IAI DOCUMENTI
n. 26|10 (novembre 2026)

La protezione delle infrastrutture critiche dai droni: governance e tecnologia

Paola Tessari, Nicolò Murgia e Alessandro Marrone

La crescente diffusione dei droni aerei sta rendendo sempre più centrale la protezione delle infrastrutture critiche nel contesto della guerra ibrida, caratterizzata da azioni che si svolgono al di sotto della soglia del conflitto armato convenzionale. I recenti episodi che hanno interessato aeroporti, basi militari e altri siti sensibili europei evidenziano la necessità di rafforzare la capacità di prevenzione e risposta attraverso soluzioni efficaci e sostenibili anche dal punto di vista economico. In questo quadro, assumono particolare rilievo le tecnologie di contrasto basate sulle attività cibernetiche ed elettromagnetiche, che integrano le dimensioni cibernetica ed elettromagnetica e si affiancano ai sistemi di difesa tradizionali, ponendo al contempo nuove sfide legate ai possibili effetti collaterali in contesti civili. Parallelamente, l'evoluzione del quadro normativo europeo richiede un rafforzamento della *governance* della sicurezza delle infrastrutture critiche e una maggiore integrazione tra innovazione tecnologica, preparazione operativa e resilienza del sistema-Paese.
Studio preparato per il seminario a porte chiuse "La protezione delle infrastrutture critiche dai droni: *governance* e tecnologia" organizzato dallo IAI a Roma il 14 settembre 2026.

Introduzione p. 2
1. Minaccia, contesto nazionale e vulnerabilità 3
2. L'asimmetria economica e operativa della minaccia 6
3. Governance, responsabilità e quadro normativo 7
4. Vantaggi e opportunità nell'utilizzo delle Cema nel contrasto ai droni 11
5. Possibili criticità nell'utilizzo delle Cema 13
6. Le principali tecnologie Cema di neutralizzazione 15
Conclusioni e raccomandazioni 20
Acronimi 22

Paola Tessari e **Nicolò Murgia** sono ricercatori nel programma "Difesa, sicurezza e spazio" dell'Istituto Affari Internazionali (IAI). **Alessandro Marrone** è responsabile del programma "Difesa, sicurezza e spazio" dello IAI. Gli autori ringraziano Michele Nones, vicepresidente vicario dello IAI, per il suo contributo alla revisione del testo.
Questo studio è stato preparato per il seminario a porte chiuse "La protezione delle infrastrutture critiche dai droni: governance e tecnologia" organizzato dallo IAI a Roma il 14 settembre 2026 con il supporto di ELT Group, ed è stato rivisto alla luce del dibattito ivi svoltosi.

© 2026 IAI

Introduzione

Le minacce alla sicurezza nazionale ed europea sono sempre più caratterizzate da azioni ibride, ovvero azioni che mirano a destabilizzare l'avversario attraverso l'uso combinato di strumenti politici, economici, tecnologici e militari senza sfociare in un conflitto aperto. Fra i principali strumenti di questa strategia, si collocano i droni aerei (*unmanned aircraft systems*, Uas, o aeromobili a pilotaggio remoto, Apr), che possono essere utilizzati in operazioni di disturbo, spionaggio e sabotaggio contro le infrastrutture critiche (IC), ovvero quei sistemi che forniscono servizi essenziali alla popolazione. L'aumento post-2022 di sorvoli da parte di droni sospetti in Italia e in Europa[1], ha portato a una crescente attenzione nei loro confronti, mettendo alla prova il livello di preparazione dei Paesi UE e le loro capacità di rispondere e di adottare contromisure qualora si verificasse un'azione ostile da parte di questi sistemi. Nel caso specifico delle infrastrutture critiche, l'attenzione è particolarmente legata agli aspetti economici e all'impatto di una sospensione delle attività provocata dai sorvoli illeciti.

Questo documento analizza la minaccia rappresentata dai droni duali (cioè progettati per uso civile ma potenzialmente impiegabili per scopi militari) nel contesto della resilienza nazionale ed europea, esaminando i casi recenti, le sfide e le opportunità tecnologiche legate alle attività cibernetiche ed elettromagnetiche (*cyber electromagnetic activities*, Cema) e l'evoluzione della normativa e della *governance*, con particolare riferimento al contesto italiano. Il perimetro d'analisi fa riferimento all'utilizzo di droni per operazioni di disturbo, per l'acquisizione di informazioni tramite ricognizione e sorveglianza o per attacchi diretti contro infrastrutture, nella cornice della cosiddetta guerra ibrida. Questo si riflette sulla tipologia di droni, sulle relative logiche di impiego e sulle Cema con cui si può contrastare tale minaccia. Si tratta in questo caso di droni duali, acquistabili sul mercato civile a costi relativamente bassi, con un livello di sofisticatezza tecnologica non particolarmente alto che ne permette un impiego illecito tramite modifiche marginali, quindi fondamentalmente diversi da sistemi più avanzati di carattere militare. L'utilizzo, infatti, di sistemi propriamente militari, secondo tattiche militari, nel contesto di quella che a quel punto diventerebbe un'operazione militare a tutti gli effetti, giustificherebbe l'utilizzo di contromisure afferenti a quel contesto operativo. Tale distinzione è importante nel quadro di *governance* italiano ed europeo pur riconoscendo che la guerra ibrida contempla l'uso combinato di strumenti civili e militari, poiché gli episodi finora registrati non si configurano come un attacco militare, e proprio sotto la soglia del conflitto armato, sono maggiori le carenze e le difficoltà nel contrastare tale minaccia alle IC.

© 2026 IAI

1 Edwards, Charlie et al., "Russia's UAV Campaign over Europe", in *IISS Research Papers*, luglio 2026, https://www.iiss.org/research-paper/2026/06/russias-uav-campaign-over-europe.

La sezione successiva analizza la natura della minaccia e la specificità italiana, con una rete di infrastrutture critiche diffusa su tutto il territorio nazionale. La sezione 2 si concentra sull'asimmetria della minaccia, che con costi e competenze limitate costringe chi si difende a mobilitare risorse considerevoli. Nella sezione 3 si analizza la normativa in vigore: mentre il quadro per la prevenzione è chiaro a livello nazionale, le misure per il contrasto a un attacco in corso presentano aspetti critici. Le sezioni 4, 5 e 6 si concentrano sul ruolo delle Cema nel contrasto ai droni duali: i loro vantaggi, i rischi operativi e un'analisi dettagliata delle principali tecnologie attualmente in uso. La sezione conclusiva raccomanda investimenti continuativi in ricerca e sviluppo, un quadro più chiaro di responsabilità e regole di ingaggio, una protezione calibrata sulle infrastrutture più esposte, e la promozione di una maggiore cultura della sicurezza tra operatori e cittadini.

1. Minaccia, contesto nazionale e vulnerabilità

Originariamente i droni sono stati sviluppati e utilizzati in ambito militare: le loro capacità di sorveglianza e ricognizione, insieme alla possibilità di operare in zone ostili, li hanno resi strumenti molto efficaci per le azioni di difesa. Negli ultimi anni, però, abbiamo assistito a un'espansione significativa del loro utilizzo al di fuori del dominio militare, con un numero sempre crescente di aziende e individui che ha iniziato a impiegare questa tecnologia per scopi commerciali e/o ricreativi. Secondo quanto riportato dal Piano d'azione sulla sicurezza dei droni e antidrone del febbraio 2026, il segmento del mercato commerciale europeo dei droni aerei è destinato a raggiungere un valore di circa 14,5 miliardi di euro entro il 2030, potrebbe superare i 50 miliardi di euro entro il 2033[2].

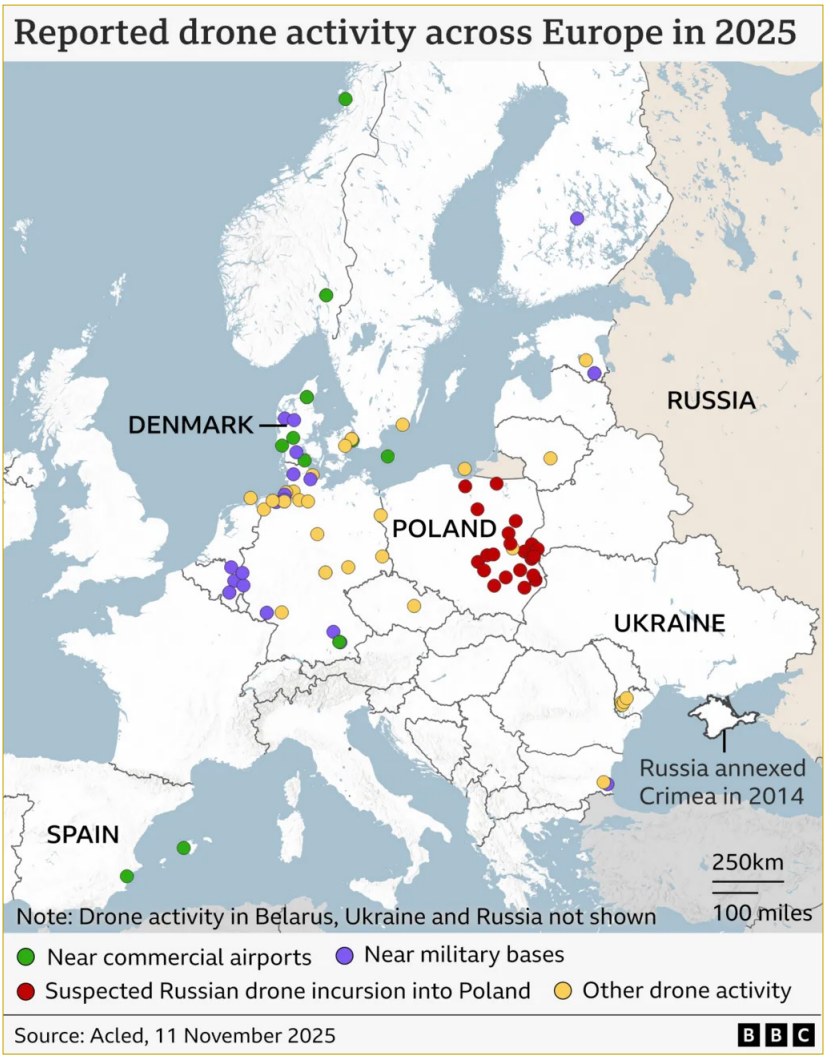
Il crescente utilizzo di droni per scopi commerciali e ricreativi, dovuto principalmente a ragioni di costo-efficacia, porta tuttavia a un aumento del rischio di utilizzi illeciti da parte di attori statali e non-statali. I droni duali vengono così inseriti tra i vettori di un'azione di minaccia ibrida, che, nel caso specifico delle infrastrutture critiche, le rende particolarmente vulnerabili in quanto esse sono ampiamente gestite, operate e/o di proprietà di attori privati e possono, di conseguenza, essere oggetto di interferenze o attacchi da parte di attori che hanno capacità e mezzi significativamente superiori rispetto ai singoli gestori privati dell'infrastruttura. Si ricordano ad esempio gli episodi che si sono verificati nel 2025 e hanno portato diversi aeroporti europei – tra cui importanti scali come Bruxelles, Monaco e Copenaghen[3] – a sospendere le

2 Commissione europea, *Piano d'azione sulla sicurezza dei droni e antidrone* (COM/2026/81), 11 febbraio 2026, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52026DC0081.

3 109 voli cancellati e 51 dirottati a Copenhagen; 17 voli cancellati per circa 3.000 passeggeri lasciati a terra a Monaco (Uyanik, Ayhan e Blasshofer Tilman, "Drone Sightings Disrupt Munich Airport, Halt Flights Impacting Thousands", in *Reuters*, 3 ottobre 2025, https://www.reuters.com/world/europe/drone-sightings-disrupt-munich-airport-halt-flights-impact-thousands-2025-10-03); 54 voli cancellati e circa 400 passeggeri a terra a Bruxelles (Cook, Lorne, "Drone Sightings Disrupt Brussels Airport,

© 2026 IAI

attività a causa di sorvoli di droni non identificati. Prima di questi, particolarmente significativa è stata la chiusura dell'aeroporto londinese di Gatwick nel 2018 a causa del sorvolo di droni. Lo scalo rimase inoperativo per diverse ore, lasciando a terra 110.000 passeggeri e causando la cancellazione di 760 voli[4]. Episodi simili hanno riguardato anche basi militari, centri di ricerca, siti industriali e impianti energetici: Interpol riporta oltre 60 avvistamenti di droni fra settembre e novembre 2025 in almeno 11 Paesi europei[5].



Fonte: Gardner, Frank, "Mysterious Drones Have Been Spotted at Night at Airports across Europe. How Worried Should We Be?", in *BBC News*, 17 novembre 2025, https://www.bbc.com/news/articles/crkl3d6pegpo.

Leaving Hundreds of Passengers Stranded", in *AP News*, 5 novembre 2025, https://apnews.com/article/9e2c6c6c3e4357e9736daccf1d873c1e.

4 Il dato si riferisce ai passeggeri in partenza e in arrivo a Gatwick, "Droni in pista a Gatwick, caos in aeroporto: cancellati tutti i voli. 'Atto deliberato'", in *Il Sole 24 Ore*, 20 dicembre 2018, https://www.ilsole24ore.com/art/droni-pista-gatwick-caos-aeroporto-chiuso-cancellati-tutti-voli-atto-deliberato-AEjLR52G.

5 Interpol, "Innovation: Defending against Drones in the Air and at Sea", in *Interpol Spotlight*, n. 4 (marzo 2026), https://www.interpol.int/en/Resources/INTERPOL-Spotlight/Spotlight-Issue-4-Innovation/Innovation-Defending-against-drones-in-the-air-and-at-sea.

© 2026 IAI

Pur non essendo certa la finalità di questi sorvoli, i droni duali possono rappresentare una minaccia per le loro caratteristiche che li rendono uno strumento particolarmente adatto allo svolgimento di attività criminali e terroristiche per diverse ragioni. In primo luogo, rispetto ad altri mezzi, i droni garantiscono un livello più elevato di anonimato per l'operatore, sia durante l'esecuzione dell'atto illecito sia nella fase di pianificazione dell'attacco, anche per le loro ridotte dimensioni. In secondo luogo, i droni si distinguono per l'elevata flessibilità operativa: possono decollare da aree differenti e spostarsi agilmente e con relativa rapidità, mantenendosi a bassa quota. Inoltre, questi mezzi sono in grado di eludere barriere fisiche e altre misure preventive adottate per la protezione di siti di interesse. A queste caratteristiche si aggiungono elementi che rendono il contrasto alle minacce veicolate dai droni particolarmente complesso a causa di almeno tre fattori: la carenza di contromisure specificamente progettate per l'impiego in ambienti urbanizzati; un quadro normativo ancora in via di definizione e non adeguato sulle misure di contrasto attuabili; l'attribuzione delle responsabilità al soggetto che attua un'azione di contrasto che potrebbe avere effetti indesiderati. Le conseguenze, sia della minaccia che delle contromisure, si estendono infatti ben oltre lo spazio aereo, incidendo sulla sicurezza delle infrastrutture critiche e degli spazi pubblici, comprese le aree ad alta densità abitativa, mettendo potenzialmente a rischio la cittadinanza.

Guardando con maggiore attenzione all'Italia, il verificarsi di sorvoli di droni sospetti ha aumentato l'attenzione e l'allerta verso questo tipo di rischi e le conseguenze sulla sicurezza che ne possono derivare. Ne è un esempio il sorvolo non autorizzato di quattro droni sugli impianti dell'ex Ilva di Taranto il 19 settembre 2025, e quello del drone di fabbricazione russa sul centro di ricerca dalla Commissione europea Joint Research Centre di Ispra (Varese) nel marzo dello stesso anno, non lontano anche da alcuni stabilimenti di aziende private del settore della difesa[6]. Il nostro Paese, inoltre, è caratterizzato da una diffusione capillare di infrastrutture critiche. Alcune di esse, come le reti ferroviarie e gli *hub* portuali, si estendono su tutto il territorio nazionale, tra catene montuose e lunghi tratti costieri che rendono più complessi il monitoraggio e la protezione. A ciò si aggiunge la crescente digitalizzazione di queste infrastrutture, i cui sistemi di controllo e comunicazione rappresentano un ulteriore punto di vulnerabilità. Data l'estensione della rete di infrastrutture e l'impegno in termini economici di un sistema di monitoraggio esteso, alcune zone risultano scarsamente controllate, creando un'ulteriore vulnerabilità. Inoltre, la sicurezza dell'infrastruttura riguarda non solo la singola organizzazione, ma tutta la catena di approvvigionamento che contribuisce al funzionamento corretto delle infrastrutture critiche. Alla luce di questo, è importante considerare che non tutte le infrastrutture

6 "Drone russo su Lago Maggiore, voli su centro ricerca Ue a Ispra. Indaga Procura di Milano", in *Sky TG24*, 30 marzo 2025, https://tg24.sky.it/cronaca/2025/03/30/drone-russo-lago-maggiore-centro-ricerca-ue-ispra.

© 2026 IAI

critiche presentano lo stesso livello di vulnerabilità e, soprattutto, che non tutte sono esposte allo stesso tipo di rischio. Si parla generalmente di "infrastrutture critiche", ma colpire un nodo ferroviario o un'autocisterna all'ingresso di un tunnel potrebbe avere effetti molto più devastanti rispetto ad altri scenari: risulta perciò importante l'individuazione delle infrastrutture maggiormente esposte, al fine di calibrare su queste le capacità di protezione.

2. L'asimmetria economica e operativa della minaccia

La principale caratteristica della minaccia rappresentata dai droni è quella dell'asimmetria, che si manifesta in una molteplicità di aspetti. Il primo è quello che attiene al costo. Mentre i droni acquistabili sul mercato civile hanno un costo che si limita a poche centinaia o migliaia di euro (e quelli militari meno sofisticati difficilmente superano i 50.000 euro), i sistemi per individuarli e neutralizzarli hanno costi di sviluppo, produzione e manutenzione esponenzialmente più alti, essendo composti da sistemi radar specializzati, sensori elettro-ottici, piattaforme Cema e architetture integrate di comando e controllo[7]. A titolo esemplificativo, un radar appositamente realizzato per la rilevazione dei droni costa circa un milione di euro, e può difficilmente essere impiegato per il contrasto di altre tipologie di minacce. Il drone, invece, è un sistema molto flessibile che, con modifiche al *payload*, può essere utilizzato per scopi diversi, come descritto in precedenza. Inoltre, i cicli di innovazione dei droni sono particolarmente brevi, data la possibilità di acquisire componenti a uso duale sul mercato civile, l'influenza di dinamiche commerciali globali e la facilità nel reperire informazioni circa nuovi sviluppi grazie a un ecosistema informativo diffuso e facilmente accessibile[8]. A questo si devono aggiungere gli avanzamenti che si stanno compiendo nel campo dell'intelligenza artificiale, con ricadute significative nell'impiego dei droni: è il caso dello *swarming*, che, proprio grazie a tecnologie che permettono una sempre maggiore automazione, rende possibile l'impiego di sciami di droni coordinati, complicando significativamente le operazioni di intercettazione e neutralizzazione. Lo sviluppo e l'impiego di sistemi di contrasto, invece, deve sottostare a tempistiche più lunghe, che riflettono la lunghezza dei processi di ricerca e sviluppo, certificazione e produzione[9]. Le lunghe tempistiche legate al processo di certificazione delle nuove tecnologie di contrasto, in particolare, si pongono in forte contrapposizione ai rapidi cicli evolutivi dei droni, con il rischio che le prime

7 Arranz, Adolfo et al., "Cheap Drones Are Reshaping the War in the Sky", in *Reuters*, 17 marzo 2026, https://www.reuters.com/graphics/IRAN-CRISIS/DRONES/dwpkyamxqpm/.

8 Williams, Holly e Erin Lyall, "Ukraine Uses Drone Innovation to Help Level Battlefield in War with Russia", in *CBS 60 Minutes*, 29 marzo 2026, https://www.cbsnews.com/news/ukraine-drone-innovation-helps-level-battlefield-war-with-russia-60-minutes-transcript.

9 Kiorri, Evi, "Drone Tech Evolves Every 3-6 Months, Leaving Europe Buying Outpaced Systems", in *Euronews*, 16 aprile 2026, https://www.euronews.com/my-europe/2026/04/16/drone-tech-evolves-every-3-6-months-leaving-europe-buying-outpaced-systems.

© 2026 IAI

raggiungano l'obsolescenza prima ancora di poter essere impiegate. Questo implica, quindi, la permanenza di un'asimmetria tra la rapidità dell'evoluzione dei droni e i processi consolidati dell'industria della difesa nello sviluppo delle contromisure.

Un ulteriore fattore di asimmetria concerne le competenze tecniche necessarie. Se infatti l'impiego di un drone, sia per missioni ostili che non, richiede oggi una competenza tecnica relativamente limitata e facilmente acquisibile, l'operatività dei sistemi di contrasto richiede personale altamente qualificato, dotato di una formazione specialistica volta a sviluppare capacità tecniche strutturate, come l'interpretazione in tempo reale di dati multisensoriali e ambientali[10]. Questa discrepanza genera un vantaggio strutturale per l'attore offensivo, che può adattarsi in minor tempo e a costi più bassi. Uno dei principali obiettivi nello sviluppo dei sistemi di contrasto dovrebbe essere quello di raggiungere una maggiore semplicità di utilizzo, in particolare nell'ottica di un impiego da parte di personale civile.

A rendere poi il drone un vettore particolarmente adatto all'impiego nell'ambito di tattiche asimmetriche, oltre alla già menzionata difficoltà nell'attribuzione della responsabilità dell'attacco, è la possibilità di avere origine, come minaccia, in prossimità dell'obiettivo. Droni di piccola taglia possono infatti decollare non lontano dall'infrastruttura critica che devono colpire, dal momento che non necessitano di sistemi di lancio e controllo sofisticati, accorciando ulteriormente le tempistiche a disposizione per intercettarli[11]. Se da un lato quindi vi è la necessità di difendere infrastrutture critiche diffuse su tutto il territorio nazionale, pur implementando criteri di prioritizzazione, dall'altro la minaccia può insorgere già all'interno del territorio nazionale (a differenza, ad esempio, di un missile proveniente da un paese ostile o un'incursione aerea), amplificando la vulnerabilità delle infrastrutture critiche.

3. Governance, responsabilità e quadro normativo

La minaccia dei droni aerei, anche per la suddetta asimmetria, rappresenta una sfida in termini di processo decisionale e di *governance*, e investe di nuove responsabilità non solo le autorità nazionali competenti, ma anche i soggetti privati che possiedono o gestiscono le infrastrutture critiche oggetto di possibili azioni illecite. Per rispondere a queste sfide sono state adottate a livello europeo e nazionale alcune importanti misure. Il 16 gennaio 2023 è entrata in vigore la Direttiva UE 2022/2557 relativa alla resilienza dei soggetti critici[12] (conosciuta anche come Direttiva Cer, *Critical entities resilience*), il cui obiettivo principale è rafforzare il coordinamento europeo

10 Intervista, 20 maggio 2026.
11 Ibid.
12 Parlamento europeo e Consiglio dell'UE, *Direttiva (UE) 2022/2557 del 14 dicembre 2022 relativa alla resilienza dei soggetti critici*, https://eur-lex.europa.eu/eli/dir/2022/2557/oj/ita.

© 2026 IAI

nell'identificazione e attuazione di misure di resilienza per i soggetti critici ed eliminare la frammentazione normativa nazionale che aveva caratterizzato il passato, promuovendo una strategia integrata e transfrontaliera. In Italia, la Direttiva Cer è stata recepita con il decreto legislativo n. 134 del 4 settembre 2024, che definisce una nuova architettura di *governance*[13]. Il decreto individua nel Presidente del Consiglio dei ministri la figura responsabile delle politiche di resilienza. In aggiunta, prevede l'istituzione del Punto di contatto unico (Pcu) presso la Presidenza del Consiglio, e identifica come Autorità settoriali competenti (Asc) ciascun ministero competente per le 11 categorie di soggetti critici. Il Pcu, in coordinamento con le Asc, è responsabile per la valutazione del rischio a livello nazionale e ha un ruolo di sostegno ai soggetti critici, per la condivisione di linee guida e metodologie di analisi, e supporto tramite attività di formazione ed esercitazioni. A queste si aggiungono il Comitato interministeriale per la resilienza (Cir) e la Conferenza per la resilienza dei soggetti critici (Crsc), ai quali possono partecipare rappresentanti e operatori dei soggetti critici. Le misure da attuare comprendono azioni necessarie a evitare il verificarsi dei rischi in modo preventivo, oltre a misure volte a contrastare e mitigare le conseguenze di eventuali incidenti e garantire la continuità operativa. A ciò si aggiungono interventi di realizzazione di protezioni fisiche (barriere, controllo degli accessi, impianti di rilevamento) e a favore della sicurezza del personale. Queste iniziative accrescono la consapevolezza dei soggetti critici in riferimento alle minacce ma impongono anche l'attuazione di nuove misure: per farvi fronte risulta quindi necessario integrare il *risk assessment* più tradizionale con un approccio che includa anche nuovi rischi e attori[14] in un panorama che ricomprende operatori critici di diverse dimensioni che hanno, di conseguenza, anche disponibilità e priorità diverse[15].

In riferimento alle iniziative riguardanti nello specifico gli Apr, la Commissione Europea ha adottato l'11 febbraio 2026 il Piano d'azione sulla sicurezza dei droni e antidrone[16]. Le misure delineate nel documento non si limitano alla gestione di problematiche relative alla sicurezza civile, ma si estendono anche alla sfera militare. Il Piano d'azione UE si propone infatti di sviluppare un approccio unitario, coordinato e globale, integrando le dimensioni civile e militare per contrastare operazioni dolose e proteggere la sicurezza interna. Riconoscendo che la responsabilità operativa rimane agli Stati membri, l'obiettivo principale del Piano è migliore la coerenza, l'interoperabilità e le capacità di risposta collettiva dell'UE. Fra i suoi scopi, mira inoltre alla promozione dell'innovazione tecnologica e dello sviluppo industriale, grazie anche a programmi di finanziamento europei dedicati che devono essere

13 Decreto legislativo n. 134 del 4 settembre 2024: *Attuazione della direttiva (UE) 2022/2557*, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2024-09-04;134.

14 Intervista, 14 maggio 2026.

15 Tessari, Paola e Karolina Muti, "Resilienza e sicurezza delle infrastrutture critiche nel contesto italiano ed europeo", in *Documenti IAI*, n. 24|11 (ottobre 2024), https://www.iai.it/it/node/19003.

16 Commissione europea, *Piano d'azione sulla sicurezza dei droni e antidrone*, cit.

© 2026 IAI

in coordinamento con gli investimenti nazionali. A tal fine, l'approccio suggerito coinvolge sinergicamente attori pubblici e privati con l'obiettivo di colmare le lacune tecnologiche e accrescere l'autonomia industriale europea nel settore. Infine, di fronte alla frammentazione dei quadri giuridici nazionali, il Piano d'azione riconosce la necessità di esplorare la possibilità di stabilire norme comuni vincolanti e non vincolanti per le autorità degli Stati membri e gli operatori privati, che chiariscano ruoli e i mandati di tutti gli attori coinvolti. In quest'ottica la Commissione avvierà uno studio di fattibilità sulle possibili opzioni per istituire un quadro normativo antidrone a livello UE entro il 2030. In aggiunta, per soddisfare le esigenze più immediate, la Commissione emanerà una raccomandazione sulle misure anti-drone, in cui saranno specificati gli orientamenti per gli operatori di pubblica sicurezza.

Con riferimento al quadro legislativo già in vigore afferente alla regolamentazione dell'uso dei droni, il principale riferimento normativo è il Regolamento di esecuzione (UE) 2019/947 della Commissione, del 24 maggio 2019, relativo alle norme e procedure per l'esercizio degli aeromobili senza equipaggio, come successivamente modificato. A livello nazionale, per gli aspetti rimasti di competenza degli Stati membri, si applica il Regolamento Uas-IT, edizione 1 del 4 gennaio 2021 dell'Ente nazionale per l'aviazione civile (Enac), che ha sostituito il precedente regolamento Enac "Mezzi aerei a pilotaggio remoto"[17]. Tramite questo regolamento l'Enac, in quanto autorità nazionale competente in materia di aviazione civile, esercita le proprie funzioni di regolazione, vigilanza e controllo nel quadro della normativa europea e nazionale. In particolare, la normativa prevede, salve le eccezioni applicabili, l'obbligo di registrazione degli operatori Uas sul portale D-Flight e di apposizione del relativo codice identificativo sui droni, nonché il rispetto di alcune restrizioni e condizioni. Un esempio è l'imposizione di zone interdette al volo per motivi di pubblica sicurezza, che rappresentano un iniziale contributo per la mitigazione delle minacce, stabilendo dei parametri relativi all'impiego lecito dei droni duali[18]. Si tratta comunque di misure di tipo preventivo: qualora si verificasse un sorvolo sospetto, la decisione di agire con contromisure è una responsabilità del gestore dell'infrastruttura interessata. Nei casi sopracitati di sorvoli illeciti sugli aeroporti, tale decisione si è concretizzata con la sospensione delle operazioni e la chiusura delle strutture. Secondo la normativa italiana, infatti, sono le autorità di pubblica di sicurezza le uniche titolate a intervenire con azioni specificamente volte a intercettare o neutralizzare un drone[19]. In alcuni casi è previsto che gli operatori di pubblica sicurezza possano avere il supporto delle Forze Armate nell'esercizio di tali funzioni. È questo il caso, ad esempio, di alcune

17 Enac, *Regolamento Mezzi aerei a pilotaggio remoto. Edizione 3*, 22 luglio 2020, https://www.enac.gov.it/?p=9449.

18 Sabatino, Ester e Francesco Pettinari (a cura di), "La minaccia dei droni duali e le sfide per l'Italia", in *Documenti IAI*, n. 20|04 (marzo 2020), https://www.iai.it/it/node/11410.

19 La Legge n. 121 del 1° Aprile 1981 stabilisce che in Italia la tutela della sicurezza pubblica è di competenza del Ministero dell'Interno, come autorità di pubblica sicurezza.

© 2026 IAI

operazioni nazionali come quelle che riguardano i grandi eventi, caratterizzati dalla presenza di un elevato numero di persone spesso in ambito urbano. Tali operazioni potrebbero fornire, in una prospettiva di lungo termine, un quadro di riferimento cui guardare per fare fronte alla minaccia in modo continuativo. La linea di demarcazione, sia tra pubblico e privato, sia tra civile e militare, diventa quindi sempre più sfumata, e questo mette sotto pressione le istituzioni competenti che sono chiamate a investire tempo e risorse in un adeguato coordinamento di un ventaglio di attori sempre più ampio e diversificato, fuori dall'approccio per "silos" settoriali e locali che impedisce di vedere gli effetti a cascata e l'impatto intersettoriale delle potenziali interruzioni del funzionamento di infrastrutture critiche.

Mentre si può affermare che le misure attuabili al fine di prevenire sorvoli illeciti siano chiaramente individuabili nella nostra normativa nazionale, diverso invece è il quadro delle procedure atte al loro contrasto, ovvero riguardanti le azioni che possono essere messe in atto per neutralizzare una minaccia nel momento in cui si verifica. Se da una parte, le uniche autorità autorizzate a intervenire sono i prefetti attraverso le forze dell'ordine o le Forze Armate, è molto difficile prevederne il dispiego su tutte le infrastrutture critiche del Paese, con il risultato di limitarne la capacità di una risposta reattiva e tempestiva[20]. In caso di abbattimento di un drone che si trovasse a sorvolare aree precluse da apposita decisione dell'amministrazione competente, bisognerebbe verificare la responsabilità per l'operatore che dovesse causare danni a terzi in ragione del fatto che conoscere in anticipo l'effettiva entità della minaccia è particolarmente complicato. Nel caso di zona interdetta al sorvolo, vi sarebbe però stata una violazione che avrebbe potuto essere ritenuta minacciosa per definizione[21].

La minaccia rappresentata dai droni è in crescita e per essere affrontata richiede strategie di difesa adatte a rispondere alle crescenti prestazioni e versatilità degli Apr, e che tengano conto di attori e misure trasversali e diversificate. Il verificarsi di un incremento di sorvoli sospetti nelle vicinanze di infrastrutture critiche diverse, con impatti e perdite economiche ingenti, mette di fronte alla necessità di agire per preservare l'incolumità pubblica e rende necessario riconoscere nei droni una sfida di "sicurezza ibrida". È importante, di conseguenza, guardare a strumenti trasversali sia dal punto di vista giuridico che operativo e tecnologico[22]. Con questa prospettiva, vengono di seguito presentate le misure Cema attuabili per il contrasto ai droni in una cornice di guerra ibrida. Come accennato nell'introduzione, si fa qui riferimento ai droni duali, solitamente acquistabili sul mercato civile, caratterizzati da costi relativamente

20 Sabatino, Ester e Francesco Pettinari (a cura di), "La minaccia dei droni duali e le sfide per l'Italia", cit.
21 Ibid.
22 Martorana, Marco, "La minaccia dei droni e lo 'scudo' europeo nei cieli: il nuovo Action Plan UE", in *Altalex*, 9 marzo 2026, https://www.altalex.com/documents/news/2026/03/09/minaccia-droni-scudo-europeo-cieli-action-plan-ue.

© 2026 IAI

contenuti e da un livello di sofisticatezza tecnologica tale da permetterne un impiego illecito con modifiche marginali.

4. Vantaggi e opportunità nell'utilizzo delle Cema nel contrasto ai droni

Nel contesto generale più ampio di un approccio nazionale volto per quanto possibile a una difesa stratificata, l'utilizzo di tecniche di neutralizzazione dei droni afferenti alle attività nello spettro elettromagnetico costituisce, attualmente, la contromisura preferibile nei confronti della minaccia posta da questi sistemi alle infrastrutture critiche[23] non in una situazione di conflitto militare aperto e nei termini trattati da questa analisi. A differenza dei sistemi "*hard kill*" che prevedono che il drone venga colpito da un effettore, le "*soft kill*", a cui le Cema appartengono, intervengono sul suo funzionamento, disabilitandolo o manipolandolo. Questo aspetto è di grande rilevanza quando si parla di infrastrutture critiche e, in generale, di ambienti urbani. Le *hard kill*, infatti, implicano la distruzione fisica del drone come risultato dell'impatto, con la conseguente produzione di frammenti che possono cadere in modo sparso e incontrollato causando danni la cui entità è difficile da prevedere, a meno che l'esplosione non sia tale da dissolvere il drone (ma questo presuppone la disponibilità di effettori particolarmente potenti). Le *soft kill*, invece, a seconda delle tecnologie impiegate e delle modalità di utilizzo, possono evitare questa conseguenza.

Questo aspetto è particolarmente significativo nel caso di un intervento in prossimità di infrastrutture critiche, dove una contromisura di tipo *hard kill* potrebbe causare, come effetto collaterale, danni potenzialmente uguali o maggiori di quelli che avrebbe provocato il drone portando a termine la sua missione. La criticità di questo aspetto è acuita dalla difficoltà di stabilire se un drone in sorvolo sopra o in prossimità di un'infrastruttura critica abbia come finalità un attacco diretto o altre azioni illecite (potrebbe ad esempio limitarsi alla raccolta di informazioni). Stabilire con certezza questo aspetto nei frangenti di un'incursione è estremamente complesso, anche in considerazione del fattore tempo, cruciale in queste situazioni[24]. Altrettanto difficile è verificare se l'incursione sia di carattere involontario, ossia un sorvolo effettuato da un operatore che ignora la normativa relativa allo spazio aereo interdetto al sorvolo, o che ha difficoltà a controllare il proprio drone, oppure se si tratti invece dell'azione volontaria di un attore malevolo. Oltre all'intento, poi, la verifica della presenza di un *payload* ostile costituisce un ulteriore fattore di criticità, non essendo possibile effettuare questa verifica se non quando il drone è sufficientemente vicino

23 González-Jorge, Higinio et al., *Counter Drone Technology: A Review*, Basel, Preprints, febbraio 2024, https://doi.org/10.20944/preprints202402.0551.v1.

24 Poppinga, Gerald et al., *Technical Developments in Counter-Drone Technology: C-UAS Detection, Tracking and Identification Technology. Annual Report*, Lussemburgo, Ufficio delle pubblicazioni dell'UE, 2025, https://doi.org/10.2760/1517220.

© 2026 IAI

all'infrastruttura, frangente nel quale potrebbe non essere più possibile intercettarlo in modo efficace[25]. La presenza poi di materiale chimico, biologico, radiologico, nucleare (Cbrn) sul drone è ancora più complessa da rilevare, e rende un possibile abbattimento in prossimità dell'infrastruttura estremamente problematico, con risultati che possono avvicinarsi a quelli previsti originariamente dall'attore malevolo che opera il drone. Il rischio è dunque quello di ricorrere a una contromisura che ha un'elevata probabilità di causare danni collaterali, quando è possibile che il drone non avrebbe, secondo le intenzioni del suo operatore, danneggiato l'infrastruttura[26].

Un aspetto fondamentale da considerare nell'impiego di misure di contrasto è l'effetto che potrebbero avere sulla continuità operativa che un'infrastruttura critica deve mantenere per garantire la fornitura di servizi essenziali. Oltre alla sicurezza, infatti, un aspetto che gli operatori devono salvaguardare quanto più possibile è il prosieguo delle attività e delle operazioni che vengono svolte nel sito. Il sistema impiegato per neutralizzare la minaccia posta da un drone deve dunque permettere di ridurre al minimo, se non evitare, l'interruzione dell'attività, il che rende insita la necessità di contenere i danni collaterali[27]. Analogamente, dato che alcune infrastrutture critiche, come gli aeroporti, sono collocate in prossimità di aree urbane, un ulteriore aspetto legato al contenimento dei danni collaterali è la sicurezza dell'ambiente circostante, che deve essere preservata quanto più possibile. Da questo punto di vista le Cema, rispetto alle alternative *hard kill*, sono coerenti con il principio di mitigazione del rischio, offrendo una soluzione di neutralizzazione scalabile, che può essere modulata a seconda dell'evoluzione della minaccia posta dal drone[28].

Diversamente dalle *hard kill* che, come chiarito sopra, portano inevitabilmente alla distruzione fisica del drone, alcune contromisure Cema rendono possibile deviarne la traiettoria e assumerne il controllo permettendo di effettuare un recupero del drone. Questo aspetto è particolarmente significativo per quanto concerne l'analisi forense degli incidenti, che si tratti di incursioni per raccogliere informazioni o di attacchi diretti ai danni di infrastrutture critiche tramite l'impiego di droni. In questi casi è necessario ricostruire chi siano gli attori coinvolti in queste operazioni[29] e il recupero del drone aiuterebbe in tal senso. Nel contesto della guerra ibrida, infatti, la difficoltà nell'attribuire la responsabilità di azioni di questo genere è uno dei fattori che

25 Sabatino, Ester e Francesco Pettinari (a cura di), "La minaccia dei droni duali e le sfide per l'Italia", cit.
26 Intervista, 11 maggio 2026.
27 Giacchero, Andrea et al., "From Business Continuity to Design of Critical Infrastructures: Ensuring the Proper Resilience Level to Datacentres", in *International Journal of Engineering & Technology*, vol. 5, n. 4 (2013), p. 3544-3553, https://hdl.handle.net/2108/100984.
28 Intervista, 11 maggio 2026.
29 Adel, Amr e Tony Jan, "Watch the Skies: A Study on Drone Attack Vectors, Forensic Approaches, and Persisting Security Challenges", in *Future Internet*, vol. 16, n. 7 (luglio 2024), art. 250, https://www.mdpi.com/1999-5903/16/7/250.

© 2026 IAI

contribuiscono ad abbassare il rischio per gli attori malevoli che le intraprendono, e a massimizzare gli effetti di destabilizzazione per le società che ne sono l'obiettivo[30]. Il recupero dei sistemi utilizzati permette inoltre di analizzare e meglio comprendere l'evoluzione di questa minaccia sotto il profilo tecnologico.

Nonostante il rischio che anche l'utilizzo di alcune tecnologie Cema possa causare dei danni collaterali, come nel caso del drone il cui collegamento con il pilota viene interrotto causandone una caduta incontrollata, un aspetto fondamentale che distingue le *hard kill* dalle *soft kill* è il livello di accettazione sociale. Nel caso di un'infrastruttura critica che si trovi in un contesto urbano, o in sua prossimità, l'impiego di sistemi militari che la popolazione associa a un contesto bellico, ad esempio un sistema di difesa aerea o l'utilizzo di munizioni da parte del personale militare, è meno accettabile e contribuisce a incrementare significativamente la percezione della minaccia, per via del contesto a cui queste contromisure rimandano[31]. Proprio in considerazione degli obiettivi di destabilizzazione sociale e politica che definiscono l'impiego di tattiche di guerra ibrida, la neutralizzazione della minaccia, in questo caso rappresentata dal drone, non può essere concepita come disgiunta dall'impatto psicologico che sia l'attacco, sia le modalità di risposta ad esso avranno sulla popolazione civile.

A quest'ultimo aspetto, ossia all'accettabilità sociale dei sistemi di contrasto in ambito urbano, si lega indissolubilmente quello della comunicazione strategica, fondamentale per rendere la popolazione civile consapevole della minaccia rappresentata dai droni e dunque meno avversa alla presenza di sistemi di contrasto in prossimità di obiettivi strategici, come può essere ad esempio una stazione ferroviaria pienamente integrata nel tessuto urbano.

5. Possibili criticità nell'utilizzo delle Cema

Oltre ai vantaggi sul piano operativo, però, le Cema presentano anche degli aspetti che possono limitarne l'efficacia. Fra questi, il primo aspetto riguarda il fatto che un drone può sfuggire con maggiore difficoltà alla neutralizzazione operata con sistemi *hard kill* quando questa viene svolta in modo corretto; diversamente le Cema, per la loro efficacia, dipendono da aspetti di vulnerabilità dei sistemi, che l'evoluzione tecnologica può ridurre in modo significativo[32]. La navigazione autonoma, le comunicazioni più robuste, i fattori di ridondanza legati alla sensoristica e, in generale, sviluppi che aumentano la resilienza del drone a fronte delle contromisure disponibili, hanno un

30 Ministero della Difesa, *Il contrasto alla guerra ibrida: una strategia attiva. Non-paper*, novembre 2025, https://www.difesa.it/assets/allegati/83696/non-paper_il_contrasto_alla_guerra_ibrida.pdf.
31 Intervista, 4 maggio 2026.
32 Drone Warfare, *Counter-UAS Electronic Warfare: Jamming, Spoofing, and Non-Kinetic Drone Defeat*, aggiornato al 20 agosto 2026, https://drone-warfare.com/?p=4003.

© 2026 IAI

impatto determinante sull'efficacia delle Cema[33]. Questo richiede dunque, come visto nel contesto della guerra in Ucraina, un costante adattamento delle difese ai cicli tecnologici evolutivi, che nel caso dei droni sono particolarmente rapidi[34]. Ciò implica anche che a una maggior sofisticatezza del drone, raggiunta alla conclusione di un nuovo ciclo evolutivo, corrisponde una minore efficacia delle Cema, fino al momento in cui queste non verranno adeguate ai nuovi sviluppi della minaccia che devono contrastare[35].

Un altro aspetto relativo a un limite dell'efficacia nell'impiego di attività Cema è quello dei danni collaterali nello spettro elettromagnetico. L'utilizzo di queste tecnologie, infatti, ha inevitabilmente una ricaduta anche sugli altri sistemi che in occasione della neutralizzazione della minaccia stanno operando in quello stesso spazio[36]. Questo è particolarmente evidente nel caso degli aeroporti, dove c'è l'elevato rischio che azioni di *jamming* o *spoofing* contro un drone non cooperativo possano impedire il corretto funzionamento dei sistemi di navigazione degli aerei in volo in prossimità dell'aeroporto, in momenti particolarmente delicati come decollo e atterraggio[37]. Considerando poi quanto siano stringenti gli standard di sicurezza nel settore dell'aviazione civile, è evidente come l'impiego di contromisure che possono causare danni collaterali significativi, o anche solo mettere a rischio l'incolumità dei passeggeri, richieda una significativa attenzione.

Anche in ragione delle limitazioni qui analizzate l'approccio ottimale al contrasto della minaccia dei droni è, laddove possibile, una difesa stratificata, che integri, a livello di effettori, sia *soft kill* che *hard kill*. Questo approccio permette infatti di integrare gli aspetti meno efficaci di una tipologia con i benefici derivanti dall'impiego dell'altra, aumentando le probabilità di successo nell'ingaggio della minaccia.

33 Vakulov, Alex, "Embedded AI in Military Drones Is Redefining Autonomy and Operations", in *IDGA Insight*, 10 febbraio 2026, https://www.idga.org/government-defense-it-communications/articles/embedded-ai-in-military-drones-is-redefining-autonomy-and-operations.

34 Stepanenko, Kateryna, "The Battlefield AI Revolution Is Not Here Yet: The Status of Current Russian and Ukrainian AI Drone Efforts", in *ISW Special Reports*, 2 giugno 2025, https://understandingwar.org/research/russia-ukraine/the-battlefield-ai-revolution-is-not-here-yet-the-status-of-current-russian-and-ukrainian-ai-drone-efforts.

35 Kallenborn, Zachary e Marcel Plichta, "Drone, Counterdrone, Counter-Counterdrone: Winning the Unmanned Platform Innovation Cycle", in *Modern War Institute Commentary & Analysis*, 23 settembre 2024, https://mwi.westpoint.edu/?p=23126.

36 Stewart, Briar, "Airlines Grapple with Spike in GPS Interference. Experts Say It's Collateral Damage from Global Conflicts", in *CBC News*, 25 maggio 2024, https://www.cbc.ca/news/world/gps-interference-airlines-1.7213538.

37 Plucinska, Joanna et al., "How Europe Might Tackle the Threat of Drone Incursions at Airports", in *Reuters*, 10 ottobre 2025, https://www.reuters.com/world/drone-incursions-what-can-airports-do-prevent-them-2025-10-10.

© 2026 IAI

6. Le principali tecnologie Cema di neutralizzazione

6.1 L'architettura di rilevamento e identificazione

Il primo elemento da considerare nell'analisi del contrasto alla minaccia dei droni è evidentemente quello riguardante il rilevamento della minaccia. Questo avviene attraverso un sistema di sensoristica che deve comprendere più tipologie di sensori, in particolare radar, ottici e acustici, i cui dati devono poi essere fusi tramite un sistema di comando e controllo. Il sensore maggiormente utilizzato è il radar, per via della sua capacità di tracciare l'obiettivo fornendo una stima della distanza, ossia del tempo che lo separa dal sistema di rilevamento. Il radar, tuttavia, rispetto ai droni di piccole dimensioni, che sono i più diffusi fra quelli commerciali, presenta alcune difficoltà. La prima è legata proprio alle dimensioni ridotte del drone, che lo rendono più difficile da individuare; vi è poi il fatto che questa tipologia di droni è realizzata sempre più in materiali compositi e in plastica, il che comporta un minore livello di riflettività; infine, il volo a bassa velocità e a bassa quota che contraddistingue questi sistemi aumenta significativamente la complessità nel distinguere il drone da elementi naturali e artificiali dell'ambiente in cui si muove, quali ad esempio dei volatili[38]. Tutti questi aspetti hanno reso necessario lo sviluppo di radar concepiti appositamente per il rilevamento dei droni, date le difficoltà di adattare quelli precedentemente sviluppati per individuare vettori molto diversi, come aerei e missili.

Al radar è poi necessario affiancare sensori ottici (elettro-ottici o infrarossi), che coprono una distanza minore, e sensori acustici, efficaci a distanze ancora più ravvicinate. I sensori ottici, oltre a fornire un riscontro visivo del drone tramite il rilevamento della firma ottica, possono contribuire a identificare il modello del drone, un aspetto molto rilevante nella selezione delle contromisure da impiegare. Perché questo sia possibile, è necessario disporre di ampie librerie di immagini da fornire al sistema di rilevamento, che andrà addestrato utilizzando questi dati con sistemi di *machine learning*[39]. Tuttavia, la semplicità con cui i droni possono essere modificati, alterando caratteristiche come la forma, rende complessa questa operazione.

I sensori acustici, poi, rilevano il rumore prodotto dal drone e lo confrontano con una banca dati nella quale sono stati precedentemente inseriti campioni sonori per permetterne l'identificazione. Anche in questo caso sono presenti, tuttavia, diverse

38 Desmarais, Anna, "The Baltic States Need More Drone-Detection Radars. Europe's Defence Bottlenecks May Slow Them Down", in *Euronews*, 6 giugno 2026, https://www.euronews.com/next/2026/06/06/the-baltic-states-need-more-drone-detection-radars-europes-defence-bottlenecks-may-slow-th.

39 Semenyuk, Vladislav et al., "Advances in UAV Detection: Integrating Multi-Sensor Systems and AI for Enhanced Accuracy and Efficiency", in *International Journal of Critical Infrastructure Protection*, vol. 49 (giugno 2025), art. 100744, https://doi.org/10.1016/j.ijcip.2025.100744.

© 2026 IAI

limitazioni legate alla possibile incompletezza della banca dati e all'inquinamento sonoro, che costituisce una variabile molto rilevante in un contesto urbano[40].

I limiti delle tecnologie di rilevamento fin qui presentate rendono necessario integrare i dati provenienti da radar e sensori in un sistema di comando e controllo, al fine di creare un adeguato livello di *situational awareness*[41]. Particolarmente significativo è l'impiego di tecnologie, come l'intelligenza artificiale, per aumentare l'automazione del processo di rilevamento, identificazione e tracciamento della minaccia.

Inoltre, nella prospettiva di un impiego di sistemi di contrasto a difesa di infrastrutture critiche, è importante riflettere sul loro utilizzo da parte degli operatori di tali infrastrutture. I sistemi militari non possono essere impiegati da operatori privati, e dunque la definizione della responsabilità nella protezione delle infrastrutture è determinante per chiarire che tipologia di sistemi debbano essere destinati a questa funzione.

Come analizzato precedentemente, la normativa italiana attualmente non definisce in modo sufficientemente chiaro chi e come si debba assumere la responsabilità della difesa delle infrastrutture critiche da minacce come quella dei droni, se non con il generale ma generico rinvio alle competenze in capo ai Prefetti. Un primo passo verso una maggiore chiarezza in questo senso non può prescindere dalla comprensione dello stato dell'arte delle tecnologie Cema da impiegare in questa funzione, evidenziandone le implicazioni, e più nello specifico i punti di forza e le vulnerabilità.

6.2 Jamming delle radiofrequenze

Il jamming delle radiofrequenze si basa sulla produzione di "rumore elettromagnetico" che disturba o interrompe la trasmissione di dati tra il drone e l'operatore, intervenendo sulle radiofrequenze utilizzate per controllo e telemetria tramite la generazione di un segnale di interferenza. Una volta interrotto il collegamento con l'operatore, nei droni commerciali si attivano delle modalità pre-programmate che portano il drone a eseguire autonomamente una o più azioni tra cui l'atterraggio automatico, il ritorno al punto di decollo oppure il cosiddetto *hovering*, ossia il volo stazionario[42]. Vi è tuttavia anche la possibilità che la funzione pre-programmata implichi il raggiungimento delle coordinate del bersaglio, neutralizzando l'effetto di questa contromisura.

40 Drone Warfare, *Counter-UAS 101 – Acoustic Drone Detection*, gennaio 2026, https://drone-warfare.com/?p=3639.
41 Lagaras, Stylianos et al., *A Counter-Drone Visualisation Platform Incorporating Sensor-Data Fusion*, Lussemburgo, Ufficio delle pubblicazioni dell'UE, 2024, https://dx.doi.org/10.2760/560445.
42 Drone Warfare, *Counter-UAS Electronic Warfare*, cit.

© 2026 IAI

Il jamming delle radiofrequenze può essere applicato anche ad altri segnali, oltre a quelli di controllo, come ad esempio quelli del feed video, fondamentali per l'operatore nel caso di droni *First Person View* (Fpv), affinché l'operatore possa visionare correttamente le immagini trasmesse dal drone, necessarie per definirne la posizione. Questa tecnologia è molto efficace contro droni commerciali standard che utilizzano il link radio per il controllo. Tuttavia, il jamming ha un'efficacia ridotta nei confronti di sistemi più sofisticati: è il caso, ad esempio, di droni con autonomia avanzata, che utilizzano link multipli attraverso reti cellulari e/o satellitari, come 5G e Lte in aggiunta a quello radio, o droni con un'elevata resistenza alle interferenze grazie a tecnologie come il *frequency hopping*, ossia il rapido spostamento del segnale tra più frequenze, o link cifrati[43]. Infine, l'efficacia si dimostra nulla nel caso di droni controllati tramite cavo in fibra ottica o con sistemi di guida terminale che sfruttano l'intelligenza artificiale[44].

Il jamming delle radiofrequenze ha il vantaggio di poter essere impiegato rapidamente e in modo scalabile, tuttavia, non essendo selettiva, comporta il rischio di interferire con comunicazioni civili ed eventualmente con le stesse infrastrutture critiche da difendere[45]. L'impiego di sistemi di direzionamento dell'onda magnetica rappresenta una soluzione solo parziale e non risolve le criticità che rendono difficile l'impiego di questi sistemi in strutture come gli aeroporti. Vi è poi il rischio che, a seguito dell'interruzione del link, il drone cada in modo non controllato, danneggiando potenzialmente le infrastrutture critiche.

6.3 Jamming del sistema di navigazione satellitare

Un'altra tipologia di jamming è quella che impedisce la ricezione del segnale satellitare necessario al drone per determinare la propria posizione e orientare la navigazione. Non potendo geolocalizzarsi, il drone devia dalla rotta e può riscontrare problemi di stabilità. È inoltre possibile che l'attivazione delle modalità programmate come il ritorno al punto di decollo non funzioni correttamente, proprio in ragione dell'inabilitazione subita. Questa tecnologia è molto efficace in particolare per droni senza pilotaggio remoto e con una rotta preimpostata che utilizzano il sistema satellitare globale di navigazione (*Global Navigation Satellite System*, Gnss), anche in considerazione del fatto che i segnali satellitari sono caratterizzati da bassa potenza, e sono dunque i più vulnerabili ad attività di intercettazione[46]. Emerge quindi una

43 Zidane, Younes et al., "Jamming and Spoofing Techniques for Drone Neutralization: An Experimental Study", in *Drones*, vol. 8, n. 12 (dicembre 2024), art. 743, https://doi.org/10.3390/drones8120743.
44 "How Ukrainian FPV Drones with Automated Terminal Guidance Work", in *Defense Express*, 30 maggio 2025, https://en.defence-ua.com/weapon_and_tech/how_ukrainian_fpv_drones_with_automated_terminal_guidance_work-14687.html.
45 Castrillo, Vittorio Ugo et al., "A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones", in *Drones*, vol. 6, n. 3 (marzo 2022), art. 65, https://doi.org/10.3390/drones6030065.
46 Ibid.

© 2026 IAI

complementarità rispetto al jamming delle radiofrequenze, che è invece efficace solo verso droni pilotati da remoto.

Tuttavia l'efficacia si riduce notevolmente nel caso gli Apr utilizzino sistemi di navigazione inerziale integrando capacità di navigazione "*dead reckoning*", o nei sistemi che operano una fusione dei sensori – camera, *Light Detection and Ranging* (LiDAR), ecc. – combinando quindi i dati provenienti da diverse fonti[47]. Oltre alla crescente resilienza dei sistemi Gnss, a rendere potenzialmente meno efficace il jamming del segnale satellitare è il rischio di disturbare operazioni che dipendono dall'attività nello spazio elettromagnetico come i trasporti, l'aviazione e i servizi di emergenza, con il rischio di aggravare ulteriormente l'interruzione della continuità operativa causata dal sorvolo di uno o più droni sopra o in prossimità di un'infrastruttura critica[48]. Inoltre, anche in questo caso la perdita di controllo del drone potrebbe portarlo a precipitare, con potenziali danni fisici all'infrastruttura critica.

6.4 Spoofing del sistema di navigazione satellitare

Lo spoofing è una contromisura che si basa sulla generazione di un falso segnale, che deve essere sufficientemente plausibile da essere accettato come quello vero dal ricevitore del drone. La tecnica di spoofing maggiormente utilizzata interviene sul segnale satellitare, portando il drone a localizzarsi in una posizione che non è quella corretta. Gli effetti sono la deviazione della rotta, l'atterraggio forzato e anche la possibilità di catturare il drone, guidandolo lungo una traiettoria prescelta[49]. Come nel caso del jamming, questa tecnologia è molto efficace contro sistemi che si basano sul Gnss per la navigazione, ma rispetto allo jamming questa misura presenta un'ulteriore significativa complessità, ovvero duplicare il segnale per "ingannare" il drone. Questo richiede una conoscenza dettagliata dei protocolli di comunicazione utilizzati dai droni sui quali si deve intervenire. Sistemi anti-spoofing, navigazione multi-sensore e algoritmi di coerenza tra sensori possono limitare significativamente l'efficacia di questa tecnologia[50].

Tuttavia, il vantaggio rispetto alle tecniche precedentemente analizzate deriva dalla possibilità di attuare una neutralizzazione controllata della minaccia, riducendo i danni collaterali. Rendendo possibile, inoltre, il recupero del drone per effettuare le

47 UAV Navigation, "Dead Reckoning Navigation for UAS", in *UAV Navigation Blog*, 4 luglio 2023, https://www.uavnavigation.com/node/252.
48 Intervista, 4 maggio 2026.
49 Tariq, Usman et al., "Systematic Review of Machine and Deep Learning Models for Unmanned Aerial Vehicles Cyber Threat Defense", in *Discover Artificial Intelligence*, vol. 6, n. 1 (dicembre 2026), art. 216, https://doi.org/10.1007/s44163-026-00960-7.
50 Gupta, Abhishek e Xavier Fernando, "Simultaneous Localization and Mapping (SLAM) and Data Fusion in Unmanned Aerial Vehicles: Recent Advances and Challenges", in *Drones*, vol. 6, n. 4 (marzo 2022), art. 85, https://doi.org/10.3390/drones6040085.

© 2026 IAI

analisi forensi necessarie ad attribuire la responsabilità dell'operazione, si rinforza un aspetto fondamentale per la deterrenza rispetto a questo tipo di minacce quale appunto l'attribuzione. Allo stesso tempo, lo spoofing richiede competenze tecniche molto elevate, oltre a un adeguato livello di intelligence sull'obiettivo, essendo necessaria una conoscenza completa delle caratteristiche tecniche del drone contro il quale è necessario intervenire[51]. Nonostante lo spoofing sia più preciso del jamming, permettendo di colpire il funzionamento del drone in modo più selettivo, rischia comunque di interferire con i sistemi di navigazione di altri apparecchi in prossimità.

6.5 Attacchi cyber (protocol-based exploitation)

Queste tecniche non si basano sulla generazione di un falso segnale come nello spoofing, o sulla sua interruzione come nel jamming, bensì sfruttano le vulnerabilità del sistema per assumere il controllo del drone. Possono avere come obiettivo la rete di comunicazione utilizzata dal drone o il suo stesso software[52]. Come nel caso dello spoofing, è necessaria una conoscenza specifica dei protocolli utilizzati dal drone, per individuare e sfruttare delle vulnerabilità nello *stack* di comunicazione[53]. Questo permette di interrompere la connessione tra il drone e l'operatore, sfruttare la finestra di disconnessione per attivare una procedura di sicurezza e assumerne così il controllo[54].

Questa tipologia di contromisure risulta per certi aspetti ottimale nella protezione delle infrastrutture critiche, data la possibilità di dirottare il drone lontano dall'area dove si trova l'infrastruttura, farlo atterrare in sicurezza e disporne per le analisi forensi, massimizzando quindi le opportunità di raccogliere informazioni circa la sua origine nonché rispetto alle tecnologie che impiega. Presenta tuttavia delle limitazioni dovute, da un lato, alla necessità di conoscere i protocolli del drone e, dall'altro, dall'essere condizionate dalla presenza di vulnerabilità che, se individuate per tempo dall'operatore, possono essere risolte facendo svanire l'opportunità di impiegare questa tecnica di neutralizzazione. È dunque necessario un elevato livello di preparazione, che tuttavia non rappresenta una soluzione agli ostacoli posti da minacce sconosciute, rispetto alle quali un attacco cyber sarebbe difficilmente impiegabile. A un elevato livello di precisione, a differenza, ad esempio, del jamming,

51 UK Department for Transport, *Countering Drone Threats to Shipping*, 20 maggio 2024, https://www.gov.uk/government/publications/countering-drone-threats-to-shipping/countering-drone-threats-to-shipping.

52 Wang, Zhaoxuan et al., "A Survey on Cybersecurity Attacks and Defenses for Unmanned Aerial Systems", in *Journal of Systems Architecture*, vol. 138 (2023), art. 102870, https://doi.org/10.1016/j.sysarc.2023.102870.

53 Uno stack di comunicazione (o stack di protocolli) è un insieme di livelli software che operano congiuntamente per consentire il trasferimento dei dati tra dispositivi.

54 Castrillo, Vittorio Ugo et al., "A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones", cit.

© 2026 IAI

si accompagnano quindi maggiori difficoltà di utilizzo.

Conclusioni e raccomandazioni

La crescente disponibilità di questi prodotti sul mercato, unitamente a un costante incremento delle loro performance, al prezzo contenuto nonché a frequenti episodi di sorvoli non autorizzati, amplia inevitabilmente anche l'esposizione al rischio. Nel caso specifico delle infrastrutture critiche, esse possono essere oggetto di azioni di spionaggio, sabotaggio e interferenze come parte di una strategia di guerra ibrida che mira a colpire servizi essenziali della società i cui fornitori spesso sono attori privati che hanno capacità e mezzi significativamente inferiori rispetto ai responsabili di tali azioni.

Il contrasto alla minaccia dei droni duali richiede una preparazione e una risposta efficaci per i quali è necessaria un'azione sinergica e coordinata tra molteplici attori: decisori politici, Forze Armate e di sicurezza e industria della difesa. Al fine di incoraggiare e favorire tale azione, si introducono di seguito alcune raccomandazioni.

- *Ricerca e sviluppo continuativi*. La capacità di garantire una risposta efficace e rapida a un possibile incidente non può prescindere da un adeguato livello di ricerca, sviluppo e innovazione. Sul piano tecnologico e industriale, è pertanto fondamentale assicurare investimenti continuativi in R&S, così da sostenere lo sviluppo di soluzioni innovative e mantenere la capacità di anticipare l'evoluzione delle minacce e di individuare per tempo le misure di contrasto più efficaci. Tale esigenza assume particolare rilevanza alla luce del rapido e costante progresso tecnologico dei droni duali, che richiede un adeguamento altrettanto dinamico delle capacità di prevenzione, rilevamento e contrasto.
- *Responsabilità e regole di ingaggio più chiare*. Il contrasto alla minaccia dei droni richiede un approccio che includa nuovi rischi, attori e scenari. Stante la difficoltà di comprendere con anticipo se eventuali sorvoli siano attacchi volontari o meno, dovrebbero essere definite con maggiore chiarezza le responsabilità dei diversi soggetti coinvolti e le modalità di coordinamento delle loro attività decisionali e operative. Particolare attenzione andrebbe rivolta alla definizione della responsabilità e alla tutela dell'operatore che attua un'azione di contrasto, soprattutto in contesti particolarmente urbanizzati e frequentati, dove potrebbero verificarsi danni collaterali, tramite regole di ingaggio chiare e un quadro giuridico di riferimento che rispecchi la natura ibrida della minaccia e sia al passo con lo stato dell'arte delle tecnologie finalizzate al suo contrasto.
- *Un approccio trasversale alla sicurezza ibrida*. Il verificarsi di sorvoli sospetti nelle vicinanze di infrastrutture critiche diverse, con impatti e perdite economiche ingenti, mette di fronte alla necessità di agire per preservare l'incolumità pubblica e rende

© 2026 IAI

necessario riconoscere nei droni una sfida di "sicurezza ibrida". È importante, di conseguenza, guardare a strumenti trasversali sia dal punto di vista giuridico che operativo e tecnologico, individuando o istituendo attori che possano agire con procedure il più possibile chiare e rapide.

- *Protezione delle infrastrutture calibrata sul rischio*. Le infrastrutture non sono esposte alla minaccia in modo uguale: diventa quindi importante individuare i siti maggiormente esposti e calibrare di conseguenza le capacità di protezione. In alcuni casi, infatti, la sola presenza di un drone può essere sufficiente a determinare un'interruzione del servizio, come negli aeroporti con il blocco del traffico aereo. In altri, invece, il rischio può essere quello di esplosioni o la dispersione di sostanze pericolose. Nello svolgimento del *risk assessment*, così come previsto dalla direttiva Cer[55], è importante che a livello nazionale e a livello di infrastruttura un approccio tradizionale sia integrato con un approccio che include anche nuovi rischi e attori.
- *Cultura della sicurezza*. Infine, il verificarsi di episodi di sorvolo sospetto in prossimità di siti sensibili e di infrastrutture su cui si fa affidamento per l'erogazione di servizi essenziali, rende cruciale una maggiore cultura della sicurezza anche tra la popolazione, che deve essere preparata ad avere un ruolo più attivo e consapevole in caso di crisi e deve conoscere i comportamenti da adottare. Allo stesso modo, una maggiore consapevolezza da parte degli stessi operatori delle infrastrutture, potrebbe portare non solo a impedire un sorvolo illecito in prima istanza, ma anche a garantire che un evento ostile non produca effetti sistemici, impedendo così impatti e interruzioni nell'erogazione di servizi essenziali. Ciò risulta particolarmente rilevante di fronte alla rapidità di sviluppo tecnologico, avanzamento e sofisticazione dei droni duali.

© 2026 IAI

55 Parlamento europeo e Consiglio dell'UE, *Direttiva (UE) 2022/2557 del 14 dicembre 2022 relativa alla resilienza dei soggetti critici*, cit., art. 12.

Acronimi

Apr	Aeromobili a pilotaggio remoto
Asc	Autorità settoriali competenti
Cbrn	Chimico, biologico, radiologico, nucleare
Cema	Cyber electromagnetic activities
Cer	Critical entities resilience
Cir	Comitato interministeriale per la resilienza
Crsc	Conferenza per la resilienza dei soggetti critici
Enac	Ente nazionale per l'aviazione civile
Fpv	First person view
Gnss	Global Navigation Satellite System
IC	Infrastrutture critiche
Lidar	Light detection and ranging
Pcu	Punto di contatto unico
R&S	Ricerca e sviluppo
Uas	Unmanned aircraft systems
UE	Unione europea

© 2026 IAI

L'Istituto Affari Internazionali (IAI) è un think tank indipendente, privato e non-profit, fondato nel 1965 su iniziativa di Altiero Spinelli. Lo IAI mira a promuovere la conoscenza della politica internazionale e a contribuire all'avanzamento dell'integrazione europea e della cooperazione multilaterale. Si occupa di temi internazionali di rilevanza strategica quali: integrazione europea, sicurezza e difesa, spazio, economia internazionale e governance globale, energia e clima, politica estera italiana; e delle dinamiche di cooperazione e conflitto nelle principali aree geopolitiche come Mediterraneo e Medioriente, Asia, Eurasia, Africa e Americhe. Lo IAI pubblica una rivista trimestrale in lingua inglese (*The International Spectator*), una online in italiano (*AffarInternazionali*), due collane di libri (*Trends and Perspectives in International Politics* e *IAI Research Studies*) e varie collane di paper legati ai progetti di ricerca (*Documenti IAI*, *IAI Papers*, ecc.).

Via dei Montecatini, 17
I-00186 Roma
T +39 06 6976831
www.iai.it

Ultimi Documenti IAI

Direttore: **Lorenzo Biondi** (l.biondi@iai.it)
ISSN 2280-6164 | DOI 10.82088/IAIdoc2610

26 | 10	Paola Tessari, Nicolò Murgia e Alessandro Marrone, *La protezione delle infrastrutture critiche dai droni: governance e tecnologia*
26 | 09	Giacomo Bridi, *In Search of a Balance: Europe and America in the Trump Era*
26 | 08	Christian Labriola, *The Russian Way to Military Recruitment and the Spectre of Mobilisation*
26 | 07	Andrea Grillo, Alessandro Marrone e Michele Nones, *Intelligenza artificiale e Difesa italiana: sfide e opportunità*
26 | 06	Alessia Chiriatti and Ettore Greco, *Sustainable Transitions and Competitiveness: Policy Directions for the European Union and Italy*
26 | 05	Federico Castiglioni and Luca Cinciripini, *The Future of European Defence: Industrial Ambition, Operational Constraints and Flexible Partnerships*
26 | 04	Matteo Bursi, Federica Marconi and Alessio Sangiorgio, *The Reshaping of the European Economic Sovereignty*
26 | 03	Karolina Muti (ed.), *Lessons for Europe and Italy from Other Space Powers: The Civil-Military Interconnection*
26 | 02	Alessia Chiriatti, *Unlocking Strategic Potential Outside the EU: Italy-Turkey Bilateral Partnership in Defence*
26 | 01	Elio Calcagno (ed.), *Taking Multi-domain Operations from Theory to Practice*