Consiglio
dell'Unione europea

Bruxelles, 18 ottobre 2023
(OR. en)

14394/23

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

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	18 ottobre 2023
Destinatario:	Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2023) 659 final
Oggetto:	COMUNICAZIONE DELLA COMMISSIONE AL CONSIGLIO E AL PARLAMENTO EUROPEO sul contrasto alle potenziali minacce poste dai droni

Si trasmette in allegato, per le delegazioni, il documento COM(2023) 659 final.

All.: COM(2023) 659 final

COMMISSIONE
EUROPEA

Bruxelles, 18.10.2023
COM(2023) 659 final

COMUNICAZIONE DELLA COMMISSIONE AL CONSIGLIO E AL PARLAMENTO EUROPEO

sul contrasto alle potenziali minacce poste dai droni

I. INTRODUZIONE

La presente comunicazione definisce la politica dell'UE per contrastare le potenziali minacce poste dai sistemi di aeromobili senza equipaggio (Unmanned Aircraft System, UAS) non cooperativi, noti comunemente come "droni". Fa parte di un più ampio pacchetto anti-droni che comprende anche due manuali contenenti orientamenti pratici sugli aspetti tecnici principali di tale politica. Il pacchetto è stato annunciato nell'ambito di un'azione faro prevista dalla comunicazione della Commissione *Strategia 2.0 per i droni per un ecosistema intelligente e sostenibile di aeromobili senza equipaggio in Europa*[1]. La presente comunicazione risponde alla necessità di: i) offrire un quadro politico globale e armonizzato; ii) pervenire a una comprensione comune delle procedure applicabili per far fronte alle minacce in continua evoluzione poste dai droni; e iii) tener conto dei rapidi sviluppi tecnologici.

A. Integrare il quadro dell'UE sui droni

L'uso legittimo dei droni è un fattore cruciale per realizzare la duplice transizione verde e digitale, come indicato nella strategia 2.0 dell'UE per i droni. I droni svolgono un ruolo importante, in particolare nei settori dei trasporti, della difesa, del commercio e dei servizi. Si prevede che il numero di droni utilizzati nell'UE crescerà sensibilmente nei prossimi anni e che si registreranno notevoli miglioramenti in termini di velocità, agilità, raggio d'azione massimo, carico utile, precisione dei sensori e uso dell'intelligenza artificiale. Tali sviluppi aumenteranno il numero di possibili usi legittimi e legali dei droni. Affinché questo potenziale si realizzi, è necessario però affrontare le potenziali minacce poste dai droni non cooperativi.
Un drone non cooperativo dev'essere definito in base alla natura della non cooperazione, che potrebbe comprendere azioni criminose, illegali (violazione intenzionale delle norme) o amatoriali (per ignoranza o negligenza).

La presente comunicazione tratta le minacce poste dai droni progettati per usi civili, con particolare riguardo alle minacce che interessano il contesto civile. Benché i droni progettati a fini di difesa non siano al centro dell'attenzione nella presente comunicazione, rimangono comunque diverse interconnessioni con il settore della difesa, tra cui l'uso potenziale di droni di dimensioni minori, progettati a fini di difesa, da parte di criminali o terroristi, nonché le sinergie fra tecnologie diverse per contrastare i droni. I droni progettati a fini di difesa potrebbero occupare lo stesso spazio aereo dei droni civili, e in questi casi devono essere identificabili dalle autorità competenti a fini di conoscenza situazionale.

Oggetto della presente comunicazione è specificamente il *contrasto* alle potenziali minacce poste dai droni. La comunicazione pertanto non si estende al più ampio ruolo dei droni nel settore della sicurezza interna, ossia al loro uso a fini di contrasto, pubblica sicurezza e incolumità pubblica.

La responsabilità di contrastare le minacce poste dai droni non cooperativi spetta in primo luogo alle autorità degli Stati membri. Gli Stati membri possono giovarsi anche dell'azione svolta a livello di Unione europea; ciò consente una più intensa collaborazione e un più stretto coordinamento dei mezzi e degli strumenti impiegati a tale scopo. La presente comunicazione pertanto promuove varie azioni connesse alla creazione di comunità e alla condivisione di informazioni. Essa inoltre offre agli Stati membri orientamenti, formazione, finanziamenti e procedure operative.

[1] Strategia 2.0 per i droni per un ecosistema intelligente e sostenibile di aeromobili senza equipaggio in Europa (COM(2022) 652 final) del 29 novembre 2022.

Gli incidenti potenzialmente pericolosi che coinvolgono droni sono divenuti più frequenti, sia all'interno dell'UE sia al suo esterno. È pertanto importante favorire l'adozione di soluzioni anti-droni fisiche o digitali da parte delle autorità di contrasto e di altre autorità pubbliche dell'UE, nonché di altri operatori di infrastrutture critiche. L'elaborazione di una politica anti-droni dell'UE contribuirà a rafforzare le procedure necessarie a mettere alla prova l'efficienza delle nuove soluzioni disponibili e a favorire l'uso mirato della ricerca e dell'innovazione in tale settore. Con la preparazione di questa politica anti-droni la Commissione contribuisce a rafforzare il mercato dell'UE per le soluzioni anti-droni. In tal modo si promuoverà lo sviluppo di una maggiore autonomia strategica e di una sovranità tecnologica rafforzata per l'UE, anche per quanto riguarda le tecnologie critiche. Si potenzierà inoltre la capacità europea di sviluppare soluzioni all'avanguardia nei settori aerospaziale, della difesa e della sicurezza civile, riducendo altresì la dipendenza da fornitori non europei. Quest'azione si baserà sui risultati della valutazione delle dipendenze in materia di tecnologie critiche[2] e fornirà ulteriori dati e analisi; inoltre: i) fornirà alla Commissione informazioni che permetteranno di comprendere meglio l'impiego delle tecnologie critiche e le dipendenze da fornitori non europei; e ii) offrirà una solida panoramica sul livello di dipendenza.

Inoltre, per contrastare le minacce poste dai droni non cooperativi dal punto di vista delle autorità pubbliche, è altresì importante: i) disporre di quadri e procedure chiari e armonizzati; ii) conferire ai portatori di interessi pubblici e privati responsabili poteri ben definiti per intervenire contro i droni non cooperativi; e iii) favorire la collaborazione tra portatori di interessi non sempre abituati a lavorare insieme (autorità di contrasto e dell'aviazione civile, operatori, fabbricanti, operatori delle reti mobili). La presente comunicazione propone azioni volte a: i) pervenire a una comprensione comune delle procedure applicabili per far fronte alle minacce poste dai droni; e ii) individuare eventuali esigenze in termini di armonizzazione delle normative.

B. Affrontare una minaccia attuale e in rapida evoluzione

Sia la strategia dell'UE per l'Unione della sicurezza[3] sia il programma di lotta al terrorismo dell'UE[4] mettono in evidenza che la minaccia dei droni non cooperativi è fonte di grave preoccupazione in Europa.

La rapida evoluzione delle capacità dei droni pone un crescente rischio per la sicurezza Negli ultimi anni sono stati scoperti piani che prevedevano la prova e l'uso di droni per attentati terroristici[5]. Sono stati anche avvistati droni sospetti intorno a infrastrutture critiche, come impianti energetici, aeroporti e porti, a dimostrazione del potenziale uso improprio dei droni per la raccolta di informazioni a fini ostili. I droni sono utilizzati da criminali per il contrabbando transfrontaliero, oppure per favorire altre operazioni illecite, tra cui il traffico di stupefacenti. I droni possono anche essere all'origine di rischi informatici, ad esempio se vengono usati per la ricognizione digitale. Le minacce poste dai droni non sono esclusivamente di natura tecnica. Oggi è possibile individuare e identificare gran parte dei droni progettati a fini civili, ma rimane assai arduo intercettarli o neutralizzarli (ad esempio prenderne il controllo, farli

[2] Una valutazione approfondita svolta nel 2022 all'interno della Commissione in materia di sistemi autonomi.

[3] Strategia dell'UE per l'Unione della sicurezza, (COM(2020) 605 final) del 24 luglio 2020.

[4] Un programma di lotta al terrorismo dell'UE: prevedere, prevenire, proteggere e reagire, (COM(2020) 795 final) del 9 dicembre 2020.

[5] Alcuni esempi: i) il piano di un jihadista fanatico condannato da un tribunale spagnolo nell'ottobre 2022 per aver pianificato un attentato in uno stadio durante un'importante partita di calcio, utilizzando un drone imbottito di esplosivo; e ii) un cittadino belga condannato per aver tentato di utilizzare i droni in un attacco bomba contro una prigione.

atterrare in sicurezza o abbatterli), spesso perché mancano le autorizzazioni giuridiche per farlo. Ciò vale soprattutto per gli operatori privati di infrastrutture critiche. Nelle future valutazioni del rischio effettuate ai sensi della direttiva relativa alla resilienza dei soggetti critici[6] sarà pertanto opportuno prendere in considerazione il contrasto alle minacce poste dai droni.

Il quadro delle minacce diviene ancora più chiaro se si considerano gli incidenti verificatisi in paesi vicini all'UE e in altre parti del mondo. I droni si sono dimostrati un tipo di piattaforma a duplice uso, efficace ed efficiente in termini di costi, che ha stimolato l'innovazione nel settore della difesa durante la guerra russa contro l'Ucraina. L'uso dei droni progettati a fini civili in attacchi distruttivi anche in altri conflitti armati (ad esempio in Yemen o in Siria) è un fenomeno che può rivestire implicazioni per la sicurezza interna dell'UE. Il modus operandi dei gruppi terroristici e le rafforzate competenze nell'uso dei droni "in pronta consegna" potrebbero raggiungere le nostre frontiere e rappresentare una minaccia. Lo stesso vale per l'uso di droni nel tentativo di perpetrare assassinii mirati[7].

Le soluzioni anti-droni tuttavia non sono necessarie soltanto per contrastarne l'uso mirato e malevolo, ma anche per scongiurare gli incidenti provocati da negligenza o imprudenza. Gran parte degli utenti di droni nell'UE (in particolare i piloti remoti professionisti provvisti di licenza o i piloti privati riuniti in associazioni) rispetta le norme, i regolamenti e le limitazioni tecniche vigenti. Gli utenti di droni ignoranti, negligenti o criminali sono però responsabili dei molti pericolosi incidenti che coinvolgono i droni in tutta l'UE. Gli eventi pubblici su larga scala sono particolarmente vulnerabili a tali turbative; lo stesso vale per alcuni settori critici come il trasporto aereo. L'uso illecito dei droni inoltre può influire anche sulla sicurezza personale e sul diritto alla riservatezza dei singoli cittadini, soprattutto quando i droni operano in zone residenziali.

C. Restare al passo con gli sviluppi tecnologici

Per proteggere le nostre società dai droni malevoli e non cooperativi è necessario adottare misure di contrasto economicamente accessibili e affidabili che consentano soluzioni flessibili. Tali soluzioni di solito trattano tre aspetti, il rilevamento, il tracciamento e l'identificazione, mentre le autorità pubbliche sono interessate anche ad altri due aspetti, la neutralizzazione e l'analisi forense.

Sia nel settore della difesa che in quello della sicurezza civile si stanno già sviluppando e collaudando soluzioni anti-droni innovative. La loro immissione sul mercato e la loro adozione da parte degli utenti finali potrebbero essere facilitate da un quadro generale dell'UE sul contrasto ai droni, come quello promosso dalla presente comunicazione. A causa dell'ampia varietà dei contesti e degli scenari operativi, non è tuttavia possibile ricorrere a un approccio univoco e standardizzato all'attuazione delle misure anti-droni.

Le misure anti-droni devono pertanto essere adattate alle diverse esigenze e ai diversi contesti operativi. Dal punto di vista delle autorità competenti per la sicurezza interna, potrebbero verificarsi situazioni in cui la completa distruzione fisica di un drone sia l'opzione migliore (e anche l'unica), ad esempio per scongiurare un attentato imminente contro persone o infrastrutture. In altri casi, come l'uso criminoso o la raccolta di informazioni a fini ostili, vi è un forte interesse ad assicurarsi il controllo del drone per farlo atterrare cercando al contempo di garantirne l'integrità, in modo da consentire l'ottimale svolgimento delle

[6] Direttiva (UE) 2022/2557, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici (GU L 333 del 27.12.2022, pag. 164).

[7] Tra gli esempi figurano il tentativo fallito di assassinare il presidente del Venezuela, e l'uso di droni da parte dei cartelli della droga messicani contro i rappresentanti di altre organizzazioni criminali.

indagini forensi. Da qui la necessità di soluzioni informatiche sofisticate per prendere il controllo del sistema operativo del drone.

Lo sviluppo di sensori per individuare i droni in maniera più precisa è una delle tendenze tecnologiche da monitorare e sfruttare attivamente. Le attuali capacità dei sensori possono essere ulteriormente sviluppate, non soltanto per individuare un drone, ma anche per valutare, mediante l'analisi del modello di volo, la definizione del carico utile e l'individuazione delle attrezzature, le minacce che esso comporta. I sensori e sistemi di individuazione devono potersi adattare alle mutevoli forme e capacità dei droni (velocità, agilità, capacità di usare falsi bersagli, eccetera). La capacità delle autorità pubbliche e degli operatori privati delle infrastrutture critiche di analizzare i dati di tali sensori sarà sempre più importante. Anche l'intelligenza artificiale avrà un ruolo da svolgere, ad esempio mediante la generazione automatica di segnalazioni, il calcolo del rischio, la previsione delle rotte o dei siti di atterraggio. Occorre pertanto monitorare continuamente le nuove tendenze che interessano i mercati dei droni e integrarle nelle soluzioni anti-droni. Il monitoraggio di questi sviluppi tecnologici dovrebbe consentire alle autorità dell'UE di identificare le priorità di investimento e sostenere gli sviluppi più adatti a soddisfare le esigenze operative espresse dalle autorità di contrasto e dagli operatori privati degli Stati membri.

Per quanto riguarda l'intercettazione e la neutralizzazione, sono necessarie ulteriori prove su tecnologie idonee in diversi contesti e scenari. Nel settore della difesa sono state individuate alcune soluzioni per distruggere fisicamente un drone o catturarlo mentre è ancora in aria, riducendo così la produzione di detriti che potrebbero ferire le persone o danneggiare oggetti. Tra queste soluzioni figurano l'energia diretta sotto forma di laser ad alta energia e l'uso di radiofrequenza ad alta potenza e sistemi di cattura a rete, nonché strumenti digitali per ottenere il controllo dei droni non cooperativi.

Per le attività di indagine e di contrasto sarebbe particolarmente utile poter neutralizzare la minaccia di un drone potendo agire sul sistema di controllo e facendolo atterrare in sicurezza, affinché le autorità e i responsabili delle indagini possano accedere nel modo migliore ai potenziali elementi probatori di tipo fisico e digitale. Pertanto si renderebbe necessaria un'ampia gamma di soluzioni diverse, convalidate per finalità diverse, in modo da soddisfare le esigenze della sicurezza interna. Occorre quindi promuovere lo sviluppo di un vero mercato e di un contesto innovativo per soluzioni anti-droni che soddisfino le esigenze della sicurezza civile. Diversamente è improbabile che gli sviluppi di soluzioni anti-droni possano tenere il passo con il numero e le capacità crescenti dei droni stessi. È altresì essenziale articolare e segmentare questo mercato per consentire alle autorità competenti di individuare le soluzioni più idonee alle loro esigenze.

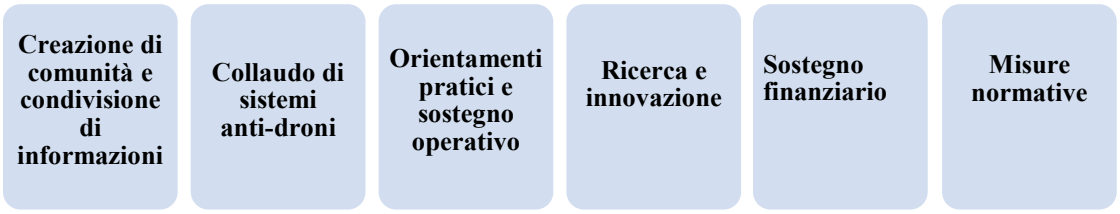
È anche importante monitorare i sistemi utilizzati dai criminali per contrastare le misure anti-droni; si tratta di dispositivi trasportati dal drone o azionati da terra e concepiti per bloccare specifiche misure anti-droni.

Molti sistemi anti-droni, infine, sono sviluppati anche a fini di difesa. Benché abbiano requisiti diversi, condividono spesso caratteristiche e tecnologie comuni con i sistemi progettati per usi civili, il che porta a un'esigenza di stretta cooperazione con il settore della difesa.

Questo panorama tecnologico richiede anche un quadro normativo coerente e continuamente aggiornato per l'impiego di sistemi anti-droni.

II. ELABORARE UNA POLITICA ANTI-DRONI DELL'UE

La Commissione ha collaborato con gli Stati membri e altri portatori di interessi sulla potenziale minaccia posta dai droni dal 2016, quando si è tenuto il primo seminario dell'UE anti-droni. Da allora è stato introdotto un ampio ventaglio di iniziative per favorire la creazione di comunità, la condivisione di informazioni, lo sviluppo di migliori pratiche e il finanziamento dedicato di progetti. In seguito alle discussioni con gli esperti degli Stati membri, la Commissione continuerà a sostenere queste iniziative in corso e nel contempo svilupperà e integrerà nuovi filoni di attività per elaborare una completa e articolata politica anti-droni dell'UE. Il lavoro si articolerà nelle sei seguenti attività principali:



A. Creazione di comunità e condivisione di informazioni

A livello di Unione europea un gran numero di reti e attori diversi sta lavorando per individuare soluzioni anti-droni. È dunque necessario razionalizzare e orientare le attività future in termini politici, tecnici e operativi allo scopo di: i) creare comunità operative di portatori di interessi; ii) realizzare un'effettiva condivisione di informazioni e migliori pratiche; e iii) evitare duplicati.

La Commissione promuoverà le iniziative esistenti a livello tecnico e istituirà un **gruppo di esperti anti-droni della Commissione** per fornire consulenza a livello politico. Il gruppo potrà offrire un contributo strategico a varie politiche dell'UE rilevanti per le attività anti-droni, come nei settori della sicurezza interna, della gestione delle frontiere o della resilienza delle infrastrutture critiche. A tale scopo il gruppo di esperti coopererà con altri gruppi di esperti e, se del caso, con i pertinenti gruppi di lavoro del Consiglio.

Si tengono regolarmente seminari e riunioni di esperti su soluzioni e politiche anti-droni, che riuniscono rappresentanti politici, esperti tecnici e ricercatori della Commissione, degli Stati membri, di altre istituzioni dell'UE, di agenzie dell'UE, di progetti finanziati dall'UE, di organizzazioni internazionali e di paesi partner. Tali attività hanno portato al continuo coinvolgimento di tutti i portatori di interessi, facilitando notevolmente la cooperazione pratica e operativa. A tale scopo la Commissione ha istituito il **polo d'informazione anti-droni**[8] che attualmente conta oltre 300 membri. Questa piattaforma online è aggiornata periodicamente e contiene diverse fonti di informazione, come i risultati dei pertinenti progetti finanziati dall'UE, presentazioni, relazioni e un bollettino semestrale.

Un'altra componente importante della creazione di comunità e della condivisione di informazioni, soprattutto per quanto riguarda le esigenze operative delle attività di contrasto, ha luogo nell'ambito delle **reti dei servizi di contrasto europee** finanziate dall'Unione. Ad esempio tutte le reti seguenti hanno avviato l'attività di contrasto alle minacce poste dai droni: la rete europea dei servizi tecnologici per attività di contrasto (ENLETS); la rete dell'UE che coordina le unità di polizia e guardie di frontiera negli aeroporti (AIRPOL); la rete dell'UE che riunisce le unità speciali d'intervento (ATLAS); e la rete "alto rischio di sicurezza" dell'UE. Il gruppo di lavoro della rete dei servizi di contrasto, di recente istituzione, è un'iniziativa della DG HOME, volta a promuovere la cooperazione tra le reti di polizia e finanziata dalla Commissione[9], che intende razionalizzare i filoni delle attività in corso nel settore del contrasto ai droni nell'ambito di un sottogruppo di lavoro dedicato.

L'**Agenzia dell'Unione europea per la sicurezza aerea (AESA)** ha elaborato orientamenti non vincolanti per aiutare le autorità e gli aeroporti a prepararsi e rispondere agli incidenti che coinvolgono droni e a riprendersi dagli stessi[10]. Per promuovere attività di sostegno informato e l'elaborazione di politiche a livello di Unione europea, è essenziale avviare scambi di informazioni attendibili e dettagliati sugli incidenti che coinvolgono droni nell'UE, oltre agli scambi che già hanno luogo in aree critiche specifiche come gli aeroporti. Pur nel pieno rispetto della riservatezza delle indagini vi è un significativo

[8] Utilizzando la piattaforma CIRCABC dell'UE, sostenuta dal programma ISA², che promuove soluzioni di interoperabilità per le amministrazioni pubbliche europee.

[9] Il gruppo di lavoro (informale) della rete dei servizi di contrasto (LENWG), presieduto dalla Commissione, si è riunito per la prima volta il 20 marzo 2023 per promuovere una cooperazione più efficace tra le reti finanziate dalla DG HOME. Dopo un periodo di valutazione di dodici mesi, il LENWG potrebbe essere trasformato in un vero e proprio gruppo di esperti della Commissione.

[10] Nel marzo 2021 l'Agenzia dell'Unione europea per la sicurezza aerea (AESA) ha pubblicato una serie di orientamenti per la gestione degli incidenti che coinvolgono droni negli aeroporti: Gestione degli incidenti che coinvolgono droni negli aeroporti (non disponibile in IT).

potenziale per migliorare la condivisione delle informazioni in materia di: i) metodi usati dagli operatori di droni non cooperativi; ii) modelli specifici delle minacce; e iii) potenziali rischi identificati. Per favorire e armonizzare la condivisione di tali informazioni relative agli incidenti, la Commissione ha distribuito agli Stati membri un modello per la segnalazione degli incidenti che coinvolgono droni. Per migliorare la qualità e intensificare la frequenza della condivisione di informazioni, la Commissione esplorerà la possibilità di istituire una **piattaforma digitale contenente informazioni sugli incidenti che coinvolgono droni,** destinata alle autorità pubbliche competenti. Questa piattaforma potrebbe servire per identificare e confrontare adeguatamente i principali incidenti di sicurezza che coinvolgono droni nell'Unione europea. Può rientrare in questo quadro anche la dimensione informatica, giacché i droni sono utilizzati non solo per la ricognizione visiva ma anche per quella digitale. Tale piattaforma sarebbe coerente con gli obblighi di segnalazione ai sensi del regolamento (UE) n. 376/2014[11] e non comporterebbe una duplicazione degli sforzi.

La Commissione organizzerà inoltre periodiche riunioni classificate per promuovere lo scambio, in un formato adeguato, di insegnamenti tratti dagli incidenti.

Azioni fondamentali per la creazione di comunità e la condivisione di informazioni

- **La Commissione istituirà un gruppo di esperti, formato da esperti degli Stati membri e altri portatori di interessi in materia di attività anti-droni.**
- **La Commissione esplorerà la possibilità di sviluppare una piattaforma digitale contenente informazioni sugli incidenti che coinvolgono droni.**
- **La Commissione organizzerà riunioni periodiche per agevolare lo scambio di informazioni classificate tra Stati membri in merito ai principali incidenti di sicurezza che coinvolgono droni.**

B. Collaudo di sistemi anti-droni: identificazione e sperimentazione delle soluzioni

Gli Stati membri e le autorità locali possono scegliere tra una vasta gamma di soluzioni commerciali anti-droni , informatiche e non informatiche, disponibili sul mercato. Si tratta di una scelta difficile, soprattutto per le entità locali che non dispongono di capacità tecniche sufficienti. La Commissione aiuterà le autorità degli Stati membri a compiere la scelta corretta in funzione delle loro esigenze operative, offrendo consulenza e orientamenti tramite l'apposito gruppo di esperti anti-droni e il lavoro del Centro comune di ricerca (JRC) della Commissione.

A livello di Unione europea le attività di prova di sistemi anti-droni, che sono state avviate nel 2019, mirano a sviluppare una metodologia comune per valutare i sistemi utilizzabili dalle autorità di contrasto e da altre autorità pubbliche per rilevare, tracciare e identificare droni potenzialmente malevoli. Pilastro centrale di queste attività è il progetto "Courageous"[12] (2021-2024), finanziato dal Fondo Sicurezza interna dell'Unione europea – Polizia (ISF - Polizia). "Courageous" è diretto dall'accademia militare reale del Belgio e ha il compito di: i) identificare gli scenari standard pertinenti per le prove di sistemi anti-droni; ii) elaborare requisiti funzionali e di prestazione; e iii) elaborare una metodologia di prova. Il progetto prevede anche la prova delle prestazioni di sensori e sistemi integrati. Gli esiti del progetto sono costantemente condivisi con gli Stati membri e con organizzazioni internazionali e paesi partner

[11] Regolamento (UE) n. 376/2014 del Parlamento europeo e del Consiglio, del 3 aprile 2014, concernente la segnalazione, l'analisi e il monitoraggio di eventi nel settore dell'aviazione civile, che modifica il regolamento (UE) n. 996/2010.

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

selezionati. Una volta completato il progetto, la Commissione e il consorzio "Courageous" presenteranno agli Stati membri opzioni per assicurare la sostenibilità del progetto e raccomanderanno una **metodologia per gli impianti per le prove anti-droni** negli Stati membri.

Gli sviluppi tecnologici rilevanti per i sistemi anti-droni sono in rapida evoluzione. Occorre pertanto integrare le attività di prova con un costante monitoraggio delle tendenze al fine di identificare sia le soluzioni più promettenti, sia le potenziali nuove sfide che si profilano per lo sviluppo di sistemi anti-droni. Il JRC ha acquisito la capacità di effettuare questo monitoraggio e identificare le nuove sfide. Ciò costituisce un vantaggio per gli Stati membri e offre un prezioso contributo alle iniziative di prove a livello di Unione europea. Le informazioni saranno condivise attraverso canali appropriati, in particolare il gruppo di esperti.

La normazione è uno strumento utile per armonizzare le soluzioni tecnologiche. Il progetto "Courageous" prevede una consulenza specifica per la fase di pre-normazione, sulla cui base è possibile valutare in maniera più approfondita la fattibilità e la necessità di processi di normazione. A livello di Unione europea sono stati compiuti progressi soddisfacenti nello sviluppo di requisiti di prestazione facoltativi per le apparecchiature di individuazione al di fuori del settore dell'aviazione (ad esempio per le apparecchiature a raggi X e i metal detector[13]). Insieme a esperti degli Stati membri e dell'industria, la Commissione svilupperà anche **requisiti di prestazione facoltativi** per i sistemi anti-droni, se del caso in modo coerente con le disposizioni del regolamento sulla cibersicurezza[14]. Stabilire un processo di certificazione per i sistemi anti-droni dovrebbe rimanere un obiettivo a medio termine. Se del caso si prenderà in considerazione anche l'opportunità di introdurre norme ibride applicabili al settore civile e a quello della difesa.

La normazione e la certificazione della cibersicurezza dei sistemi anti-droni, in particolare se questi provengono da fornitori di paesi terzi, costituiscono un altro elemento essenziale. In questa fase permane l'incertezza sul livello di protezione dei dati raccolti da taluni sistemi di individuazione. Inoltre è importante prevenire, per quanto possibile, la pirateria e l'uso improprio dei sistemi anti-droni garantendo la ciberresilienza delle loro componenti.

Nel settembre 2022 la Commissione ha adottato una proposta di regolamento sulla ciberresilienza[15], volta a stabilire norme generali in materia di cibersicurezza per i prodotti con elementi digitali - hardware e software - che entrano nel mercato unico. La nuova proposta di regolamento intende introdurre requisiti obbligatori di cibersicurezza per questi prodotti. Tali requisiti comprenderanno la cibersicurezza fin dalla progettazione e per impostazione predefinita, nonché requisiti per contrastare la vulnerabilità. Com'è stato proposto dalla Commissione, i sistemi di droni che non sono sviluppati esclusivamente a fini militari o di sicurezza nazionale, e che non sono già certificati in conformità del regolamento (UE) 2018/1139, sarebbero coperti da queste nuove norme in quanto prodotti con elementi digitali, a eccezione di quelli sviluppati esclusivamente a fini militari o di sicurezza nazionale.

[13] Raccomandazione della Commissione sui requisiti di prestazione facoltativi per le apparecchiature a raggi X utilizzate negli spazi pubblici (C(2022) 4179 final).

[14] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione.

[15] Proposta di regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020 (COM(2022) 454 final).

Azioni fondamentali per le prove di sistemi anti-droni

- **La Commissione lavorerà all'attuazione di una metodologia di prova armonizzata per i sistemi anti-droni, sulla base degli esiti del progetto "Courageous".**
- **Il JRC redigerà una relazione annuale sugli sviluppi tecnici della tecnologia anti-droni.**
- **La Commissione, in cooperazione con i gruppi di esperti pertinenti, come le reti dei servizi di contrasto ENLETS, HRSN, AIRPOL, svilupperà un insieme di requisiti di prestazione facoltativi per i sistemi anti-droni.**

C. Orientamenti pratici e sostegno operativo

Varie pubblicazioni del JRC hanno già identificato nel contrasto alle minacce poste da droni non cooperativi una priorità, ad esempio gli orientamenti sulla protezione del perimetro degli edifici[16] e lo studio specifico sulle cariche esplosive trasportate da droni[17]. Inoltre la recente pubblicazione[18] sul concetto di sicurezza fin dalla progettazione evidenzia l'importanza di integrare misure protettive proporzionate, appropriate e multifunzionali secondo un approccio meditato fin dall'inizio della fase di studio e progettazione di un progetto, nonché misure volte a contrastare attentati in cui si faccia uso di droni.

Inoltre il manuale dell'AESA sulla *Gestione degli incidenti che coinvolgono droni negli aeroporti* fornisce orientamenti sullo sviluppo di modalità e procedure adeguate a sostegno di un sistema di risposta agli incidenti negli aeroporti che sia rapido, efficace e proporzionato. In tal modo è possibile evitare o ridurre al minimo le interruzioni del traffico aereo e le chiusure delle piste o dello spazio aereo, e la chiusura degli aeroporti rimarrebbe una soluzione di ultima istanza. L'attività dell'AESA tiene conto degli orientamenti dell'Organizzazione per l'aviazione civile internazionale in materia di sicurezza aerea[19].

Il JRC ha elaborato due nuovi manuali:

- ***Protezione dai sistemi aeromobili senza equipaggio:*** *Manuale sulla protezione dai sistemi di aeromobili senza equipaggio per le infrastrutture critiche e gli spazi pubblici - Un approccio in cinque fasi per i portatori di interessi C-UAS*

- ***Protezione dai sistemi aeromobili senza equipaggio:*** *Manuale sulla valutazione dei rischi UAS e sui principi per l'aumento della sicurezza fisica di edifici e siti*.

Per quanto riguarda la **formazione**, il progetto DroneWISE finanziato dall'UE[20] ha realizzato un pacchetto di strategie di comando, controllo e coordinamento anti-droni per il primo intervento. Il progetto ha elaborato anche 10 moduli formativi, un manuale e un portale di formazione online. I moduli

[16] Karlos, V. e Larcher, M., Orientamenti - Protezione del perimetro degli edifici (non disponibile in IT), EUR 30346 EN, Ufficio delle pubblicazioni dell'Unione europea, Lussemburgo, 2020.

[17] La minaccia degli UAS che utilizzano esplosivi è stata trattata dal JRC in: Larcher M, Karlos V, Valsamos G, Solomos G: Studio di scenario: droni che trasportano esplosivi (non disponibile in IT), JRC107683, 2018

[18] Commissione europea, Sicurezza fin dalla progettazione: Protezione degli spazi pubblici dagli attentati terroristici (non disponibile in IT), JRC131172, 2022.

[19] Il manuale per la sicurezza aerea dell'ICAO (doc. 8973 – Riservato) coadiuva gli Stati membri nell'attuazione dell'allegato 17 della convenzione di Chicago fornendo orientamenti sull'applicazione delle proprie norme e procedure raccomandate (SARP) Aviation Security Manual.

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

sono stati integrati nel piano formativo dell'Agenzia dell'Unione europea per la formazione delle autorità di contrasto (CEPOL). Un altro progetto del Fondo sicurezza interna dedicato alla formazione anti-droni è Skyfall.
È necessario estendere ulteriormente la formazione disponibile ai fornitori privati di servizi di sicurezza, in particolare a coloro che sono responsabili della protezione di infrastrutture critiche.

Il **programma dei consulenti UE sulla protezione della sicurezza (EU PSA)**[21] ha una sezione dedicata alle attività anti-droni che offre: i) una specifica valutazione della vulnerabilità per impianti e infrastrutture ad alto rischio; ii) consulenza pratica sul modo di affrontare la minaccia dei droni; e iii) consulenza pratica sul modo di gestire l'uso di apparecchiature di individuazione di droni durante eventi ad alto rischio.
La Commissione considererà l'esigenza di creare un insieme condiviso di apparecchiature anti-droni a livello di Unione europea, disponibile per coadiuvare gli Stati membri in occasione di eventi su vasta scala.

Esercitazioni come quelle organizzate a livello di Unione europea con la rete dei servizi di contrasto contribuiscono alla preparazione operativa in diversi settori della sicurezza interna. Se del caso la Commissione collaborerà con le reti competenti per includere gli elementi anti-droni nelle future esercitazioni. Si contribuirà così ad ampliare ulteriormente le conoscenze e lo scambio di migliori pratiche, adottando soluzione diverse. Per assicurare una risposta efficace alle minacce poste dai droni è necessario realizzare comunicazioni sicure e affidabili tra le diverse autorità. Il contrasto delle minacce poste dai droni pertanto farà parte della programmazione delle esercitazioni future da svolgere nell'ambito del progetto di preparazione BroadEU.Net finanziato dall'UE, in modo da sperimentare le basi del futuro sistema dell'UE di comunicazioni critiche[22]. Inoltre potrebbero essere svolte esercitazioni congiunte con la partecipazione di esperti di cibersicurezza e sicurezza dei droni per studiare i rischi informatici posti dai droni nonché le soluzioni digitali per neutralizzare i droni.

Azioni fondamentali per gli orientamenti pratici e il sostegno operativo

- **Il JRC pubblicherà due manuali che faranno parte del pacchetto anti-droni.**
- **La Commissione, in cooperazione con le agenzie competenti, sosterrà l'estensione dell'attuale formazione anti-droni al settore della sicurezza privata.**
- **La Commissione integrerà le componenti anti-droni nella programmazione delle esercitazioni, in cooperazione con le reti dei servizi di contrasto.**

D. Ricerca e innovazione

L'UE sta continuando a finanziare il suo programma di ricerca in materia di sicurezza nel quadro di **Orizzonte Europa (2021-2027)**[23].. Tale programma rappresenta circa il 50 % dei finanziamenti pubblici complessivi investiti nel settore della sicurezza nell'Unione europea e negli Stati membri. Questo ricerca

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

[22] Il sistema di comunicazione critica dell'UE offrirà un'infrastruttura a banda larga sicura per garantire l'interoperabilità transfrontaliera dei sistemi di comunicazione utilizzati dalle autorità di contrasto e dagli operatori di primo intervento nell'area Schengen.

[23] In passato, fino alla fine del 2020, le attività di ricerca e innovazione in materia di sicurezza sono state finanziate nel quadro di Orizzonte 2020 e del settimo programma quadro.

in materia di sicurezza, che reca un contributo strategico a varie priorità dell'UE nel settore della sicurezza, ha già iniziato a trattare le minacce poste dai droni. Si pensi in particolare ad ALADDIN, che offre soluzioni per rilevare e neutralizzare droni in aree regolamentate[24] oppure a 7SHIELD, che ha studiato lo sviluppo di soluzioni anti-droni per i segmenti terrestri delle infrastrutture spaziali critiche. Il progetto ALFA ha avuto successo anche nello sviluppo di un sistema per rilevare e tracciare droni utilizzati per il contrabbando[25]. Queste iniziative di ricerca e innovazione possono essere portate avanti nel quadro di Orizzonte Europa, convalidate o integrate da azioni nell'ambito dell'ISF-Polizia.

In futuro la Commissione favorirà lo scambio più sistematico degli esiti dei progetti pertinenti con i portatori di interessi, anche tramite la Comunità per la ricerca e l'innovazione europea in materia di sicurezza[26]. In tal modo si rafforzerebbe ulteriormente lo scambio di dati specifici. Sarebbe inoltre possibile raccogliere in maniera più efficiente informazioni sulle esigenze degli utenti e comunicarle all'industria per orientare l'innovazione. Lo scambio sistematico degli esiti dei progetti consentirà inoltre un dialogo strutturato con gli Stati membri e i portatori di interessi per identificare soluzioni, strumenti e tecnologie promettenti che potrebbero essere adottati da un gruppo di autorità degli Stati membri. In tale contesto la Commissione valuterà insieme agli Stati membri[27] la possibilità di: i) creare un campo di ricerca autonomo in materia di soluzioni anti-droni nei futuri programmi di lavoro di Orizzonte Europa; e ii) sostenere specifici sistemi innovativi tramite appalti pre-commerciali[28]. Tutto questo è perfettamente in linea con l'approccio basato sulle capacità definito dettagliatamente nel documento di lavoro dei servizi della Commissione "Rafforzare la sicurezza attraverso la ricerca e l'innovazione"[29].

È dunque cruciale rafforzare le sinergie in termini di soluzioni anti-droni tra i settori europei della sicurezza civile, della difesa e dello spazio, con l'obiettivo di favorire le sinergie nelle tecnologie dei droni e nelle tecnologie anti-droni fra i tre settori[30]. In pratica, grazie al rafforzamento di tali sinergie, i progetti di difesa possono trarre vantaggio dagli sviluppi innovativi nel settore civile, mentre l'aeronautica civile può trarre vantaggio dagli sviluppi nel settore della difesa.

Il **Fondo europeo per la difesa (FED)** e i relativi programmi precursori incentivano e sostengono attività collaborative e transfrontaliere di ricerca e sviluppo nel settore della difesa. Integrando e amplificando gli sforzi degli Stati membri, il FED promuove la cooperazione tra le imprese e i ricercatori dell'UE, a prescindere dalle dimensioni e dallo Stato membro di provenienza. I programmi precursori del FED hanno già finanziato progetti anti-droni nell'ambito delle attività di ricerca e sviluppo nel settore della difesa.

---

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

[25] ALFA è anche alla base del progetto ISF Courageous e delle sue attività di prove.

[26] La Comunità per la ricerca e l'innovazione europea in materia di sicurezza (CERIS) riunisce i portatori di interessi nel settore della ricerca in materia di sicurezza: dai rappresentanti politici agli utenti finali, al mondo accademico e all'industria fino alla sicurezza civile: https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en

[27] Nella formazione del comitato di programma "Sicurezza civile per la società" di Orizzonte Europa.

[28] L'appalto pre-commerciale (PCP) è un approccio agli appalti pubblici di servizi di ricerca e sviluppo (R&S) delineato nella comunicazione sugli appalti pre-commerciali (C(2007) 799 final) del 14.12.2007. Si tratta di uno strumento importante per stimolare l'innovazione, giacché consente al settore pubblico di orientare lo sviluppo di nuove soluzioni in funzione delle proprie esigenze.

[29] Documento di lavoro dei servizi della Commissione "Rafforzare la sicurezza attraverso la ricerca e l'innovazione" (non disponibile in IT), (SWD (2021) 422 final) del 15.12.2021.

[30] SWD(2022) 362 del 10.11.2022. Come si illustra nella relazione sullo stato di avanzamento dell'attuazione del piano d'azione sulle sinergie tra i settori della difesa civile e dello spazio, nell'ambito dell'azione 9.

Il programma di lavoro del FED per il 2023 contiene un'azione per lo sviluppo di iniziative anti-droni[31], con un bilancio indicativo di 43 milioni di EUR. L'azione intende sviluppare moduli hardware e software per una soluzione mobile e a tutto campo volta a contrastare un'ampia gamma di droni, compresi gli sciami.

Il principale esito atteso dal sostegno del FED nel settore del contrasto ai droni, per il periodo 2021-2027, è lo sviluppo di un prototipo di una soluzione anti-droni che in futuro potrebbe tradursi in un appalto congiunto a livello di Unione europea. Per raccogliere le sfide tecnologiche nel settore dei sistemi anti-droni si ricorre al sistema di innovazione nel settore della difesa dell'UE (EUDIS). L'EUDIS inoltre comprende un filone per gli incubatori a duplice uso, allo scopo di migliorare la collaborazione tra il settore civile e quello della difesa, e di stimolare l'adattamento e la maturazione tecnologici.

Un altro pilastro fondamentale dell'innovazione, e in particolare per la ricerca applicata sul modo di contrastare le minacce poste dai droni, è l'attività del JRC. Nel quadro del suo progetto anti-droni, il JRC riesaminerà le tecnologie delle contromisure attive e passive, e il modo in cui si possono utilizzare tali tecnologie per garantire la sicurezza degli spazi pubblici e delle infrastrutture critiche.

A questo scopo, e come primo passo, il JRC istituirà un **laboratorio vivente** in cui studiare le tecnologie anti-droni e il modo in cui applicarle in contesti reali. L'allestimento del laboratorio comprenderà la programmazione, la preparazione e la realizzazione di una soluzione. Includerà altresì le attività di rilevamento, tracciamento, identificazione e neutralizzazione, nonché l'integrazione di processi e portatori di interessi. L'ambito di applicazione del laboratorio vivente comprenderà l'integrazione con sistemi di gestione del traffico con e senza equipaggio, in particolare lo U-space[32]. Nel laboratorio vivente si studierà inoltre il modo di integrare l'apprendimento automatico e l'intelligenza artificiale per migliorare le prestazioni complessive di una soluzione anti-droni.

Nel medio termine, il laboratorio vivente del JRC diventerà un **centro di eccellenza anti-droni.**

Azioni prioritarie per sfruttare al meglio ricerca e innovazione

- **La Commissione e gli Stati membri decideranno in merito alle future esigenze di nuove soluzioni anti-droni, da trattare nell'ambito dei pertinenti programmi europei di ricerca e innovazione, in particolare Orizzonte Europa.**
- **La Commissione e gli Stati membri identificheranno un elenco di soluzioni anti-droni promettenti e valuteranno la fattibilità in termini di appalti pre-commerciali di alcune di esse.**
- **La Commissione identificherà le idee, le tecnologie e le soluzioni da integrare nello sviluppo delle capacità di difesa e sosterrà i progetti che cercano di divulgare tali idee, tecnologie e soluzioni nei settori civili.**
- **Il JRC istituirà un centro di eccellenza anti-droni quale ulteriore evoluzione di un laboratorio vivente.**

[31] Decisione di esecuzione della Commissione C(2023) 2296, del 29.3.2023, relativa al finanziamento del Fondo europeo per la difesa istituito dal regolamento (UE) 2021/697 del Parlamento europeo e del Consiglio e all'adozione del programma di lavoro per il 2023 - Parte II (non disponibile in IT).

[32] Regolamento di esecuzione (UE) 2021/664 della Commissione relativo a un quadro normativo per lo U-space. Il termine "U-space" è stato adottato per descrivere la gestione del traffico aereo senza equipaggio allo scopo di garantire interazioni sicure con le altre entità che utilizzano lo stesso spazio nelle aree urbane e altrove.

E. Sostegno finanziario

La Commissione continuerà a fornire sostegno finanziario alle pertinenti attività anti-droni, essenzialmente attraverso l'ISF ma anche tramite lo strumento di sostegno finanziario per la gestione delle frontiere e la politica dei visti (BMVI) e il programma Orizzonte Europa (per le azioni legate alla ricerca e all'innovazione).

Lo strumento tematico dell'ISF sosterrà: i) le reti dei servizi di contrasto europee; ii) l'attività correlata del JRC; iii) il nuovo gruppo di esperti anti-droni; e iv) la creazione di una piattaforma per lo scambio di informazioni. La Commissione sta già finanziando alcuni progetti per verificare e convalidare sistemi volti a rilevare e localizzare i droni che attraversano illegalmente le frontiere esterne dell'UE. Tali progetti si basano sui risultati ottenuti da precedenti progetti di ricerca finanziati dall'UE[33].

Nel quadro dello strumento tematico dell'ISF la Commissione lancerà, nella prima metà del 2024, un **invito a presentare proposte** volto soprattutto a sostenere il ricorso a soluzioni anti-droni suscettibili di essere ampiamente adottate.

Si incoraggeranno gli Stati membri ad attuare la presente comunicazione e a tradurre i risultati della ricerca finanziata dall'UE in soluzioni anti-droni mediante i rispettivi programmi dell'ISF.

Azioni fondamentali per il sostegno finanziario

- **La Commissione lancerà un invito a presentare proposte di soluzioni anti-droni nel quadro dei programmi di lavoro relativi allo strumento tematico dell'ISF per il periodo 2026-2027.**
- **Si incoraggeranno gli Stati membri a sfruttare appieno i programmi dell'ISF per il periodo 2021-2027, al fine di individuare ed attuare efficienti soluzioni anti-droni.**

F. Analisi di misure normative

Benché l'UE abbia disciplinato l'uso legittimo dei droni, attualmente a livello di Unione europea non esistono regolamenti anti-droni specifici che stabiliscano un quadro comune armonizzato per le autorità, gli operatori e i fabbricanti degli Stati membri. Gli orientamenti non vincolanti dell'AESA che trattano gli incidenti che coinvolgono droni negli aeroporti (cui si è fatto riferimento in precedenza nella presente comunicazione) sono stati accolti favorevolmente dal settore, ma a causa del limitato ambito di

[33] Tra gli esempi ricordiamo i progetti finanziati nell'ambito di azioni specifiche BMVI in materia di: i) innovazione per quanto riguarda le coste e le frontiere terrestri e/o marittime; e ii) Frontex. Alcuni progetti finanziati nell'ambito di azioni specifiche in materia di innovazione per quanto riguarda le coste e le frontiere terrestri e/o marittime sono incentrate sulla verifica delle tecnologie innovative di sorveglianza. Vi è anche un'azione specifica per acquistare e mettere a disposizione delle autorità di frontiera europee le apparecchiature necessarie a rilevare e localizzare i droni che attraversano le frontiere, in relazione ad attività illegali o criminose. Quest'azione specifica consentirà agli Stati membri di acquistare due sistemi anti-droni. Quale valore aggiunto dell'UE, su richiesta presentata da Frontex nell'ambito dei negoziati annuali bilaterali, le apparecchiature tecniche acquistate nel quadro di azioni specifiche devono essere messe a disposizione di Frontex fino a quattro mesi all'anno, per essere utilizzate nel corso delle sue operazioni congiunte.

applicazione e della natura consultiva non sono sufficienti ad attenuare la minaccia posta dai droni non cooperativi. Poiché si fa sempre più pressante l'esigenza di prevenire in maniera efficace l'uso non autorizzato dei droni, la Commissione, in stretta collaborazione con esperti degli Stati membri, analizzerà ulteriormente la necessità di introdurre misure legislative o non legislative in futuro. A tale scopo la Commissione avvierà un apposito **studio di mappatura** per stabilire l'attuale panorama normativo. Lo studio di mappatura dovrebbe anche tenere conto degli sviluppi e del quadro dell'ICAO, senza dimenticare che le norme volte a contrastare le potenziali minacce poste dai droni non dovrebbero intralciare indebitamente le operazioni legittime, comprese le attività delle organizzazioni di piloti privati.

Gli aeroporti dell'UE beneficiano di dettagliate norme generali sulla sicurezza, estese anche alle minacce poste dai droni. Per accrescere la resilienza degli aeroporti e delle autorità aeronautiche di fronte ai rischi posti dai droni, secondo un approccio basato su elementi concreti, la Commissione, in cooperazione con gli Stati membri, **identificherà le ulteriori potenziali vulnerabilità in materia di protezione dai droni non cooperativi nel quadro di una valutazione dei rischi per la sicurezza che potrà richiedere modifiche normative**.

In tale contesto è necessario avviare un dialogo strutturato con il settore e i fabbricanti di droni in materia di misure di sicurezza fin dalla progettazione (ad esempio solidi sistemi contro la falsificazione di dati (spoofing), limitazioni della capacità, condivisione dei protocolli di comunicazione e aggiornamenti delle banche dati anti-droni).

Azioni fondamentali per l'analisi di misure normative

- **La Commissione avvierà uno studio di mappatura per identificare le esigenze normative e la possibilità di armonizzare leggi e procedure degli Stati membri.**
- **In linea con un approccio basato su elementi concreti la Commissione intraprenderà una valutazione dei rischi per la sicurezza dell'aviazione posti dai droni, allo scopo di identificare le ulteriori potenziali vulnerabilità degli aeroporti, che potrebbero richiedere modifiche normative.**
- **La Commissione si impegnerà in un dialogo strutturato con il settore sulla necessità e la natura di eventuali nuove misure specifiche concernenti la sicurezza dei droni.**

III. PROSSIME TAPPE

Per evitare che i rapidi sviluppi tecnologici e il numero crescente di droni producano un aumento incontrollato delle minacce poste dai droni non cooperativi è necessario intensificare la cooperazione a livello di Unione europea, sulla base della politica globale anti-droni dell'UE delineata nella presente comunicazione. A tale scopo le attuali attività a livello di Unione europea saranno portate avanti e integrate dall'insieme di azioni fondamentali, elencate nella presente comunicazione, che saranno attuate nei prossimi anni.

Le attività delineate nella presente comunicazione si estenderanno fino al 2030. Entro il 2027 sarà effettuata una valutazione intermedia tramite il gruppo di esperti, mentre una revisione completa del programma anti-droni dell'UE è prevista al più tardi per il 2030.