)[29].

Il est essentiel de renforcer les synergies entre les industries européennes de la sécurité civile, de la défense et de l'espace dans le domaine des solutions antidrones, l'objectif étant de favoriser les synergies entre les trois secteurs dans les technologies liées aux drones et les technologies antidrones[30]. Dans la pratique, l'accroissement de ces synergies signifie que les projets de défense pourront bénéficier des développements innovants intervenant dans le domaine civil, tandis que l'aéronautique civile pourra bénéficier des développements dans le domaine de la défense.

Le **Fonds européen de la défense (FED)** et ses programmes précurseurs encouragent et soutiennent les activités de recherche et de développement collaboratives et transfrontières en matière de défense. Pour compléter et amplifier les efforts déployés par les États membres, le FED encourage la coopération entre les entreprises et les chercheurs, quels que soient leur taille et leur État membre d'origine dans l'Union. Les programmes précurseurs du FED ont déjà financé des projets antidrones dans le cadre de la recherche et du développement dans le domaine de la défense.

---

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

[25] ALFA constitue également la base du projet FSI «Courageous» et de ses activités d'essai.

La Communauté européenne pour la recherche et l'innovation en matière de sécurité (CERIS) réunit des acteurs de la recherche dans le domaine de la sécurité, à savoir des décideurs politiques, des utilisateurs finaux, des universitaires et des représentants de l'industrie ou de la sécurité civile: https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en

[27] Dans la configuration du comité du programme Horizon Europe «Sécurité civile pour la société».

[28] Les achats publics avant commercialisation (APAC) constituent une approche de la passation des marchés publics de services de recherche et de développement (R&D) qui a été exposée dans la communication sur les APAC [C (2007) 799 final] du 14.12.2007. Il s'agit d'un moyen important de stimuler l'innovation, car il permet au secteur public d'orienter le développement de nouvelles solutions en fonction de ses besoins.

[29] Document de travail des services de la Commission intitulé «Enhancing security through research and innovation», SWD (2021) 422 final du 15.12.2021.

[30] SWD(2022) 362 du 10.11.2022. Comme le décrit le rapport sur l'état d'avancement de la mise en œuvre du plan d'action sur les synergies entre les industries de la défense civile et de l'espace, dans le cadre de l'action 9.

Le programme de travail du FED pour 2023 contient une action de développement antidrones[31], dotée d'un budget indicatif de 43 millions EUR. L'action vise à développer des modules matériels ou logiciels pour une solution mobile globale visant à contrer un large éventail de drones, y compris les essaims.

Le principal résultat attendu du soutien du FED dans le domaine de la lutte antidrone en 2021-2027 est la mise au point d'un prototype de solution antidrone, en vue d'une éventuelle passation conjointe de marchés au niveau de l'UE. Les défis technologiques posés par les systèmes antidrones sont à l'étude dans le cadre du programme de l'UE pour l'innovation dans le domaine de la défense (EUDIS). En outre, EUDIS comprend un volet consacré aux incubateurs à double usage, afin de favoriser une meilleure collaboration entre les domaines civil et de la défense et de stimuler la maturation et l'adaptation technologiques.

Les travaux du JRC constituent un autre pilier essentiel de l'innovation, et en particulier de la recherche appliquée sur les moyens de contrer les menaces que représentent les drones. Dans le cadre du projet Drone C-UAS du JRC, ce dernier examinera les technologies de contre-mesures actives et passives et comment les utiliser pour garantir la sécurité des espaces publics et des infrastructures critiques.

À cette fin, et dans un premier temps, le JRC créera un **laboratoire vivant** pour étudier les technologies antidrones et la manière de les appliquer en conditions réelles. La configuration du laboratoire couvrira la planification, la préparation et la mise en œuvre d'une solution. Elle couvrira également la détection, le suivi, l'identification et la neutralisation, ainsi que l'intégration des parties prenantes et des processus. Le champ de mise en œuvre du laboratoire vivant couvrira l'intégration dans des systèmes de gestion du trafic d'aéronefs avec ou sans équipage à bord, en particulier l'U-space[32]. Le laboratoire vivant étudiera également comment intégrer l'apprentissage automatique et l'intelligence artificielle en vue d'améliorer les performances globales d'une solution antidrone.

À moyen terme, ce laboratoire vivant du JRC deviendra un **centre d'excellence de la lutte antidrone**.

Actions prioritaires pour tirer le meilleur parti de la recherche et de l'innovation

- **La Commission et les États membres décideront des besoins futurs de nouvelles solutions antidrones auxquels répondront les programmes européens de recherche et d'innovation pertinents, notamment Horizon Europe.**
- **La Commission et les États membres dresseront une liste de solutions antidrones prometteuses et évalueront la faisabilité d'achats publics avant commercialisation pour certaines de ces solutions.**
- **La Commission déterminera les idées, les technologies et les solutions à intégrer dans le développement des capacités de défense et soutiendra des projets visant à diffuser ces idées, technologies et solutions dans les secteurs civils.**
- **Le JRC mettra en place, à partir d'un laboratoire vivant, un centre d'excellence de la lutte antidrone.**

[31] Décision d'exécution de la Commission C(2023) 2296 du 29 mars 2023 relative au financement du Fonds européen de la défense établi par le règlement (UE) 2021/697 du Parlement européen et du Conseil et à l'adoption du programme de travail pour 2023 – Partie II

[32] Règlement d'exécution (UE) 2021/664 de la Commission du 22 avril 2021 relatif à un cadre réglementaire pour l'U-space. Le terme «U-space» a été adopté pour désigner la gestion du trafic d'aéronefs sans équipage à bord destinée à assurer une interaction en toute sécurité avec d'autres entités utilisant le même espace dans les zones urbaines et dans tout autre lieu.

E. Soutien financier

La Commission continuera d'apporter un soutien financier aux activités pertinentes de lutte antidrone, principalement par l'intermédiaire du FSI, mais aussi de l'instrument de soutien financier à la gestion des frontières et à la politique des visas (IGFV) et du programme Horizon Europe (pour les actions liées à la recherche et à l'innovation).

Le mécanisme thématique du FSI soutiendra: i) les réseaux européens de services répressifs; ii) les travaux en la matière du JRC; iii) le nouveau groupe d'experts antidrones; et iv) la création d'une plateforme d'échange d'informations. La Commission finance déjà des projets visant à piloter et à valider des systèmes de détection et de localisation des drones qui franchissent illégalement les frontières extérieures de l'UE. Ces projets sont fondés sur les résultats de projets de recherche antérieurs financés par l'UE[33].

Au titre du mécanisme thématique du FSI, la Commission lancera, au premier semestre de 2024, un **appel à propositions** destiné à soutenir le déploiement de solutions antidrones à fort potentiel d'adoption.

Les États membres seront encouragés à mettre en œuvre la présente communication et à reprendre les résultats de la recherche sur les solutions antidrones financée par l'UE dans leurs programmes relevant du FSI.

Actions clés pour le soutien financier

- **Dans le cadre des programmes de travail du mécanisme thématique du FSI pour la période 2026-2027, la Commission lancera un appel à propositions relatif aux solutions antidrones.**
- **Les États membres seront encouragés à utiliser pleinement leurs programmes relevant du FSI pour la période 2021-2027, afin de trouver et d'appliquer des solutions efficaces de lutte contre les drones.**

F. Étude de mesures réglementaires

Bien que l'UE ait réglementé l'utilisation légitime des drones, il n'existe actuellement, au niveau de l'UE, aucune réglementation spécifique en matière de lutte antidrone qui établisse un cadre commun harmonisé pour les autorités, les opérateurs et les fabricants des États membres. Même si les lignes directrices non contraignantes de l'AESA concernant les incidents liés aux drones dans les aéroports (mentionnées précédemment dans la présente communication) ont été accueillies favorablement par le secteur, leur

[33] À titre d'exemple, on peut citer les projets financés au titre des actions spécifiques de l'IGFV concernant: i) l'innovation pour les frontières maritimes/littorales et/ou terrestres et ii) Frontex. Certains projets financés par l'action spécifique sur l'innovation pour les frontières maritimes/littorales et/ou terrestres sont axés sur la mise à l'essai pilote de technologies de surveillance innovantes. Il existe également une action spécifique pour l'achat et la mise à disposition d'équipements destinés à être déployés par les autorités frontalières européennes afin de détecter et de localiser des drones qui franchissent les frontières aux fins d'activités illégales ou criminelles. Cette action spécifique permettra aux États membres de se procurer deux systèmes antidrones. Pour apporter une valeur ajoutée européenne, à la demande de Frontex lors des négociations bilatérales annuelles, l'équipement technique acheté au titre des actions spécifiques doit être mis à la disposition de Frontex pour une durée maximale de quatre mois par an, en vue de son utilisation dans le cadre de ses opérations conjointes.

caractère non contraignant et leur portée limitée les rendent insuffisantes pour atténuer la menace que représentent les drones non coopératifs. La nécessité de prévenir efficacement l'utilisation non autorisée de drones ne cessant de croître, la Commission, en étroite collaboration avec des experts des États membres, analysera plus avant la nécessité d'adopter des mesures législatives ou non législatives à l'avenir. À cette fin, la Commission lancera une **étude cartographique** spécifique, en vue d'établir le paysage réglementaire actuel. Cette étude cartographique devrait également tenir compte du cadre de l'OACI et des évolutions à ce niveau, et du fait que les règles visant à contrer les menaces potentielles posées par les drones ne devraient pas entraver indûment les opérations légitimes, notamment les activités des pilotes de loisirs organisés.

Les aéroports de l'UE disposent de règles de sécurité détaillées et complètes qui recouvrent également la menace provenant des drones. Pour que les autorités aéronautiques et les aéroports soient plus résilients face aux risques posés par les drones, et conformément à une approche factuelle, la Commission, en coopération avec les États membres, **recensera les éventuels autres points faibles de la protection contre les drones non coopératifs, dans le cadre d'une évaluation des risques pour la sécurité, qui pourrait exiger des modifications réglementaires**.

Un dialogue structuré avec le secteur et les fabricants de drones sur les mesures de sécurité dès la conception est nécessaire dans ce contexte (par exemple, des systèmes robustes contre l'usurpation, des limitations de capacité, le partage de protocoles de communication et des mises à jour pour les bases de données antidrones).

Actions clés pour l'étude de mesures réglementaires

- **La Commission procédera à une étude cartographique afin de recenser les besoins réglementaires et les possibilités d'harmoniser les législations et les procédures des États membres.**
- **Conformément à une approche factuelle, la Commission réalisera une évaluation des risques pour la sécurité aérienne liés aux drones, afin de recenser les éventuels autres points faibles des aéroports, qui pourraient exiger des changements réglementaires.**
- **La Commission entamera un dialogue structuré avec le secteur sur la nécessité et la nature d'éventuelles mesures spécifiques supplémentaires relatives à la sécurité des drones.**

III. LA VOIE A SUIVRE

Pour que les rapides évolutions technologiques et le nombre croissant de drones n'entraînent pas une augmentation incontrôlée des menaces que représentent les drones non coopératifs, il est nécessaire d'intensifier la coopération au niveau de l'UE, sur la base de la politique globale antidrones de l'UE exposée dans la présente communication. À cette fin, les activités actuelles au niveau de l'UE seront poursuivies et complétées par la série d'actions clés énumérées dans la présente communication, qui seront mises en œuvre dans les années à venir.

Les activités décrites dans la présente communication couvriront la période allant jusqu'en 2030. En 2027 au plus tard, un bilan à mi-parcours sera effectué par l'intermédiaire du groupe d'experts, tandis qu'une révision complète du programme de lutte antidrone de l'UE est prévue pour 2030 au plus tard.