Istituto Affari Internazionali



ISSN 2280-6164

DOCUMENTI IAI 20 | 04 - MARZO 2020

# La minaccia dei droni duali e le sfide per l'Italia

a cura di Ester Sabatino e Francesco Pettinari


## ABSTRACT

Negli ultimi anni la proliferazione dei droni duali ha accresciuto l'intensità della minaccia ibrida e asimmetrica che tali prodotti possono rappresentare. Questa minaccia, esacerbata dall'elevato livello tecnologico raggiunto dai droni duali, affligge sia la sicurezza nazionale che quella del personale impiegato in missioni fuori area. Il costante sviluppo tecnologico che interessa i droni duali non è stato infatti accompagnato dalla definizione di norme che ne regolino l'utilizzo e che stabiliscano con chiarezza le procedure impiegabili al fine di contrastare eventuali impieghi illeciti. Appare necessaria, quindi, la definizione di un quadro regolatorio completo, che tuteli sia gli utilizzatori che gli operatori posti al contrasto dei droni duali. In questo contesto, la definizione dei requisiti operativi e lo sviluppo di sistemi di contrasto all'avanguardia della frontiera tecnologica sono tra le esigenze primarie che l'Italia deve affrontare per assicurare una difesa efficace. Tali sistemi, inoltre, devono essere in grado di garantire elevati standard di sicurezza, tenendo in considerazione le specificità degli ambienti in cui la minaccia si presenta. Finora l'Italia si è contraddistinta per la volontà di guidare lo sviluppo di tali capacità a livello europeo: rafforzare tale posizione tramite un'azione sinergica e coordinata tra decisori politici, Forze Armate e di sicurezza e industria della difesa appare tanto necessario quanto potenzialmente fruttuoso.


keywords

*Droni* | *Sicurezza* | *Trasporti* | *Infrastrutture* | *Industria della difesa* | *Politica militare dell'Italia* | *Missioni militari*

# La minaccia dei droni duali e le sfide per l'Italia

a cura di Ester Sabatino e Francesco Pettinari*



ISSN 2280-6164

## Indice



* Ester Sabatino è ricercatrice nel programma Difesa dell'Istituto Affari Internazionali (IAI). Francesco Pettinari è stato ricercatore junior nei programmi Difesa e Sicurezza dello IAI. I curatori ringraziano Gaia Ravazzolo, tirocinante presso lo IAI, per il prezioso contributo nella fase di ricerca preliminare. Si ringraziano per la collaborazione: Leonardo, il Centro di eccellenza C-M/M APR, il Comando Artiglieria Controaerei, il Comando generale dei Carabinieri (2° Sezione), ENAC e lo Stato Maggiore dell'Aeronautica (3° e 4° Reparto).

· Questo studio è stato realizzato con il supporto di Leonardo e completato il 22 gennaio 2020.

ISSN 2280-6164

DOCUMENTI IAI 20 | 04 - MARZO 2020

## Executive Summary

In seguito a una prima fase di sviluppo avvenuta esclusivamente nel dominio militare gli aeromobili a pilotaggio remoto (APR) o droni[1], hanno iniziato ad essere utilizzati anche per scopi civili. Un numero sempre crescente di aziende e privati ha iniziato a impiegare questi prodotti per scopi commerciali o ricreativi. I droni impiegati per scopi non militari rientrano, in larga parte, nelle categorie mini e micro e sono diventati progressivamente più facilmente reperibili sul mercato, anche tramite acquisti online.

Benché i benefici in termini di costo-efficienza derivanti dall'impiego di droni per le suddette finalità siano molteplici, la proliferazione di queste tecnologie porta con sé delle profonde implicazioni per quanto riguarda la *safety* del sorvolato. Eventuali malfunzionamenti del velivolo o comportamenti erronei da parte dell'operatore che ne causino la caduta, nonché intromissioni involontarie in aree interdette al sorvolo, possono causare danni consistenti sia in termini fisici, che economici e reputazionali.

In virtù delle loro caratteristiche intrinseche, i droni di dimensioni ridotte si contraddistinguono per la loro natura duale, essendo possibile impiegarli anche per finalità illecite di varia natura. I droni duali vengono così inseriti tra i mezzi attraverso cui è possibile realizzare una minaccia ibrida, connotata da profonda asimmetria per ciò che afferisce alla *security* di persone, proprietà, traffico aereo convenzionale, infrastrutture critiche, siti di interesse strategico, nonché delle missioni civili e militari in teatro operativo.

Gli UAS duali *off-the-shelf*, ossia senza aver subìto alcuna modifica rispetto alle caratteristiche previste dal costruttore, possono essere impiegati per scopi illeciti. Tuttavia, esistono tecniche di contrasto relativamente semplici e già implementabili dagli stessi costruttori. Da contro, se modificati *ad hoc* da operatori sofisticati, i droni duali rappresentano una minaccia ben più difficile da arginare.

Tra le varie implicazioni dell'impiego per finalità illecite dei droni duali sul territorio nazionale, a preoccupare maggiormente è l'eventuale ricorso a tali tecnologie da parte di singoli individui o organizzazioni terroristiche, soprattutto qualora si impiegassero UAS appositamente modificati e armati. Tali circostanze potrebbero interessare l'aviazione civile, infrastrutture critiche di varia natura, o eventi caratterizzati da grandi assembramenti di persone tramite l'impiego di esplosivi o materiali chimici, biologici, radiologici o nucleari (CBRN).

[1] In questo studio, ad eccezione del capitolo 2 sul contesto giuridico e istituzionale nazionale, si privilegia il termine inglese *Unmanned Aerial System* (UAS).

ISSN 2280-6164

DOCUMENTI IAI 20 | 04 - MARZO 2020

I droni duali rappresentano uno strumento particolarmente adatto per la conduzione di attività criminali e terroristiche per diversi motivi. Grazie al loro impiego, infatti, l'operatore ha maggiori garanzie di mantenere l'anonimato nel compiere il fatto illecito rispetto all'utilizzo di altri mezzi, anche per quanto riguarda la fase di pianificazione dell'attacco. In secondo luogo, i droni duali sono connotati da una grande flessibilità riguardo alla zona di decollo o di lancio e possono muoversi a velocità sostenuta all'interno di perimetri considerevoli. Inoltre, queste tecnologie sono totalmente in grado di aggirare barriere fisiche o altre misure di sicurezza preventiva poste a protezione dei luoghi d'interesse strategico. Da ultimo, il contrasto alle minacce veicolate tramite UAS di dimensioni ridotte risulta particolarmente complesso per la mancanza di strumentazioni adatte allo scopo, come dimostrato da alcuni recenti eventi di cronaca.

Per quanto concerne i teatri operativi, l'impiego di droni duali da parte di entità non statuali e milizie irregolari rappresenta un elemento d'innovazione relativamente recente, ma che si sta consolidando in maniera sostanziale. In tal senso, i principali utilizzi di droni duali possono riguardare attacchi diretti a contingenti in movimento o basi militari e vari assetti dislocati sul territorio, nonché attività di *Intelligence, Surveillance, Target Acquisition and Reconnaissance* (ISTAR). Oltre a comportare maggiori rischi per il personale civile e militare dispiegato, l'utilizzo di droni duali potrebbe anche fornire alle milizie irregolari degli strumenti in grado di ridurre il loro svantaggio tecnologico, mettendo quindi a rischio la buona riuscita delle missioni regolari.

Indipendentemente dall'ambito in cui possono verificarsi, le minacce correlate ad impieghi illeciti dei droni duali sono esacerbate dall'elevato livello tecnologico raggiunto dai droni, che li rende particolarmente performanti e versatili. L'incremento delle caratteristiche tecnologiche degli UAS è stato accompagnato da una tendenza alla riduzione dei prezzi di questi prodotti sul mercato e si è sviluppata principalmente intorno a tre tendenze: miniaturizzazione dei componenti, autonomia del drone rispetto all'operatore e possibilità di agire in sciami. Grazie al processo di miniaturizzazione risulta attualmente possibile montare sul drone componenti tecnologicamente molto avanzati senza inficiarne le potenzialità d'utilizzo. La volontà di accrescere l'autonomia del drone rispetto all'operatore ha portato allo sviluppo di componenti hardware e software grazie ai quali è possibile limitare il ruolo dell'operatore alle fasi preliminari al decollo. Risulta, infatti, possibile pianificare la rotta dei droni basandosi sull'elaborazione autonoma di segnali GPS, o su sistemi a odometria visivo-inerziale (VIO) che ne garantiscono il funzionamento anche in assenza di segnali satellitari. Da ultimo, la possibilità di impiegare su larga scala gli sciami, ossia gruppi di UAS guidati dall'intelligenza artificiale (AI) in grado di reagire in maniera coordinata o cooperativa ad eventuali stimoli esterni inattesi, sembra essere sempre più prossima.

Date le considerevoli implicazioni per la sicurezza nazionale e i contingenti impegnati in missioni fuori area, si riscontra l'impellente necessità di normare l'impiego dei droni duali sia a livello nazionale che europeo e internazionale. Necessità resa ancor più stringente dal ritardo con cui i vari legislatori si sono

mossi rispetto alla proliferazione di questi prodotti.

Il Regolamento di esecuzione dell'UE n. 947 del 24 maggio 2019, così come il successivo Regolamento Mezzi Aerei a Pilotaggio Remoto, edizione n. 3 dell'11 novembre 2019 emanato dall'Ente Nazionale per l'Aviazione Civile (ENAC) per recepire quanto normato dall'Unione europea, rappresentano un iniziale contributo per la mitigazione delle minacce. Stabilendo dei parametri relativi all'impiego dei droni duali per scopi leciti, tali regolamenti potrebbero sostanzialmente ridurre il numero di intromissioni involontarie in aree interdette al sorvolo o in prossimità di siti di interesse strategico. Al contempo, fissare l'obbligo per produttori e operatori di inserire appositi dispositivi per permettere l'identificazione del velivolo o prevenirne lo sconfinamento in aree interdette, renderebbe più semplice distinguere tra i droni autorizzati alle operazioni di volo da quelli che non lo sono.

Se è possibile categorizzare come potenzialmente minaccioso un UAS che non rispetti tali parametri, non si ha però garanzia del fatto che prodotti che risultano in regola non rappresentino una minaccia. Come già ampiamente dimostrato dai fatti, esistono numerose possibilità per aggirare tali norme e sistemi. Va pertanto chiarito quali siano le autorità preposte al contrasto di droni ostili o potenzialmente tali. Inoltre, con particolare riferimento al contesto nazionale, risulta necessario definire le modalità secondo cui le Forze Armate possono supportare le autorità preposte al mantenimento della pubblica sicurezza. Le peculiari capacità acquisite in ambito militare, infatti, possono risultare determinanti nel contrastare una minaccia veicolata per mezzo di droni duali, soprattutto nel caso in cui questa dovesse essere portata da prodotti modificati *ad hoc*.

In maniera similare, risulta necessaria un'analisi del quadro legislativo nazionale e internazionale relativo all'attribuzione di responsabilità nel caso in cui dovessero verificarsi danni a terzi durante un'operazione di contrasto ai droni duali, nonché delle scriminanti per le autorità o i singoli operatori. Le differenze esistenti nell'attuale quadro normativo derivanti dall'ambito nel quale le operazioni di contrasto vengono effettuate, sia esso nazionale o afferente ai teatri operativi, aprono a scenari parzialmente diversi. Ciononostante, qualora le azioni degli operatori preposti al contrasto degli UAS duali rispettassero i parametri fissati, l'esenzione di responsabilità sarebbe prevista dalla legislazione vigente.

Introdurre norme volte a limitare il concretizzarsi di una minaccia non è però sufficiente a scongiurarla. Si rende quindi necessario lo sviluppo di sistemi e procedure che permettano di contrastare le minacce portate dagli UAS duali sia tramite mezzi cinetici, che con strumenti tecnici.

Le attività di contrasto attuabili sono particolarmente influenzate dal contesto nel quale esse vengono messe in atto. In un contesto urbano, l'abbattimento di un drone con mezzi cinetici risulta scarsamente indicato poiché con lo schianto al suolo si rischierebbe di provocare impatti simili a quelli intesi da chi ha condotto l'attività illecita. Creare strumenti capaci di contrastare il drone senza causarne la caduta e il successivo schianto al suolo risulta dunque fondamentale. Nei


ISSN 2280-6164

teatri operativi l'abbattimento tramite mezzi cinetici è più attuabile, ma si rende comunque necessaria la capacità di rilevare e tracciare (*detection and tracking*) il drone ostile.

Presa coscienza di tali necessità, sia il settore privato che quello pubblico nazionale e internazionale, hanno iniziato ad investire copiosamente nello sviluppo di sistemi *counter-drones* (o *Counter-Unmanned Aerial Systems* – C-UAS) idonei allo scopo.

Per poter essere considerato efficace e garantire elevati standard di protezione, un sistema C-UAS dovrebbe essere modulare, ossia in grado di compiere tutte le azioni necessarie a un contrasto efficace della minaccia utilizzando gli strumenti più appropriati a seconda dell'ambito in cui essa si verifica. I sistemi C-UAS devono essere in grado di individuare il drone, rilevandone dapprima la presenza per poi identificarlo e categorizzarlo come ostile. Questi sistemi devono in seguito garantire la possibilità di tracciare il velivolo al fine di stabilire se esso si stia dirigendo verso siti d'interesse strategico o aree interdette al sorvolo. Tali capacità risultano fondamentali per poter mettere in campo gli strumenti più appropriati all'interdizione della minaccia tra quelli di cui il sistema C-UAS dovrebbe essere dotato, limitando quanto più possibile il ruolo dell'operatore alla scelta e attuazione delle misure di interdizione a seconda dell'ambiente circostante.

Le tecniche d'interdizione non cinetiche già impiegate dai sistemi C-UAS sono molteplici, ma rischiano di essere inefficaci in presenza di droni tecnologicamente avanzati o che abbiano subìto modifiche rispetto alla configurazione di fabbrica. Infatti, il disturbo delle comunicazioni tra il drone e l'operatore (*jamming*) non ha alcun effetto su droni che si muovono seguendo rotte preimpostate, e l'inibizione dei segnali GPS (*spoofing*) non è in grado di fermare l'avanzata di un velivolo che impieghi piattaforme VIO nella navigazione.

Allo scopo di creare sistemi C-UAS efficaci e, più in generale, di sviluppare soluzioni e procedure in grado di contrastare efficacemente la minaccia, alcune organizzazioni internazionali, come la NATO e l'UE, hanno lanciato numerose iniziative e progetti. Allo stato attuale manca, infatti, una standardizzazione di procedure e sistemi da impiegare in caso di attacco da droni duali. Ciò inficia non solo la possibilità di avere sistemi interoperabili tra loro, ma diversifica, non sempre tramite coordinamento, gli sforzi.

A livello NATO, le iniziative si sono sviluppate principalmente all'interno del programma Science for Peace (SPS), della Emerging Security Challenges Division (ESDC) e, soprattutto a livello di studi preliminari, dal Joint Air Power Competence Centre (JAPCC). L'inclusione delle capacità C-UAS all'interno del NATO Defence Planning Process (NDPP), non ancora avvenuta ma in fase di studio, è uno degli obiettivi principali che l'Alleanza si è preposta nel campo C-UAS. Per quanto riguarda l'UE, l'attenzione posta dalla classe politica alle minacce portate dai droni duali risulta essere molto alta, sia sul versante civile che su quello militare e interessa ugualmente la definizione di un quadro regolatorio completo e lo


ISSN 2280-6164

sviluppo capacitivo. Tramite i programmi Horizon 2020 e quelli rientranti nel Programma europeo di sviluppo del settore industriale della difesa (*European Defence Industrial Development Programme*, EDIDP), la Commissione europea ha stanziato fondi per lo sviluppo di strumenti e procedure di *counter-drones* efficaci e condivisi.

In Italia, la volontà di dotarsi delle necessarie capacità per difendersi dalle minacce veicolate dai droni duali è stata affermata in maniera chiara dalla difesa. Sia nelle priorità di ammodernamento delle Forze Armate del 2018, che nel Documento programmatico pluriennale (DPP) 2019-2021 è stata posta grande attenzione al tema C-UAS. Ciò si è tradotto nello stanziamento di fondi per l'acquisizione di queste capacità, così come nell'istituzione del Centro di eccellenza Counter Mini/Micro Aeromobili a Pilotaggio Remoto (CDE C-M/M APR) a valenza interforze presso il Comando Artiglieria Controaerei (COMACA) di Sabaudia. La collaborazione delle Forze Armate è volta allo svolgimento di attività di studio e sperimentazione di sistemi di contrasto dei droni duali, nonché al supporto delle autorità di pubblica sicurezza in occasione di eventi pubblici sul territorio nazionale. L'Italia ambisce a diventare il Paese di riferimento in Europa per quanto riguarda le attività di contrasto ai droni duali, ed ha pertanto assunto il ruolo di leader di due progetti PeSCo volti allo sviluppo di sistemi e procedure C-UAS.

Rimangono ancora non definiti, a livello italiano, degli aspetti di particolare rilevanza. Affinché il Paese sia in grado di assicurare livelli di sicurezza adeguati a livello nazionale e di presentarsi a livello regionale e internazionale come un interlocutore di rilievo, all'Italia manca una strategia nazionale chiara che indichi requisiti operativi e numerici nonché procedure operative inerenti alle capacità C-UAS. Per giungere a tale obiettivo, si rende necessario uno sforzo congiunto, da una parte, dei ministeri e delle amministrazioni coinvolte nel definire una posizione condivisa e nell'allocare le risorse finanziarie necessarie, dall'altra, degli attori statali e delle imprese operanti nel settore per mantenere le capacità C-UAS alla frontiera tecnologica.


ISSN 2280-6164

## 1. Le nuove minacce

di Francesco Pettinari

Tra le evoluzioni tecnologiche degli ultimi due decenni, i droni meritano sicuramente una menzione speciale. Il termine droni ha riscosso ampio successo mediatico e, ad oggi, esso viene utilizzato per riferirsi indiscriminatamente a concetti che presentano alcune differenze tra loro. In particolare, si può parlare di *Unmanned Aerial Vehicle* (UAV) per riferirsi al velivolo in sé, o di Sistemi aeromobili a pilotaggio remoto (SAPR, o *Remotely Piloted Aircraft System*, RPAS) in virtù della possibilità di pilotare questi velivoli da remoto. Più spesso però ci si riferisce a *Unmanned Aircraft System* (UAS), definizione che fa riferimento al velivolo e tutti i suoi componenti, inclusi sensori ed eventuali carichi trasportati[2].

Dopo una prima fase di applicazione e innovazione in ambito esclusivamente militare, lo sviluppo tecnologico ha interessato anche droni progettati per essere utilizzati in ambito civile e questi prodotti hanno iniziato a diffondersi in maniera capillare in molteplici settori[3]. Di conseguenza, il mercato globale degli UAS risulta essere tra quelli in maggiore espansione, tanto da far stimare che entro il 2020 vi saranno opportunità di mercato e investimenti complessivi superiori ai 90 miliardi di euro. Nonostante circa il 70 per cento di questo valore sia previsto rimanere legato al comparto militare, i droni stanno seguendo le orme di altre tecnologie che, pur nascendo per uso esclusivo del dominio militare, permeano ormai totalmente la vita dei singoli cittadini, come è avvenuto con Internet o i sistemi GPS. La quota di mercato che secondo Goldman Sachs sarà occupata dai droni commerciali dovrebbe raggiungere 11,5 miliardi di euro entro il 2020, mentre quella relativa ai prodotti acquistati dai singoli utenti (prodotti *consumer*) si attesterebbe intorno ai 15 miliardi di euro[4].

La proliferazione di droni progettati per scopi civili presenta profonde implicazioni per ciò che riguarda la *safety* di persone e proprietà nonché di molteplici infrastrutture critiche, traffico aereo convenzionale o aree nelle quali sono presenti grandi concentrazioni di persone[5]. Ciò è dovuto al fatto che questi velivoli potrebbero cadere al suolo creando danni a persone o cose, introdursi anche involontariamente in aree ristrette al volo causando alterazioni nel funzionamento

[2] Per una panoramica delle differenze esistenti tra gli acronimi utilizzati si veda: International Civilian Aviation Organization (ICAO), *Unmanned Aircraft System (UAS)* (Cir 328 AN/190), Montréal, 2011, https://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf.

[3] Philip Boucher, "Civil Drones in Society. Societal and Ethics Aspects of Remotely Piloted Aircraft Systems", in *JRC Science and Policy Reports*, 2014, p. 7-8, http://dx.doi.org/10.2788/146.

[4] Goldman Sachs, *Drones. Reporting for Work*, 2016, https://www.goldmansachs.com/insights/technology-driving-innovation/drones.

[5] Filippo Tomasello, Marco Ducci, *Research for TRAN Committee: Safe Integration of Drones Into Airspace*, Brussels, European Parliament, settembre 2016, http://www.europarl.europa.eu/thinktank/it/document.html?reference=IPOL_STU(2016)585894.

ISSN 2280-6164

delle infrastrutture sottostanti o causare *mid-air collision* con velivoli, aerei ed elicotteri convenzionali pilotati.

Anche a livello di *security* i droni rappresentano un elemento che richiede grande attenzione. Infatti, i droni attualmente disponibili in commercio sono connotati da un'intrinseca natura duale, in quanto le loro caratteristiche, oltre a permettere consistenti miglioramenti in termini qualitativi in tutti quei settori nei quali possono essere impiegati correttamente, ne consentono altresì l'utilizzo per scopi illeciti di vario genere.

L'impiego di droni duali da parte di singoli soggetti o organizzazioni non statuali con scopi illeciti costituisce una minaccia sempre più concreta, tanto per la sicurezza nazionale, quanto per il personale civile e militare impegnato in missioni fuori area. Tale minaccia è esacerbata dalla crescente disponibilità di questi prodotti sul mercato, unitamente a un costante incremento delle loro performance.

Di pari passo, il prezzo dei prodotti acquistabili sul mercato e dotati di elevate caratteristiche tecniche si è ridotto in maniera considerevole, mentre gli strumenti necessari per il rilevamento e il tracciamento (*detection and tracking*) nonché per l'interdizione (*interdiction*) dei droni duali rimangono costosi, complessi e con efficacia ancora non ottimale, fattori che amplificano il carattere asimmetrico della minaccia. Tutti questi elementi hanno portato i droni ad assumere un ruolo di primo piano nel panorama delle minacce ibride e l'elaborazione di una strategia sistemica di contrasto appare oggi come una necessità primaria.

### *1.1 Le caratteristiche*

L'utilizzo crescente di droni per scopi non militari è dovuto alla loro caratteristica principale, ossia all'assenza del pilota a bordo. Tale assenza è resa possibile da sistemi di pilotaggio remoto basati su radiocomandi modulati su frequenze preimpostate, o che utilizzano connessioni stabilite tramite reti Wi-Fi e facilmente generabili da comuni smartphone. In entrambi i casi, il pilotaggio di questi UAS può avvalersi di vari livelli di supporto derivanti dall'utilizzo di segnali GPS[6].

Grazie alle innovazioni tecnologiche più recenti, alcuni UAS sono in grado di operare in modo completamente autonomo, rendendo necessarie azioni da parte dell'operatore esclusivamente nella fase precedente al decollo. Ciò è reso possibile da software che permettono ai droni di elaborare autonomamente i segnali GPS e di seguire rotte preimpostate. Inoltre, si è recentemente assistito all'integrazione di sistemi di navigazione inerziale (*Inertial Navigation System*, INS)[7] nell'hardware del drone che, se utilizzati in maniera coordinata con sistemi a odometria visuale, permettono al drone di muoversi in autonomia senza avvalersi dell'ausilio di

[6] John Patrick Pullen, "This is How Drones Work", in *Time*, 3 aprile 2015, https://time.com/3769831.

[7] UAV Navigation Blog: *UAV Navigation in Depth: Inertial Navigation*, https://www.uavnavigation.com/node/316.


ISSN 2280-6164

segnali GPS. Tali sistemi consentono l'acquisizione di dati e la conseguente mappatura tridimensionale (3D) dell'area di volo, dando al drone la possibilità di stabilire la propria rotta fino al punto o obiettivo indicato dall'operatore senza incorrere in collisioni con oggetti fissi o mobili presenti sul percorso[8]. Le case produttrici pongono grande importanza sul tema dell'autonomia dei loro UAS rispetto all'operatore ed è lecito attendersi che questa caratteristica subisca grandi e repentini miglioramenti nel prossimo futuro, così come è avvenuto per tutte le altre caratteristiche tecniche dei droni[9].

Pertanto i droni duali possono anche essere sistemi molto complessi, ma ne esistono di svariate tipologie che presentano diversi gradi di avanzamento tecnologico.

In linea generale è possibile definire le componenti presenti in tutti gli UAS, inclusi quelli meno sofisticati dal punto di vista tecnologico[10]. Queste componenti sono identificabili con il velivolo in sé, il carico utile trasportato (*payload*), la sensoristica di cui è provvisto, gli elementi di supporto come le piattaforme e i sistemi di lancio (fatta eccezione per gli UAS lanciati a mano), gli eventuali sistemi di comunicazione con l'operatore e, secondo alcune definizioni, anche l'operatore stesso[11].

Ciononostante, la loro classificazione viene generalmente effettuata tenendo conto di altre caratteristiche come l'altitudine a cui operano, la distanza massima che possono raggiungere rispetto alla postazione (o zona) di lancio e il peso complessivo dell'UAS, includendo quindi l'eventuale carico trasportato. Tuttavia, le principali classificazioni esistenti, sia in ambito militare[12] che civile[13], usano quest'ultima specifica come discriminante per la classificazione e solo in un secondo momento a ogni categoria vengono associati dei valori rappresentativi per tutte le altre caratteristiche. Le categorie identificate sono:

- micro o nano droni, con peso compreso tra i 250 gr e i 2 kg;
- mini droni, con peso compreso tra i 2 e i 20 kg;
- droni piccoli, con peso superiore ai 20 kg;
- droni medi, o tattici, con peso compreso tra 150 e 600 kg;
- droni grandi, con peso superiore ai 600 kg.

[8] Si veda, ad esempio, il drone sviluppato dal Massachusetts Institute of Technology (MIT) nel 2018. Rob Matheson, "Fleets of Drones Could Aid Searches for Lost Hikers", in *MIT News*, 1 novembre 2018, http://news.mit.edu/2018/fleets-drones-help-searches-lost-hikers-1102.

[9] "The World's Smallest "Better Than GPS" Inertial Navigation System Now Available", in *Inside Unmanned Systems*, 7 settembre 2017, https://insideunmannedsystems.com/?p=22018.

[10] Tight Camera, *Toy Drones vs Enthusiast Drones: What's the Difference?*, 28 marzo 2018, https://tightcamera.com/?p=964.

[11] Joint Air Power Competence Centre (JAPCC), *Strategic Concept of Employment for Unmanned Aircraft Systems in NATO*, Kalkar, JAPCC, gennaio 2010, http://www.japcc.org/wp-content/uploads/UAS_CONEMP.pdf.

[12] Ibid.

[13] Tania Latici, *Civil and Military Drones. Navigating a Disruptive and Dynamic Technological Ecosystem*, Brussels, European Parliament, ottobre 2019, http://www.europarl.europa.eu/thinktank/it/document.html?reference=EPRS_BRI(2019)642230.


ISSN 2280-6164

Mentre i droni grandi sono per ora impiegati esclusivamente per scopi militari con finalità strategiche e possono coprire distanze intercontinentali trasportando *payload* di alcune tonnellate, gli UAS che ricadono in tutte le altre categorie hanno natura duale e, pertanto, possono potenzialmente rappresentare una minaccia[14].

Un primo esempio di utilizzo dei droni a fini civili è fornito dai governi nazionali, i quali impiegano droni piccoli – o in alcuni casi droni medi – per scopi di ordine pubblico, contrasto alla criminalità comune e organizzata, monitoraggio di zone a rischio di disastri naturali e operazioni di *disaster recovery*[15]. Questi prodotti hanno un costo superiore ai 10 mila euro, sono caratterizzati da un'elevata complessità d'utilizzo, e sono difficilmente reperibili sul mercato *consumer*, fattori che rendono complessa l'acquisizione e l'impiego di questa tipologia di droni da parte di soggetti che vogliano utilizzarli per scopi illeciti[16].

Diverso è invece il caso dei droni impiegati da aziende e privati per scopi commerciali e industriali, i quali ricadono nelle prime tre categorie sopraelencate, ossia droni micro, mini e piccoli. Anche in virtù dei costi decisamente più contenuti di questi prodotti rispetto alle loro controparti utilizzate da enti governativi, un numero sempre crescente di professionisti e aziende che operano in vari ambiti[17] si affida sempre più ai droni per ottenere prestazioni migliori in termini qualitativi e di costo-efficienza[18]. Inoltre, negli ultimi anni si è assistito alla crescita esponenziale del numero di hobbisti, amatori e appassionati che acquistano droni a fini ricreativi. Come mostrato da una ricerca pubblicata dal consorzio europeo Single European Sky ATM Research (SESAR)[19] nel 2016, il numero di questi prodotti in circolazione nell'UE sta aumentando esponenzialmente ed è previsto passare da 1,5 milioni di esemplari nel 2016 a più di 5 milioni nel 2020[20]. Secondo altre stime, il numero di questi prodotti in Europa potrebbe raggiungere addirittura gli 8 milioni

[14] Peter Novitzky, Ben Kokkeler, Peter-Paul Verbeek, "The Dual Use of Drones", in *Tijdschrift voor Veiligheid*, Vol. 17, No. 1-2 (2018), p. 79-95.

[15] Phil Goldstein, "Drones Take Flight for a Variety of Missions in Government", in *FedTech Magazine*, 20 dicembre 2018, https://fedtechmagazine.com/article/2018/12/drones-take-flight-variety-missions-government. Per l'Italia si veda: Maurizio Vallone e Alessandro Carini, "Il drone con la divisa", in *Polizia moderna*, 7 novembre 2017, https://poliziamoderna.poliziadistato.it/articolo/3535a01cb03b650d306343761.

[16] UK Secretary of State for the Home Department, *UK Counter-Unmanned Aircraft Strategy*, ottobre 2019, p. 8, https://www.gov.uk/government/publications/uk-counter-unmanned-aircraft-strategy.

[17] Tra i settori nei quali gli UAS sono maggiormente utilizzati a fini commerciali si annoverano edilizia, agricoltura, rilevazioni geografiche, fotografia e cinematografia.

[18] Jon Walker, *Industrial Uses of Drones – 5 Current Business Applications*, Emerj, 30 gennaio 2019, https://emerj.com/ai-sector-overviews/industrial-uses-of-drones-applications.

[19] Il consorzio SESAR è stato lanciato su iniziativa della Commissione europea e di EUROCONTROL nel 2004. Ad oggi esso conta 19 membri pubblici e privati che, anche in virtù della loro natura consorziata, raggruppano più di 100 enti che rappresentano l'intera comunità attiva nella gestione del traffico aereo europeo. Per maggiori informazioni si veda il sito del SESAR: *Partnering for Smarter Aviation*, https://www.sesarju.eu/index.php/node/20.

[20] SESAR, *European Drones Outlook Study. Unlocking the Value for Europe*, novembre 2016, https://www.sesarju.eu/node/2951.

ISSN 2280-6164

entro il 2022[21]. Similmente, la Federal Aviation Administration (FAA) statunitense stima che nel 2020 i droni duali utilizzati per scopi ricreativi e commerciali negli Stati Uniti saranno circa 2,5 milioni[22].

I prezzi dei droni di piccole dimensioni dipendono in larga misura dalle specifiche tecniche in termini di velocità, raggio d'azione, durata delle batterie o altre fonti di alimentazione, ma sono anche influenzati dal tipo di sensoristica e componenti aggiuntive applicate[23]. La grande espansione del mercato dei droni ha portato le case produttrici ad innescare una corsa alla miniaturizzazione ed evoluzione tecnologica volta a migliorare le specifiche dei loro prodotti, avviando anche una tendenza alla riduzione dei costi dei prodotti finali e rendendo accessibili, a prezzi più contenuti rispetto al passato, prodotti che garantiscono prestazioni sempre più elevate[24]. Per prezzi inferiori ai mille euro è possibile acquistare droni che rientrano nella categoria mini capaci di volare a velocità sostenute (spesso intorno ai 50 Km/h) per dei tempi che variano tra i 20 e i 30 minuti e che possono essere pilotati da remoto fino a distanze che raggiungono i 5 km. Inoltre, questi prodotti presentano software in grado di utilizzare segnali GPS che assistono il pilota o che garantiscono la possibilità di navigazione completamente autonoma basata su rotte preimpostate[25]. In alcuni casi, i droni che rientrano in questa fascia di prezzo presentano anche la capacità di volo autonomo derivante dall'utilizzo di sistemi a odometria visivo-inerziale (*Visual-Inertial Odometry*, VIO), o risultano comunque idonei per supportare l'istallazione di queste tipologie di componenti.

Anche dal punto di vista del carico utile trasportabile questi droni risultano avere una capacità considerevole, potendo il carico ammontare fino a circa il 20 per cento dell'intero peso del velivolo[26]. Va però notato come l'eventuale trasporto di questi *payload* possa incidere, in maniera più o meno consistente, sulle altre prestazioni, a seconda del peso del drone, dei materiali di cui questo è composto e delle condizioni atmosferiche in cui si trova ad operare[27].

[21] Commissione europea, *European Commission and European Investment Bank Announce Launch of "European Drone Investment - Advisory Platform"*, 17 ottobre 2019, https://ec.europa.eu/transport/modes/air/news/2019-10-17-european-drone-investment-advisory-platform_en.

[22] Federal Aviation Administration (FAA), *FAA Aerospace Forecast. Fiscal Years 2019-2039*, aprile 2019, https://www.faa.gov/data_research/aviation/aerospace_forecasts. Si veda anche: Philly by Air, *33 Eye-Opening Drone Stats - Key Trends for 2019*, 12 marzo 2019, https://www.phillybyair.com/?p=7499.

[23] Jack Brown, "Cost of Drones: A Quick Glance Before the Purchase", in *DroneLab*, aggiornato 7 dicembre 2019, https://www.mydronelab.com/?p=852.

[24] Michel Busch, "Unmanned Aerial Systems Miniaturization", in *JAPCC Journal*, No. 25, inverno 2017/2018, p. 75-79, https://www.japcc.org/unmanned-aerial-systems-miniaturization.

[25] Drone Supremacy: *The Best Drones Under $1000*, https://www.drone-supremacy.com/best-drones-under-1000.

[26] Drone Tech Planet, *How Much Weight Can a Drone Carry?*, 2019, https://www.dronetechplanet.com/how-much-weight-can-a-drone-carry.

[27] Alex Sayad, "10 Facts on How Much Weight a Small Drone Can Carry", in *DD Counter Measures*, 24 agosto 2019, https://www.ddcountermeasures.com/how-much-weight-a-small-drone-can-carry.


ISSN 2280-6164

Salendo leggermente di prezzo si possono acquistare UAS che garantiscono prestazioni più elevate, le quali possono essere sfruttate anche da quegli operatori che vogliono utilizzarli per scopi illeciti. Droni pilotabili da distanze che possono raggiungere i 7 km, capaci di toccare picchi di velocità anche di 90 Km/h e che possono restare in volo per almeno 40 minuti[28], ben possono essere sfruttati per perpetrare attacchi terroristici o svolgere attività criminali. Le componenti e la sensoristica associate a questi droni risultano essere solitamente molto avanzate, soprattutto in termini di supporto GPS al pilotaggio e di capacità di navigazione autonoma. In virtù del loro peso maggiore (raramente inferiore ai 3 kg) e dei materiali con i quali sono costruiti, essi risultano più stabili rispetto a droni più piccoli ed economici anche in condizioni atmosferiche avverse. Inoltre, sono in grado di trasportare *payload* più pesanti con un impatto minore in termini di stabilità e velocità e, pertanto, potrebbero essere armati con quantità considerevoli di cariche esplosive o agenti chimici, biologici, radiologici, nucleari (CBRN).

Riguardo alla distanza massima tra l'operatore e il drone, è importante sottolineare come l'avvento di tecnologie cellulari di quinta generazione (5G) possa ridurre o addirittura abbattere queste barriere. Tramite la comunicazione satellitare della rete 5G, gli UAS potranno essere in grado di coprire distanze molto maggiori rispetto all'operatore e si può ritenere che l'unica limitazione nelle distanze percorse sarà quella derivante dalla durata delle batterie[29]. Inoltre, in virtù della grande velocità alla quale viaggiano le comunicazioni su tali reti e in virtù della loro capacità di raggiungere ogni punto del mondo ricorrendo all'ausilio dei satelliti, è teoricamente possibile immaginare che gli UAS, utilizzando tali tecnologie, possano essere pilotati (o attivati nel caso di volo autonomo) anche da distanze intercontinentali.

Indipendentemente dalle fasce di prezzo nelle quali ricadono, UAS duali che presentano sofisticati livelli di sviluppo tecnologico e loro componenti sono facilmente reperibili sia in negozi di elettronica che online, fattore che amplifica la possibilità di utilizzo di droni *off-the-shelf*[30] per scopi malevoli. Tuttavia, va tenuto in considerazione il ruolo degli operatori sia per quanto concerne la loro capacità di apportare modifiche agli UAS sia per ciò che riguarda la volontarietà delle azioni potenzialmente minacciose. Secondo uno studio dell'Università di Austin[31], gli operatori sono categorizzabili in non sofisticati e sofisticati. I primi sono quegli operatori in grado di pilotare, impostare rotte o settare i parametri di navigazione autonoma per i droni, ma incapaci di assemblarli da zero o modificarli. I secondi

[28] Joseph Flynt, "7 Most Expensive Drones", in *3D Insider*, 4 aprile 2019, https://3dinsider.com/most-expensive-drones.

[29] Charles Moore, "Long Range Commercial Drone Control in 5G Wireless Technology", in *NextGen*, 28 maggio 2019, https://nextgenexecsearch.com/?p=2975.

[30] Con l'espressione droni *off-the-shelf* si intendono quei prodotti utilizzati così come si presentano al momento dell'acquisto senza modifiche di sorta da parte dell'operatore.

[31] Todd Humphreys, "Prepared Statement", in US House of Representatives Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, *Hearing: Unmanned Aerial System Threats: Exploring Security Implications and Mitigation Technologies*, Washington, 18 marzo 2015, p. 10-15, https://www.govinfo.gov/app/details/CHRG-114hhrg94580/context.


ISSN 2280-6164

invece sono in grado di assemblare un drone *ex novo* potendo modificarne anche le componenti hardware e software al fine di incrementarne le caratteristiche tecniche. È in quest'ultima categoria che vengono fatti ricadere gli operatori in grado di equipaggiare il velivolo con *payload* potenzialmente ostili.

Inoltre, i diversi tipi di operatori possono veicolare minacce di intensità diversa a seconda del grado di intenzionalità dell'utilizzo di droni su aree ristrette al volo e luoghi sensibili. I tipi di minaccia possono essere categorizzati in tre classi[32]: (1) intromissioni involontarie; (2) intromissioni volontarie, effettuate da operatori non sofisticati; (3) intromissioni volontarie, effettuate da operatori sofisticati.

La linea di demarcazione tra operazioni volontarie e involontarie è spesso molto labile e l'involontarietà può essere utilizzata come giustificazione da parte dell'operatore qualora venisse perseguito dalle autorità. Un esempio è rappresentato dal caso dell'atterraggio di un drone nelle immediate vicinanze di un sito della BAE System usato per effettuare test sui sottomarini. Quest'intromissione ha portato alla prima condanna nel Regno Unito per uso improprio di droni ricreativi nonostante l'operatore avesse dichiarato di averne solamente perso il controllo[33]. Sebbene il drone utilizzato non trasportasse materiale esplosivo o di altro genere, né fosse dotato di particolari telecamere e sensori per l'acquisizione di dati, questo esempio mostra le potenziali minacce derivanti dall'impiego di droni duali da parte di soggetti privati.

Un sostanziale contributo alla mitigazione delle minacce derivanti dall'intromissione di droni duali *off-the-shelf* in aree sensibili può arrivare dagli stessi produttori tramite l'installazione di sistemi di *geo-fencing* nel software del drone[34], così come l'istallazione un codice identificativo (ID) potrebbe facilitare l'identificazione dei droni non autorizzati al sorvolo di determinate aree e distinguerli da quelli ammessi[35]. Molte case produttrici stanno implementando entrambe queste misure[36].

[32] Ibid. L'autore si riferisce ad "intromissioni" in aree riservate ma, per le finalità di questo rapporto, è possibile estendere il concetto ad operazioni di varia natura anche diverse da intromissioni in aree riservate.

[33] Charles Arthur, "UK's First Drone Conviction Will Bankrupt Me, Says Cumbrian Man", in *The Guardian*, 2 aprile 2014, https://gu.com/p/3z4pf.

[34] Con l'espressione *geo-fencing* si fa riferimento a una funzione automatica che, basandosi su posizione e dati di navigazione del drone, acquisiti tramite GPS e forniti tramite apposito transponder, impedisce l'accesso in aree interdette al sorvolo e indicate dalle autorità di pubblica sicurezza. Per una definizione più approfondita si veda: John Patterson, "Heliguy's Guide to Geofencing", in *Heliguy Insider Blog*, 16 febbraio 2017, https://www.heliguy.com/blog/2017/02/16/heliguys-guide-to-geofencing.

[35] European Aviation Safety Agency (EASA), *Explanatory Note on 'Prototype' Commission Regulation on Unmanned Aircraft Operations*, 22 agosto 2016, https://www.easa.europa.eu/sites/default/files/dfu/Explanatory%20Note%20for%20the%20UAS%20Prototype%20regulation%20final.pdf.

[36] Haye Kesteloo, "DJI Welcomes FAA and Industry Reports on Improving Drone Safety", in *DroneDJ*, 17 ottobre 2019, https://wp.me/p9Rwpe-5im.


ISSN 2280-6164

Più in generale, le forme e le caratteristiche dei droni commerciali potrebbero essere inserite in database forniti alle autorità[37]. Conoscere la forma degli UAV, la velocità di crociera e i tipi di onde elettromagnetiche emesse potrebbe facilitare le funzioni di *detection and tracking* dei sistemi di contrasto dei droni duali. Ciò andrebbe a complementare i sistemi già esistenti basati sul rilevamento dei droni in base ai suoni emessi, i quali risultano però poco efficaci in ambiente urbano o laddove siano presenti considerevoli rumori di sottofondo[38], considerando anche che molti droni utilizzano la propulsione elettrica.

Altro fattore che potrebbe risultare decisivo nelle operazioni di contrasto è la conoscenza delle frequenze radio o Wi-Fi sulle quali avviene la comunicazione tra il velivolo e il pilota, nonché il tipo di sensori utilizzati per l'acquisizione dei segnali GPS. Conoscendo questi elementi risulterebbe relativamente più semplice aggirare la minaccia portata dal drone disturbando la comunicazione tra UAS e operatore, o impedendo l'acquisizione dei segnali GPS. Ciò causerebbe l'attivazione delle funzioni *fail safe*, *freeze* o *return home*[39].

Tuttavia, le contromisure sopracitate risulterebbero inefficaci in presenza di droni adeguatamente modificati da operatori sofisticati. Infatti, eventuali sistemi di *geo-fencing* o codici identificativi potrebbero essere facilmente rimossi tramite software reperibili in rete[40] e i transponder necessari ad impedire il sorvolo di determinate aree o a comunicare l'ID del drone potrebbero essere rimossi o disattivati[41]. Anche l'effettuazione di operazioni di *detection and tracking* efficaci basate sulle informazioni contenute nei suddetti database e relative a prodotti *off-the-shelf* risulterebbe impossibile qualora il drone fosse assemblato artigianalmente con componenti di marche e modelli differenti o costruiti dallo stesso operatore sofisticato. Inoltre, il software del drone potrebbe essere alterato in modo tale da rispondere in maniera differente da quella prevista dal costruttore qualora si tentasse di alterare la comunicazione tra drone e pilota o di inabilitarne l'acquisizione di segnali GPS.

Questo tipo di disturbo potrebbe risultare impossibile in presenza di UAS dotati della capacità di volo autonomo che non si avvale di sistemi di posizionamento e

[37] Jan Farlik et al., "Multispectral Detection of Commercial Unmanned Aerial Vehicles", in *Sensors*, Vol. 19, No. 7, aprile 2019, art. 1517, https://doi.org/10.3390/s19071517.

[38] Matthew Peacock, Michael N. Johnstone, *Towards Detection and Control of Civilian Unmanned Aerial Vehicles*, 14th Australian Information Warfare Conference, Perth, 2-4 dicembre 2013, https://doi.org/10.4225/75/57a847dfbefb5.

[39] Queste funzioni sono programmate dai produttori per attivarsi in seguito alla perdita improvvisa delle comunicazioni tra il drone e l'operatore, o dei segnali GPS. La funzione *fail safe* prevede la lenta discesa verticale e l'atterraggio sicuro del drone, la funzione *freeze* fa sì che il drone si immobilizzi in aria, e la funzione *return home* attiva il ritorno automatico del drone al punto di decollo/lancio impostato.

[40] Feilidh Dwyer, "Is Drone Geofencing Software Too Easy to Hack?", in *WeTalkUAV*, 6 marzo 2019, https://wp.me/p88IHs-6xc; Department 13, *White Paper: Anatomy of DJI's Drone Identification Implementation*, 16 novembre 2017, p. 10, http://department13.com.au/?p=1080.

[41] Lisa Vaas, "Hacked Drones Flying Up, Up And Away Over Geofencing Restrictions", in *Naked Security*, 18 luglio 2017, https://wp.me/p120rT-1AeW.

ISSN 2280-6164

navigazione GPS. Pertanto, l'eventuale utilizzo di droni a scopi illeciti da parte di operatori sofisticati rappresenta una minaccia ben più consistente rispetto a quelle precedentemente indicate sia nel caso in cui essi venissero utilizzati da singoli operatori che da organizzazioni strutturate.

La criminalità comune e organizzata può trarre vantaggio dall'utilizzo di droni sia nel campo cibernetico, che tramite applicazioni più convenzionali. Per quanto riguarda le prime, droni modificati possono essere in grado di favorire l'accesso ai server di grandi aziende o enti governativi estorcendo informazioni[42], nonché la penetrazione nei sistemi operativi dei dispositivi elettronici di soggetti privati, violandone la privacy e acquisendone dati sensibili[43]. La penetrazione nei server e nei sistemi operativi di dispositivi elettronici può avvenire tramite diverse modalità, anche se la più semplice e immediata è quella basata sull'utilizzo di determinati payload capaci di violare le reti wireless, le comunicazioni tramite tecnologia bluetooth o quelle basate sull'identificazione a radio-frequenza (RFID)[44]. Tra i payload che potrebbero essere utilizzati per compiere azioni di questo tipo si annoverano i cosiddetti WiFi Pineapple, ossia dispositivi inizialmente progettati per condurre analisi sulle vulnerabilità delle reti (*penetration test*) ma le cui potenzialità ne ammettono l'utilizzo per scopi illeciti[45]. Inoltre, un vasto numero di altri dispositivi facilmente reperibili in commercio potrebbero servire allo scopo, come dimostrato dal recente episodio riguardante la sottrazione di dati – anche sensibili – dai server della NASA compiuta tramite l'utilizzo di un microcomputer Raspberry Pi[46]. Nonostante in questo caso il microcomputer sia stato introdotto manualmente nella struttura, le dimensioni di questi prodotti ne permettono il trasporto tramite droni che volando in prossimità dei siti d'interesse potrebbero rivelarsi un vettore particolarmente adatto per intromissioni volte a violare il dominio cibernetico.

Applicazioni più convenzionali possono riguardare il trasporto di sostanze illecite, soprattutto con operazioni trans-frontaliere[47], o intromissioni in istituti penitenziari al fine di recapitare materiali non consentiti o di istigare rivolte[48]. Per

[42] "Le nuove minacce da droni e come prevenirle", in *Safety and Security Magazine*, 15 marzo 2018, https://www.safetysecuritymagazine.com/?p=3312.

[43] Bianca Soare, "Cybersecurity and Drones – A Rising Threat?", in *Heimdal Security Blog*, 31 maggio 2019, https://heimdalsecurity.com/blog/?p=14392.

[44] "Companies and Data Centers Should Consider Drones When Assessing Security Risks", in *911 Security Blog*, 17 ottobre 2018, https://www.911security.com/blog/companies-and-data-centers-should-consider-drones-when-assessing-security-risks.

[45] Daniel Oberhaus, "How a Wi-Fi Pineapple Can Steal Your Data (And How to Protect Yourself From It)", in *Vice*, 20 novembre 2017, https://www.vice.com/en_us/article/pa39xv/pineapple-wifi-how-to-mitm-hack.

[46] "Raspberry Pi Used to Steal Data from Nasa Lab", in *BBC News*, 24 giugno 2019, https://www.bbc.com/news/technology-48743043.

[47] Brenda Fiegel, "Narco-Drones: A New Way to Transport Drugs", in *Small Wars Journal*, 5 luglio 2017, hhttps://smallwarsjournal.com/node/71481.

[48] Miriam McNabb, "Drones at Prisons: The Results of This 9-Month Study Show Exactly Why We Need Counter Drone Tech", in *DroneLife*, 15 marzo 2019, https://dronelife.com/?p=63997.


ISSN 2280-6164

quanto riguarda la prima casistica, uno dei teatri nei quali si sono verificati più episodi è quello del confine tra Stati Uniti e Messico dove sono stati riportati più di 560 casi tra il 2011 e il 2018[49]. Con riferimento alle prigioni, invece, sono stati registrati 15 casi di tentativi d'intromissione in istituti penitenziari in Europa tra il 2017 e il 2019[50]. Inoltre, i droni possono essere usati da criminali per effettuare ricognizioni anche per quanto riguarda furti e attività simili[51]. Gruppi terroristici organizzati e singoli individui possono veicolare una seria minaccia terroristica tramite l'impiego di droni duali modificati *ad hoc* per colpire obiettivi sensibili e infrastrutture critiche. I casi degli aeroporti inglesi di Gatwick[52] e Heathrow[53], di quello italiano di Malpensa[54], così come quello di una centrale nucleare situata nelle vicinanze di Lione[55] in Francia, dimostrano la vulnerabilità di queste infrastrutture. Gli UAV che si sono intromessi nelle aree riservate avevano subìto modifiche da parte degli operatori[56] anche se sono risultati essere sprovvisti di cariche esplosive o CBRN. Vanno però tenuti in considerazione gli enormi danni economici e reputazionali derivanti da questi episodi. Prendendo in esame il caso di Gatwick, si nota come la cancellazione o il dirottamento di più di 1.000 voli durante le 33 ore di blocco dell'aeroporto abbiano causato danni economici che ammontano a più di 50 milioni di euro. Inoltre, sono stati più di 140 mila i passeggeri che hanno subito disagi derivanti dal blocco dell'aeroporto. Questi passeggeri sono poi stati risarciti dalle compagnie aeree, le quali, oltre al danno economico, hanno anche subito danni d'immagine al pari della struttura aeroportuale[57]. Sullo sfondo, risulta facile immaginare quali avrebbero potuto essere gli effetti di intromissioni compiute, invece, per finalità terroristiche.

Con particolare riferimento agli aeroporti, è possibile immaginare che qualora l'obiettivo di attività terroristiche dovesse essere un aereo commerciale, l'attacco si verificherebbe proprio in prossimità di questi siti, vista l'impossibilità per i droni

[49] Gina Harkins, "Illicit Drone Flights Surge Along U.S.-Mexico Border As Smugglers Hunt for Soft Spots", in *The Washington Post*, 25 giugno 2018,https://wapo.st/2K6dMkA.

[50] Sito Dedrone: *Worldwide Drone Incidents*, https://www.dedrone.com/resources/incidents/all.

[51] Sito Calder Security: *Theft by Drone?*, https://www.caldersecurity.co.uk/theft-by-drone.

[52] Tom Burridge, "'Sustained' Drone Attack Closed Gatwick, Airport Says", in *BBC News*, 20 febbraio 2019, https://www.bbc.com/news/business-47302902. Inoltre, nell'aprile 2019 un avvistamento di droni nelle vicinanze del medesimo aeroporto ha causato il dirottamento di tre voli, su questo evento si veda: "Flights Diverted after Gatwick Airport 'Drone Sighting'", in *BBC News*, 28 aprile 2019, https://www.bbc.com/news/uk-england-sussex-48086013.

[53] "Heathrow Airport: Drone Sighting Halts Departures", in *BBC News*, 8 gennaio 2019, https://www.bbc.com/news/uk-46803713.

[54] "Drone a Malpensa, 4 voli dirottati", in *Ansa*, 1 aprile 2019, http://www.ansa.it/sito/notizie/topnews/2019/04/01/drone-a-malpensa-4-voli-dirottati_d2c67922-9099-4236-a4dd-eab753e4f857.html.

[55] Geert De Clercq, "Greenpeace Crashes Superman-Shaped Drone Into French Nuclear Plant", in *Reuters*, 3 luglio 2018, https://reut.rs/2tXzAnC.

[56] Nel caso dell'aeroporto di Malpensa non è chiaro se il drone avesse subito modifiche o meno.

[57] Simon Calder, "Gatwick Drone Disruption Cost over £50m", in *The Independent*, 22 gennaio 2019, https://www.independent.co.uk/travel/news-and-advice/gatwick-drone-airport-cost-easyjet-runway-security-passenger-cancellation-a8739841.html; Jamie Grierson, "Gatwick Returns to Normality But Drone Threat Remains", in *The Guardian*, 4 gennaio 2019, https://gu.com/p/acvjq.


ISSN 2280-6164

duali di raggiungere quote elevate. Questa minaccia appare sempre più probabile non solo perché i casi degli aeroporti citati in precedenza hanno dimostrato che queste infrastrutture possono essere violate, ma anche in virtù del fatto che nel solo Regno Unito, nel 2018, sono stati registrati 30 casi di rischi di collisione aerea di classe A, ossia i più pericolosi per la sicurezza aerea (*near-miss*), che hanno visto coinvolti droni[58]. Nessuno di questi rischi di collisione si è poi tradotto in effettiva collisione, né sono emerse evidenze del fatto che i droni in questione fossero usati per entrare in collisione con gli aerei convenzionali, ma la frequenza di questi episodi sottolinea la possibilità concreta che operatori malevoli possano portare a compimento azioni di questo tipo.

In linea generale, è lecito affermare che molteplici tipologie di infrastrutture critiche siano potenziali obiettivi di attacchi veicolati a mezzo droni. Infatti, qualora droni equipaggiati con cariche esplosive o CBRN dovessero schiantarsi sui sistemi di controllo di infrastrutture quali una centrale nucleare, un aeroporto, un porto o una diga impedendone il corretto funzionamento, l'ammontare dei danni economici e il numero di vittime sarebbero enormi. Inoltre, va tenuta in debita considerazione la possibilità che anche attacchi di tipo cibernetico, effettuati tramite UAV, avrebbero conseguenze rilevanti se ad essere attaccate fossero le stesse infrastrutture critiche sopracitate. Per di più, grazie alla capacità degli UAS di raggiungere luoghi impervi e non accessibili via terra è possibile che altri tipi di infrastrutture, come gli acquedotti, divengano oggetto di attacchi tramite l'introduzione di agenti chimici, biologici o radiologici, eventualità che avrebbe effetti drammatici per la popolazione coinvolta. Tali effetti interesserebbero un numero di persone molto elevato vista la capillarità del sistema di fornitura idrica e sarebbero persistenti nel tempo per via delle lunghe e consistenti procedure di bonifica che si renderebbero necessarie al fine di riabilitare l'infrastruttura.

I droni potrebbero anche essere utilizzati per colpire personalità pubbliche di rilievo come esponenti politici o edifici governativi sia tramite collisione diretta con il bersaglio, che attraverso l'utilizzo di cariche esplosive. Episodi di questo tipo si sono verificati in varie zone del mondo, dalla Germania, dove un drone si è avvicinato al Cancelliere Angela Merkel[59] durante un comizio elettorale nel 2013, al Giappone dove un UAS che trasportava minime tracce di materiale radioattivo, non sufficiente a causare danni alla salute delle persone, si è posato sul tetto del palazzo del Primo ministro nel 2015[60]. Nel 2018 la presenza di un drone durante un discorso del Presidente venezuelano Maduro ha scatenato il panico tra civili e militari presenti in quello che, in Venezuela, è stato definito un attentato alla vita

[58] Helen Coffrey, "How Many Drone-Plane Near Misses We Had in the UK This Year", in *The Independent*, 21 dicembre 2018, https://www.independent.co.uk/travel/news-and-advice/drones-planes-collision-uk-gatwick-flights-airports-aircraft-caa-airprox-a8694526.html.

[59] Von Friederike Heine, "Merkel Buzzed by Mini-Drone at Campaign Event", in *Der Spiegel*, 16 settembre 2013, https://www.spiegel.de/international/germany/merkel-campaign-event-visited-by-mini-drone-a-922495.html.

[60] Will Ripley, "Drone with Radioactive Material Found on Japanese Prime Minister's Roof", in *CNN*, 22 aprile 2015, https://edition.cnn.com/2015/04/22/asia/japan-prime-minister-rooftop-drone.


ISSN 2280-6164

del Presidente[61]. Nei primi due casi si è trattato di proteste organizzate da attivisti per vari motivi e non ideate per creare danni a cose o persone, mentre il caso del Venezuela rappresenta verosimilmente un tentativo di attentato ad un leader politico durante il quale sono rimaste ferite nove persone.

Le vulnerabilità dimostrate da siti ed eventi dove la sicurezza dovrebbe essere ai massimi livelli dimostrano l'impellenza delle minacce derivanti dall'impiego di droni duali con finalità terroristiche su larga scala. Benché non si siano ancora registrati eventi di questo tipo nei Paesi occidentali, negli ultimi anni le autorità preposte al contrasto al terrorismo hanno sventato diversi piani che prevedevano l'impiego di UAS[62]. Tra i vari Paesi nei quali queste attività sono state registrate figura anche l'Italia. In provincia di Potenza, un individuo è stato arrestato nel 2018 dalle Forze dell'Ordine perché stava tentando di armare un drone grazie a video dimostrativi reperiti illegalmente online, con l'intento di utilizzarlo poi per un attacco terroristico[63].

La minaccia portata dai droni duali, data la particolarità del mezzo, rende non efficaci alcune delle misure di sicurezza attuate in vari Paesi europei dopo l'ondata di attacchi terroristici verificatasi a partire dal 2014. Si pensi, ad esempio, alle barriere fisse o rimovibili sistemate in prossimità di aree urbane affollate al fine di prevenire l'impiego di autoveicoli per scopi terroristici. Queste barriere verrebbero bypassate grazie all'uso di droni che possono essere fatti schiantare con una carica esplosiva sulla folla o addirittura far sganciare l'ordigno dal drone in volo. Allo stesso modo, qualora l'attacco prevedesse la dispersione di agenti chimici, biologici o radiologici in aree urbane, si assisterebbe ad un numero elevato di vittime dirette e indirette tra la popolazione coinvolta[64]. Indipendentemente dal tipo di attentato portato a compimento, è certo che durante l'attacco effettuato con droni duali si scatenerebbe il panico tra la folla, incrementando notevolmente il numero di vittime indirette[65]. Inoltre, va notato come per creare il panico potrebbe essere sufficiente impiegare sostanze di uso comune o comunque non nocive per la salute. Si pensi, ad esempio, ad un drone che sorvolando una folla rilasci sostanze urticanti o, addirittura, semplice farina. Il panico generato nella folla sottostante

[61] "Venezuela, attentato con droni contro Maduro (illeso) che promette vendetta", in *Il Sole 24 Ore*, 5 agosto 2018, https://www.ilsole24ore.com/art/venezuela-attentato-droni-contro-maduro-illeso-che-promette-vendetta-AEb3qPXF.

[62] Zak Doffman, "Warning Over Terrorist Attacks Using Drones Given by EU Security Chief", in *Forbes*, 4 agosto 2019, https://www.forbes.com/sites/zakdoffman/2019/08/04/europes-security-chief-issues-dire-warning-on-terrorist-threat-from-drones.

[63] "Terrorismo, arrestato macedone di 29 anni a Potenza: si addestrava per attentati", in *Il Messaggero*, 10 luglio 2018, https://www.ilmessaggero.it/primopiano/cronaca/terrorismo_arresto_potenza_macedone-3847576.html.

[64] Per una valutazione dei rischi connessi ad attacchi di questo tipo anche se condotti con quantità molto limitate di materiale tossico si veda: Lawrence M. Wein, David L. Craft, Edward H. Kaplan, "Emergency Response to an Anthrax Attack", in *PNAS*, Vol. 100, No. 7, 1 aprile 2003, p. 4346-4351, https://doi.org/10.1073/pnas.0636861100.

[65] Scott Steward, "When Drones Attack: The Threat Remains Limited", in *Stratford Wordview*, 17 luglio 2018.


ISSN 2280-6164

potrebbe innescare un tentativo di fuga incontrollata che, a sua volta, metterebbe a repentaglio l'incolumità delle persone[66].

Va anche considerato l'impatto psicologico sulla popolazione nel medio-lungo periodo generato da un attacco terroristico che veda il coinvolgimento di droni. La possibilità di impiegare UAS per condurre attentati su larga scala, infatti, darebbe alle organizzazioni, o ai singoli individui che li utilizzassero, la capacità di veicolare una minaccia dal cielo con relativa semplicità, cosa che è stata fino ad ora preclusa. Pertanto, l''utilizzo di droni potrebbe fornire un contributo essenziale nel raggiungimento dello scopo ultimo del terrorismo, ossia quello di creare una sensazione di vulnerabilità diffusa e destabilizzare la società colpita, andando anche ad aumentare le pressioni sulla classe politica[67].

Inoltre, data la grande disponibilità di UAS sul mercato e l'ingente numero di individui che li acquistano quotidianamente, potenziali terroristi potrebbero dotarsi di questi prodotti senza destare il minimo sospetto nelle autorità preposte al loro contrasto, garantendo segretezza nella fase di pianificazione e preparazione dell'attacco. In maniera analoga, le dimensioni dei droni ne permettono la modifica in ambienti di uso comune e senza richiedere strumentazioni particolarmente avanzate. Va anche sottolineato il fatto che i tradizionali sistemi di difesa aerea si sono dimostrati molto più fallibili nell'individuare, tracciare e contrastare velivoli lenti che volano a quote basse (*Low, Small and Slow*, LSS) come gli UAS duali rispetto ad altri mezzi come velivoli convenzionali o missili balistici[68].

I droni duali utilizzati a fini illeciti presentano anche il grande vantaggio di essere flessibili riguardo alle modalità di decollo/lancio. Essendo spesso molto leggeri, essi possono essere fatti decollare senza l'ausilio di piattaforme di lancio particolarmente ingombranti o anche da piattaforme mobili (terrestri o navali), nonché direttamente da terra o da un veicolo. Inoltre, i droni duali hanno un raggio d'azione piuttosto considerevole. Grazie all'elaborazione di segnali GPS, questi prodotti presentano livelli di accuratezza molto elevati nella navigazione e, dunque, nella capacità di raggiungere il punto in cui eventualmente schiantarsi o rilasciare il carico trasportato. Va però notato che il lancio di un drone armato effettuato da qualche km di distanza dal bersaglio non sempre rappresenta la scelta ottimale. Un lancio o decollo in prossimità dell'obiettivo potrebbe esser preferito per ridurre i rischi di interdizione e di contrasto. Infatti, va notato che, qualora gli UAS fossero armati con cariche esplosive o altri materiali dannosi, essi non potrebbero essere abbattuti con mezzi cinetici in prossimità di folle o in centri urbani: con il conseguente schianto al suolo, infatti, ci sarebbe il rischio concreto di esplosione o

[66] Stephen Prior, "What Does the Future Hold for Drones in Security and Defence?", in *Government Europa*, 9 luglio 2018, https://www.governmenteuropa.eu/?p=89325.

[67] Benjamin Seibert, "The Dark Side of Drones: Implications for Terrorism", in *CTX Journal*, Vol. 5, No. 4, novembre 2015, p. 43-54, https://globalecco.org/documents/10180/605826/Vol5No4.pdf.

[68] Xuwang Zhang et al., "Low-Altitude and Slow-Speed Small Target Detection Based on Spectrum Zoom Processing", in *Mathematical Problems in Engineering*, Vol. 2018, Art. 4146212, 10 maggio 2018, https://doi.org/10.1155/2018/4146212.


ISSN 2280-6164

di rilascio di sostanze tossiche che causerebbero danni paragonabili o equivalenti a quelli a cui mirava l'attentatore. Pertanto, in aree urbane o zone densamente affollate i droni malevoli potrebbero essere contrastati solo tramite sistemi non cinetici volti a farlo allontanare dalla zona di rischio e, eventualmente, farlo atterrare in zone di quarantena precedentemente identificate. L'unica alternativa, quella della distruzione totale del drone, richiederebbe l'impiego di armi altamente sofisticate (in particolare quelle ad energia diretta) quasi impossibili da dislocare e impiegare in contesti urbani.

La minaccia rappresentata dai droni duali non interessa solo la sicurezza nazionale ma interessa anche la sicurezza dei contingenti civili e militari impegnati in missioni fuori area e, più in generale, la conduzione e la buona riuscita di tali missioni. In questo contesto, ciò che preoccupa maggiormente è l'impiego di droni da parte di gruppi terroristici e attori non statali che si è registrato in maniera crescente negli ultimi anni. I riferimenti vanno al teatro mediorientale e a quello africano nei quali sono presenti anche contingenti italiani, ma anche al conflitto che interessa la zona orientale dell'Ucraina.

L'impiego di UAS da parte di gruppi terroristici e attori non statali rappresenta una novità relativamente recente sia per quanto riguarda droni militari che, soprattutto, per quelli duali. Per i primi, va notato che Hezbollah ha fatto spesso ricorso a tali tecnologie contro le forze israeliane e, già nel 2011, i ribelli libici si erano dotati di un drone militare dal costo complessivo di circa 90 mila euro da impiegare contro le truppe fedeli a Gheddafi[69]. Al contempo, però, sia queste forze che il sedicente Stato islamico hanno dimostrato di essere in grado di impiegare anche droni duali principalmente per scopi di *Intelligence, Surveillance, Target Acquisition and Reconnaissance* (ISTAR)[70] e in maniera più limitata per colpire fisicamente truppe e assetti rivali[71].

Un primo effetto che l'utilizzo di droni duali da parte di milizie irregolari e entità non statuali potrebbe avere è di tipo propagandistico e psicologico. Tramite la dimostrazione e la strumentalizzazione della capacità di colpire per via aerea le truppe nemiche, questi gruppi potrebbero reclutare nuovi miliziani ed estorcere il supporto della popolazione, anche incutendo il timore di diventare un obiettivo. Un esempio di questo tipo di propaganda è identificabile con il video rilasciato dall'agenzia di stampa Amaq nel quale vengono mostrati droni operati dal sedicente Stato islamico al fine di colpire forze irachene[72]. Benché permangano perplessità

[69] Alexander Harper, "Drones Level the Battlefield for Extremists", in *The Interpreter*, 20 aprile 2018, https://www.lowyinstitute.org/node/346766.

[70] Spencer Ackerman, "Libyan Rebels Are Flying Their Own Minidrone", in *Wired*, 23 settembre 2011, https://www.wired.com/2011/08/libyan-rebels-are-flying-their-own-mini-drone.

[71] Don Rassler, *The Islamic State and Drones: Supply, Scale, and Future Threats*, West Point, Combating Terrorism Center, 11 luglio 2018, https://ctc.usma.edu/islamic-state-drones-supply-scale-future-threats.

[72] Video disponibile in YouTube: Wall Street Journal, *Islamic State Uses Weaponized Drones Against Iraqi Forces*, 24 febbraio 2017, https://youtu.be/Xeqz4XI4Wag.


ISSN 2280-6164

circa l'autenticità del video, la sua valenza a fini di propaganda risulta indubbia. Un ulteriore esempio è rappresentato dai messaggi inviati dai separatisti filo-russi presenti nella regione orientale dell'Ucraina agli smartphone di cittadini residenti in prossimità delle zone di conflitto, per i quali risulta altamente probabile che sia stato usato un drone come mezzo per introdursi nei telefoni e installare malware[73].

In secondo luogo, l'acquisizione di strumenti facilmente accessibili e dai prezzi estremamente contenuti con i quali effettuare operazioni ISTAR riduce lo svantaggio tecnologico di milizie e attori non statali. Benché questi strumenti risultino rudimentali se paragonati a quelli in dotazione alle forze armate regolari, la possibilità di acquisire informazioni sul posizionamento delle truppe avversarie e sui loro spostamenti potrebbe facilitare imboscate e attentati di varia natura oltre a permettere una migliore pianificazione tattica dei gruppi terroristici o delle milizie irregolari[74]. In aggiunta, in maniera più rudimentale e con risultati inferiori, ma tramite modalità simili, i droni potrebbero essere usati per fornire informazioni alle unità di artiglieria impiegate dalle milizie irregolari per ottenere indicazioni *near-real-time* che permettano di aggiustare il tiro, incrementando la precisione[75]. Questa eventualità potrebbe compromettere la sicurezza delle missioni o, comunque, renderle più complesse, esponendo a rischi maggiori il personale civile e militare impiegato.

Per quanto riguarda la conduzione di attacchi cibernetici tramite droni, i rischi nei teatri operativi risultano simili a quelli della sicurezza dei siti sensibili e delle infrastrutture critiche sul territorio nazionale. Infatti, attacchi che compromettano sistemi radar o di comunicazione sia interni alle basi militari che durante pattugliamenti o operazioni di tipo *combat*, potrebbero causare ingenti danni sia in modo diretto che indiretto. Ad esempio, qualora operatori di UAS duali adeguatamente equipaggiati dovessero riuscire a interrompere le comunicazioni tra le diverse unità impegnate in operazioni sul campo, risulterebbe particolarmente complicato riuscire a raggiungere l'obiettivo e si esporrebbero le truppe a rischi particolarmente elevati.

Infine, l'impiego massiccio di droni duali armati aumenterebbe i già elevati rischi per il personale dispiegato derivanti dalle tecniche di guerriglia in uso in molteplici teatri operativi. Questa minaccia va ad aggiungersi a quelle già esistenti con marcata connotazione asimmetrica quali l'impiego di dispositivi esplosivi

[73] Raphael Satter, Dmytro Vlaslov, "Ukraine Soldiers Bombarded by 'Pinpoint Propaganda' Texts", in *AP News*, 12 maggio 2017, https://apnews.com/9a564a5f64e847d1a50938035ea64b8f.

[74] Larry Friese, N.R. Jenzen-Jones,Michael Smallwood, "Emerging Unmanned Threats: The Use of Commercially-available UAVs by Armed Non-state Actors", in *ARES Special Reports*, No. 2, febbraio 2016, p. 10; 50, http://armamentresearch.com/wp-content/uploads/2016/02/ARES-Special-Report-No.-2-Emerging-Unmanned-Threats.pdf.

[75] Jonathan Ferguson, N.R. Jenzen-Jones, "Raising Red Flags: An Examination of Arms & Munitions in the Ongoing Conflict in Ukraine", in *ARES Research Reports*, No. 3, aprile 2014, http://armamentresearch.com/Uploads/Research%20Report%20No.%203%20-%20Raising%20Red%20Flags.pdf.


ISSN 2280-6164

ISSN 2280-6164



improvvisati (*Improvised Explosive Devices*, IED) o la conduzione di attacchi suicidi tramite veicoli caricati con materiale esplosivo. Qualora non adeguatamente protette, anche le basi militari e i compound, nonché i convogli in movimento, potrebbero divenire obiettivi vulnerabili tramite UAS armati con materiali esplosivi o agenti CBRN, eventualità che causerebbe un numero ingente di vittime. Le tradizionali protezioni fisiche come recinzioni o *check-point* risulterebbero non efficaci di fronte ad una minaccia che fino a poco tempo fa non si pensava di dover fronteggiare.

Proprio per le caratteristiche di questa minaccia, anche i sistemi anti-aerei posti a protezione delle basi militari risultano meno performanti nell'individuare e neutralizzare velivoli LLS, o non sono costo-efficienti. Infatti, i sistemi di difesa aerea che impiegano munizioni *surface-to-air* sono progettati per colpire target di tipo diverso e dal valore ben maggiore dei droni duali. Ferma restando la necessità di utilizzare tali sistemi di contrasto qualora fosse veicolata tramite UAS una minaccia a obiettivi di particolare interesse strategico, si riscontra una profonda asimmetria in termini di costi tra i vettori della minaccia e i sistemi eventualmente impiegabili per contrastarla[76].

A differenza di quanto accade per i contesti urbani, nei teatri operativi è possibile abbattere il drone con armi convenzionali in quanto le aree esposte al rischio di esplosioni o rilascio di agenti nocivi successivi allo schianto al suolo potrebbero essere molto meno affollate e sottoponibili a quarantena in tempi rapidi. Tuttavia, risulta necessario effettuare l'individuazione e tracciamento del drone in maniera repentina per evitare l'intromissione in aree nelle quali l'abbattimento fisico non sarebbe più possibile. Occorre pertanto che anche in tali contesti ci si doti di strumenti *ad hoc* per contrastare questo tipo di minaccia.

Sia le minacce presentate per la sicurezza nazionale che per i contingenti dispiegati all'estero possono essere amplificate in maniera considerevole dall'eventuale impiego di sciami di droni (*swarm*), ossia gruppi di UAS che agiscono in maniera autonoma e congiunta fino al raggiungimento dell'obiettivo indicato dall'operatore. Il recente attacco all'impianto petrolifero della compagnia di idrocarburi saudita Aramco[77] ha evidenziato il potenziale di attacchi di questo tipo ma, ad oggi, l'impiego di sciami risulta difficile per singoli terroristi o organizzazioni mediamente strutturate in assenza di appoggio da parte di entità statali. Queste difficoltà derivano dallo stadio non particolarmente avanzato di questa capacità nei droni disponibili in commercio e dalla complessità della produzione di software che permetta tali utilizzi[78]. Tuttavia, molteplici progetti volti a sviluppare

[76] André Haider, "A Comprehensive Approach to Countering Unmanned Aircraft Systems", in *JAPCC Flyers*, agosto 2019, https://www.japcc.org/portfolio/a-comprehensive-approach-to-countering-unmanned-aircraft-systems.

[77] Associated Press, "Major Saudi Arabia Oil Facilities Hit by Houthi Drone Strikes", in *The Guardian*, 14 settembre 2019, https://gu.com/p/cb793.

[78] Robert J. Bunker, *Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications*, Carlisle, Strategic Studies Institute-U.S. Army War College Press, agosto 2015, p. x,

ulteriormente questa capacità sono già stati avviati da governi nazionali di vari Paesi in sinergia con il mondo della ricerca e alcune industrie[79], facendo pensare a una possibile rapida accelerazione nella sua implementazione anche su droni commerciali.

### *1.2 L'evoluzione tecnologica*

Il grande interesse suscitato dai benefici in termini qualitativi e di costo-efficienza ottenibili dall'impiego di droni duali sia a scopi governativi, che commerciali e ricreativi ha favorito un rapido e sostanziale sviluppo tecnologico di questi prodotti. Di conseguenza, anche le loro caratteristiche tecniche sono migliorate considerevolmente nel corso degli ultimi anni.

Per quanto concerne i droni particolarmente sofisticati e costosi impiegati per svariate attività dai governi, il divario tecnologico con gli UAS ad uso militare si è assottigliato in maniera netta. Ciò è stato possibile grazie alla creazione di importanti sinergie tra le industrie operanti nel campo della difesa in vari Paesi ed enti governativi, che hanno portato le tecnologie militari e civili a svilupparsi in parallelo[80]. Sebbene i droni duali impiegati oggi dai governi nazionali presentino un livello tecnologico particolarmente avanzato che ne ha amplificato le possibilità d'impiego e garantiscono risultati più elevati di quanto avvenisse in passato, anche i droni commerciali hanno sperimentato un forte avanzamento tecnologico.

L'evoluzione tecnologica dei droni duali si è verificata principalmente per due ordini di ragioni. Innanzitutto, in seguito alla costante espansione della domanda di droni, le imprese produttrici hanno impiegato ingenti risorse nello sviluppo tecnologico dei loro prodotti al fine di rendersi sempre più competitive sul mercato. Tali risorse sono state reperite tramite investimenti pubblici e privati destinati anche a piccole e medie imprese (PMI) e start-up impegnate nel proporre innovazioni per tutte le componenti hardware e software degli UAS. Nel periodo compreso tra il 2012 e il 2019, i finanziamenti da investimenti privati alle compagnie coinvolte nel mercato mondiale dei droni duali sono ammontati a più di 2,3 miliardi di euro[81]. Inoltre, in virtù del potenziale innovativo rappresentato dal settore degli UAS, anche molteplici enti pubblici hanno deciso di effettuare investimenti considerevoli. Tra i finanziatori pubblici è compresa l'Unione europea

https://www.hsdl.org/?view&did=786817.

79 Stav Dimitropoulos, "If One Drone Isn't Enough, Try a Drone Swarm", in *BBC News*, 6 agosto 2019, https://www.bbc.com/news/business-49177704; si veda, inoltre, il progetto cinese recentemente lanciato e che ambisce a creare sciami di droni da 1.000 componenti: Scott N. Romaniuk, Tobias Burgers, "China's Swarms of Smart Drones Have Enormous Military Potential", in *The Diplomat*, 3 febbraio 2018, https://thediplomat.com/2018/02/chinas-swarms-of-smart-drones-have-enormous-military-potential.

80 Vicki Speed, "Building on Benchmarks", in *Inside Unmanned Systems*, 10 luglio 2019, https://insideunmannedsystems.com/?p=25342.

81 Philip Finnegan, "VC Funding for Drones Surges in 2019, with More Focused Bets", in *Forbes*, 22 luglio 2019, https://www.forbes.com/sites/philipfinnegan/2019/07/22/vc-funding-for-drones-surges-in-2019-with-more-focused-bets.


ISSN 2280-6164

(UE) che, tramite il Programma Horizon 2020, ha finanziato tre progetti di ricerca e innovazione nel campo dei droni duali condotti da compagnie operanti in Europa (33 milioni di euro dal 2018 al 2020[82]) e ha istituito una piattaforma consultiva per gli investimenti sui droni in ambito europeo[83]. Grazie ai vari investimenti effettuati e alla volontà delle industrie produttrici di controllare porzioni sempre più grandi di mercato, gli UAS hanno beneficiato di migliorie tecniche per quanto riguarda tutte le loro caratteristiche e componenti aggiuntive. Da notare come all'avanzamento tecnologico non sia seguito un aumento dei prezzi dei droni, ma piuttosto si sia verificata una diminuzione degli stessi, a fronte di una domanda elevata e di una forte competitività di mercato.

In secondo luogo, l'evoluzione tecnologica dei droni duali è stata favorita dalla necessità di rispettare i parametri relativi alla loro presenza nello spazio aereo civile fissati da autorità nazionali e sovranazionali. Infatti, un numero sempre crescente di Paesi si è dotato di regolamenti, più o meno rigidi, che regolano l'utilizzo dei droni a finalità commerciali o ricreative[84]. La Commissione europea ha emanato nel maggio 2019 il Regolamento di esecuzione 2019/947 relativo a norme e procedure per l'esercizio di aeromobili senza equipaggio, il quale entrerà pienamente in vigore in tutti i Paesi membri nel luglio 2020 sostituendo i regolamenti nazionali preesistenti[85]. Tra le principali restrizioni presenti nei regolamenti emanati sia dall'UE che dai vari governi degli Stati membri vi è l'impossibilità, per droni operati da singoli operatori, di sorvolare aree affollate o di volare a distanze che vadano oltre la linea visiva dell'operatore (*Beyond Visual Line of Sight*, BVLOS), rendendo il loro impiego possibile solo in determinate aree prestabilite[86], anche se operazioni BVLOS potrebbero essere presto consentite.

Questa limitazione è stata adottata per ridurre le minacce alla *safety* di cittadini, proprietà private e aviazione civile, inducendo le imprese produttrici a sviluppare tecnologie in grado di garantire gli elevati standard di sicurezza previsti dalle normative vigenti.

Indipendentemente dalle ragioni che hanno favorito lo sviluppo tecnologico, si nota come questo sia stato guidato principalmente da tre trend: la miniaturizzazione

[82] Commissione europea, *Horizon 2020 Work Programme 2018-2020. Smart, Green and Integrated Transport*, luglio 2019, http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-transport_en.pdf.

[83] Commissione europea, *European Commission and European Investment Bank Announce Launch of "European Drone Investment - Advisory Platform"*, cit.

[84] Therese Jones, *International Commercial Drones Regulation and Drone Delivery Services*, Santa Monica, RAND, 2017, https://doi.org/10.7249/RR1718.3.

[85] Commissione europea, *Regolamento di esecuzione (UE) 2019/947 del 24 maggio 2019 relativo a norme e procedure per l'esercizio di aeromobili senza equipaggio*, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32019R0947. Per maggiori informazioni si veda il paragrafo 2.1 del presente studio.

[86] Claudia Stöcker et al., "Review of the Current State of UAV Regulations", in *Remote Sensing*, Vol. 9, No. 5, Art. 459, 9 maggio 2017, https://doi.org/10.3390/rs9050459. Specifici dettami del Regolamento europeo saranno analizzati nel dettaglio nel capitolo 2 del presente studio.


ISSN 2280-6164

dei componenti, l'aumento dell'autonomia del drone rispetto all'operatore e la possibilità di agire in sciami[87]. Questi trend evolutivi hanno contribuito ad aumentare notevolmente le possibilità d'impiego di droni duali per scopi civili, sia commerciali che ricreativi. Di pari passo, gli avanzamenti tecnologici aprono però anche alla possibilità di nuovi utilizzi illeciti da parte di operatori sofisticati e non, amplificando considerevolmente la minaccia ibrida rappresentata dai droni duali sia in ottica di sicurezza nazionale che per quanto concerne i contingenti impiegati in missioni all'estero.

La miniaturizzazione delle componenti hardware dei droni duali e la possibilità di impiegare nano-materiali[88] nella loro fabbricazione possono essere considerati come i fattori che hanno permesso le evoluzioni tecnologiche successive[89]. Infatti, il comparto degli UAS duali pensati per scopi civili aveva sempre incontrato un limite oggettivo legato alle dimensioni dei componenti, in quanto quelli tecnologicamente più avanzati risultavano troppo grandi e pesanti per essere montati su UAV dal peso di pochi kg e di dimensioni estremamente ridotte. Inoltre, la loro eventuale inclusione tra i componenti di micro o mini droni ne avrebbe impedito il decollo o limitato enormemente le performance in termini di velocità, durata delle batterie e capacità di trasportare *payload* aggiuntivi. Tuttavia, gli sviluppi tecnologici che hanno avuto ripercussioni su peso, dimensioni e potenza (*Size, Weight and Power*, SWaP) di vari componenti, ne hanno permesso l'implementazione anche su mini e micro droni[90], come è il caso dei sistemi INS e sistemi VIO.

Uno dei componenti che ha goduto dei maggiori miglioramenti è sicuramente rappresentato dalle batterie. Le loro dimensioni sono state ridotte aprendo anche alla possibilità di dotare il drone di due o più batterie aumentandone le potenzialità[91]. Alla riduzione esponenziale di peso e dimensioni delle tradizionali batterie si è correlata anche una maggiore diversificazione nella tipologia di materiali impiegabili nella loro costruzione come, ad esempio, le batterie al litio. La maggiore densità energetica che contraddistingue questo tipo di batterie garantisce una durata maggiore del tempo di volo del drone[92]. Inoltre, queste batterie permettono di fornire ai vari componenti del drone livelli di potenza

[87] Michel Busch, "Unmanned Aerial System Miniaturization", cit.

[88] T.X. Hammes, "Technologies Converge and Power Diffuses: The Evolution of Small, Smart, and Cheap Weapons", in *Cato Institute Policy Analysis*, No. 786, 27 gennaio 2016, https://www.cato.org/node/62520.

[89] Michel Busch, "Unmanned Aerial System Miniaturization", cit.

[90] Rory Jackson, "Small Is Beautiful: Nano Drone Tech Is Advancing", in *Defence IQ*, 20 luglio 2017, https://www.defenceiq.com/defence-technology/articles/nano-drone-tech-is-advancing.

[91] C. Bennet, "Learn, How to Add a Second Battery to Drone for Extended Flight Time", in *BestDroneUnderHalfaPound*, 1 luglio 2018, https://bestdroneunderhalfapound.com/learn-how-to-add-a-second-battery-to-drone-for-extended-flight-time.

[92] Si vedano: Joe Pappalardo, "New Lithium Metal Batteries Can Power Drones for Longer (and It Could Change Everything)", in *Popular Mechanics*, 16 aprile 2019, https://www.popularmechanics.com/flight/drones/a27155551; Katie Fehrenbaher, "A New Lithium-Metal Battery Takes Flight in Drones", in *Greentech Media*, 29 gennaio 2018, https://www.greentechmedia.com/articles/read/a-new-lithium-metal-battery-takes-flight-in-drones.


ISSN 2280-6164

elettrica più elevati, consentendo l'utilizzo di motori più potenti[93] e di sensori con consumi più elevati.

Grazie alla miniaturizzazione di alcuni elementi come, ad esempio, i condensatori, questi motori hanno iniziato a essere implementabili anche su micro e mini droni[94]. Dalla motoristica del drone dipende la sua capacità di decollare anche in presenza di *payload* aggiuntivi e di compiere operazioni di volo con determinate caratteristiche[95]. Pertanto, ad un incremento delle performance del motore corrisponde un incremento in termini di velocità massima a cui il drone può viaggiare e di durata del tempo di volo[96].

L'avanzamento tecnologico di queste ultime caratteristiche è stato favorito anche dalla possibilità di utilizzare materiali compositi come polimeri rinforzati in fibra di carbonio per la creazione dei telai degli UAS. L'impiego di questi materiali ha permesso una riduzione considerevole del peso complessivo dei droni senza inficiarne la capacità di trasportare *payload*. Infatti, i materiali utilizzati per la fabbricazione di UAV sono connotati da elevati livelli di proprietà chimico-fisiche e meccaniche come la resistenza meccanica, ossia la capacità del materiale di sopportare forti sollecitazioni come, ad esempio, un carico aggiuntivo. Si è, quindi, ridotto il peso dell'UAV favorendo l'incremento della velocità massima dei droni e del tempo di volo e si è garantita la possibilità di trasportare *payload* superiori rispetto a quanto avvenisse prima dell'avvento dei materiali compositi[97].

Un'ulteriore innovazione tecnologica è rappresentata dalla possibilità di ricorrere con sempre maggiore frequenza e semplicità alle tecnologie di stampa tridimensionale (3D o *additive manufacturing*). Questa tecnologia è oggi utilizzata per la fabbricazione di alcuni componenti hardware degli UAS. Tra i componenti più spesso prodotti tramite stampa 3D si annoverano i telai, le eliche, i supporti sui quali vengono montate telecamere o altri *payload*, le antenne che permettono la comunicazione con l'operatore e altri elementi metallici che fanno da protezione per il drone in caso di urto.

L'*additive manufacturing* presenta numerosi vantaggi sia per i produttori di droni che per gli utilizzatori. Infatti, tramite la stampa 3D, le caratteristiche dei

[93] Boris Galkin, Luiz A. DaSilva, *UAVs as Mobile Infrastructure: Addressing Battery Lifetime*, eprint arXiv:1807.00996, 3 luglio 2018, https://arxiv.org/abs/1807.00996.

[94] GetFPV, *All About Multirotor Drone FPV Electronic Speed Controllers*, 2 febbraio 2018, https://www.getfpv.com/learn/?p=145.

[95] Fintan Corrigan, "How a Quadcopter Works with Propellers and Motors Explained", in *DroneZon*, 4 ottobre 2019, https://www.dronezon.com/learn-about-drones-quadcopters/how-a-quadcopter-works-with-propellers-and-motors-direction-design-explained.

[96] GetFPV, *All About Multirotor Drone FPV Electronic Speed Controllers*, cit.

[97] Si vedano: Michael Legault, "Drones: Composite UAVs Take Flight", in *CompositesWorld*, 1 luglio 2018, https://www.compositesworld.com/articles/drones-composite-uavs-take-flight; Andres Gameros, "The Use of Composite Materials in Unmanned Aerial Vehicles (UAVs)", in *AZO Materials*, 6 agosto 2015, https://www.azom.com/article.aspx?ArticleID=12234.

ISSN 2280-6164

materiali compositi possono essere sfruttate appieno e ulteriormente migliorate, facendo ridurre il peso degli UAS, ma aumentandone le caratteristiche fisiche e tecnologiche[98]. Inoltre, l'*additive manufacturing* permette ai singoli utilizzatori di personalizzare il proprio drone tramite la creazione di componenti progettate *ad hoc*[99], incrementando anche le possibilità di riuscita di atti illeciti che gli operatori sofisticati vogliano effettuare. Si pensi ad un attacco terroristico tramite lo sgancio di materiale esplosivo da un drone su un determinato obiettivo. In mancanza di congrue soluzioni reperibili sul mercato, sarebbe possibile fabbricare, anche tramite stampa 3D, l'apposito sistema meccanico necessario a trasportare e poi rilasciare il materiale esplosivo. La carica esplosiva potrebbe essere innescata tramite comando diretto dell'operatore o automaticamente in corrispondenza di coordinate GPS preimpostate.

Questa possibilità, insieme alle altre migliorie descritte, contribuiscono a rendere la minaccia dei droni duali sempre più credibile e difficile da contrastare. La possibilità di rilevare, identificare, e tracciare il drone il più lontano possibile dall'obiettivo sensibile (*early warning*) risulta, quindi, un fattore chiave nel contrasto ai droni ostili. La rilevazione tempestiva può permettere all'operatore di pubblica sicurezza o delle forze armate di prendere decisioni ponderate e mettere in campo gli strumenti più adeguati per allontanare o eliminare la minaccia prima che il velivolo raggiunga o si porti nelle immediate vicinanze dell'obiettivo che si vuole proteggere[100]. L'incremento della velocità degli UAS riduce i tempi che intercorrono tra il momento di un cui il drone entra nel raggio di copertura dei sistemi preposti alla *detection* e quello in cui vengono raggiunte le immediate vicinanze dell'obiettivo sensibile. Pertanto, le potenziali tecniche di contrasto risultano limitate soprattutto in centri urbani dove l'abbattimento con mezzi cinetici non sarebbe possibile se non in aree precedentemente perimetrate e poste in quarantena. Inoltre, l'aumento del *payload* trasportabile apre a nuove possibilità per quanto riguarda il trasporto di esplosivi o materiali CBRN, andando a incrementare il potenziale impatto che un attacco terroristico potrebbe avere. Di pari passo, l'incremento della durata del tempo di volo, anche in presenza di *payload*, garantisce al potenziale operatore malevolo di poter effettuare il decollo da posizioni che non devono trovarsi nelle strette vicinanze dell'obiettivo prefissato, aumentando la flessibilità di tali operazioni.

Anche i componenti necessari a migliorare le caratteristiche tecniche degli UAS in termini di stabilità durante le operazioni di volo, semplicità di utilizzo e, soprattutto, autonomia rispetto all'operatore sono stati oggetto di consistenti avanzamenti tecnologici resi possibili dal processo di miniaturizzazione. In particolare, negli

[98] Zaman Khan, "Ultra-Light and Strong Drones Possible through New 3D Printing Innovation", in *Khalifa University-Exploration*, 26 febbraio 2019, https://www.ku.ac.ae/?p=20304.

[99] Manya Jha, "How 3D Printing is making Drones Affordable and Accessible", in *Entrepreneur*, 14 aprile 2017, https://www.entrepreneur.com/article/292815.

[100] Linda Ziemba, "Observe and Report: Considerations for Evaluating Drone Detection Systems", in *SIA Technology Insights*, 6 settembre 2019, https://wp.me/p9rsz1-3gR.

DOCUMENTI IAI 20 | 04 - MARZO 2020 ISSN 2280-6164

ultimi anni si è assistito allo sviluppo di *Micro Electro-Mechanical Systems* (MEMS), ossia processori, sensori e altre apparecchiature tecnologicamente avanzate che si presentano in dimensioni particolarmente ridotte, spesso nell'ordine di pochi millimetri e dal peso di pochi grammi[101]. Grazie a queste tecnologie, è stato possibile dotare anche i mini e micro droni di elevate capacità computazionali, garantendo l'elaborazione di dati in *real time* e di supportare l'istallazione di software sempre più complessi e performanti. Queste tipologie di componenti sono ad oggi presenti nelle configurazioni di fabbrica dei droni duali disponibili in commercio o possono essere acquistate separatamente e poi istallate sul drone[102].

L'introduzione di componenti MEMS risulta fondamentale nel garantire la stabilità delle operazioni di volo degli UAS principalmente perché permettono di minimizzare gli errori derivanti da calibrazioni non accurate della motoristica, dinamiche di sistema alterate dal trasporto di *payload* o condizioni geografiche e atmosferiche avverse[103]. Sensori inerziali MEMS, come le *Inertial Measurement Units* (IMU) che incorporano accelerometri, giroscopi e sistemi elettronici[104], possono fornire dati fondamentali per il corretto funzionamento di sistemi di navigazione inerziali in grado di calcolare in tempo reale la posizione del drone, la direzione verso la quale si sta muovendo e la sua velocità[105]. Questi dati possono poi essere utilizzati per complementare le informazioni acquisite tramite segnali GPS e la loro conseguente elaborazione effettuata da appositi dispositivi installati sul drone[106]. Grazie all'impiego congiunto di questa sensoristica, è possibile far seguire al drone una rotta preimpostata basata su punti chiave (*waypoint*) identificati da coordinate GPS, garantendo l'autonomia del drone rispetto all'operatore nelle fasi successive al decollo. Infatti, il ruolo dell'operatore può limitarsi all'elaborazione di un piano di volo che includa le coordinate dei punti chiave attraverso i quali il drone deve transitare, la velocità da seguire e l'altitudine da tenere nei vari passaggi, con questi ultimi due dati che possono essere calcolati dagli INS in tempo reale[107].

[101] Sergej Scheiermann, "MEMS Sensors Are the Heart of a Drone", in *FierceElectronics*, 3 gennaio 2019, https://www.fierceelectronics.com/node/163656.

[102] Si veda, ad esempio, il sito di BoschSensortec: *Sensing Solutions for Drones*, https://www.bosch-sensortec.com/applications-solutions/drones.

[103] HQEW, *The Impact of MEMS Sensors on Drones*, 7 agosto 2019, http://www.hqew.net/news/news-37821.

[104] Fintan Corrigan, "Drone Gyro Stabilization, IMU and Flight Controllers Explained", in *DroneZon*, 2 luglio 2019, https://www.dronezon.com/learn-about-drones-quadcopters/three-and-six-axis-gyro-stabilized-drones.

[105] Si vedano: "Honeywell Expands Navigation Offerings", in *Intelligent Aerospace*, 19 settembre 2019, https://www.intelligent-aerospace.com/unmanned/article/14040282; e il sito di VectorNav Technologies: *Inertial Measurement Units and Inertial Navigation*, https://www.vectornav.com/support/library/imu-and-ins.

[106] Sito di TerrisGPS: *Using UAV GPS*, http://www.terrisgps.com/how-is-gps-used-in-uav.

[107] Fintan Corrigan, "Drone Waypoint GPS Navigation Technology and Uses Explained", in *DroneZon*, 24 marzo 2019, https://www.dronezon.com/learn-about-drones-quadcopters/drone-waypoint-gps-navigation-technology-explained.


ISSN 2280-6164

Il volo autonomo degli UAS può anche essere svincolato dai segnali GPS tramite l'introduzione di sensori VIO. Questa tipologia di sensori permette l'elaborazione di immagini acquisite da videocamere installate sul drone e la loro correlazione con mappe 3D precaricate. L'integrazione dei sensori VIO con rotte preimpostate che indicano i *waypoint* aumenta ancora di più l'autonomia del piano di volo del drone dall'operatore. L'intero processo risulta ad oggi piuttosto semplice grazie alla disponibilità di numerose applicazioni scaricabili gratuitamente da internet, le quali possono essere istallate sui droni duali reperibili in commercio[108]. La possibilità di effettuare operazioni di volo tramite l'acquisizione di immagini è stata facilitata anche dalla presenza di videocamere dalle elevate caratteristiche tecniche che si trovano sui droni *off-the-shelf*. Esse garantiscono immagini in alta risoluzione (4K)[109], indipendentemente dalle condizioni atmosferiche e dalle oscillazioni provocate dal volo del drone[110].

Per far volare il più autonomamente possibile un UAS tramite l'integrazione di coordinate GPS preimpostate e sensori INS, piuttosto che tramite l'acquisizione ed elaborazione di immagini in tempo reale, servono software particolarmente complessi e in grado di poter contare su metodi di intelligenza artificiale (*Artificial Intelligence*, AI). Grazie alle potenzialità di questi processori, i droni possono elaborare enormi quantità di dati tramite tecniche di *machine learning* e *deep learning* e garantire la trasmissione e gestione dei dati in tempo reale. Ciò è reso possibile grazie al lavoro simultaneo e coordinato di tutti gli apparati, che sono anche in grado di elaborare risposte, durante le operazioni di volo, a situazioni non previste[111]. Tra queste ultime, risulta di primaria importanza la capacità dei droni di individuare potenziali ostacoli sulla loro rotta e di superarli in maniera autonoma tramite sistemi di *detection and avoid* (DAA). La necessità di dotare i droni di tali capacità deriva anche dalla volontà delle case produttrici di rispettare i criteri relativi all'inclusione dei droni commerciali nello spazio aereo civile, i quali richiedono elevati standard di sicurezza soprattutto nelle operazioni di volo autonomo[112]. Pertanto, sono stati sviluppati appositi software che, tramite metodi di *Computer Vision*, rendono la navigazione autonoma più efficace e sicura[113].

[108] Si veda, ad esempio, Drones Made Easy Support Center, *Map Pilot for DJI – Introduction*, 5 maggio 2019, https://support.dronesmadeeasy.com/hc/en-us/articles/206018633.

[109] Adam Juniper, "The 10 Best Camera Drones in 2020: These Are the Best Drones for Photography", in *Digital Camera World*, 15 gennaio 2020, https://www.digitalcameraworld.com/buying-guides/the-10-best-camera-drones.

[110] Marck LaFay, "How to Stabilize Your Drone Camera with a Gimbal", in *Dummies*, 26 marzo 2016, https://www.dummies.com/?p=142443.

[111] Lukas Schroth, "Drones and Artificial Intelligence", in *Drone Industry Insights*, 28 agosto 2018, https://wp.me/p7bVQh-oHA.

[112] SESAR Joint Undertaking, *European ATM Master Plan: Roadmap for the Safe Integration of Drones Into All Classes of Airspace*, 19 marzo 2018, https://www.sesarju.eu/node/2993.

[113] Si vedano: Gaurav Kaila, "How to Easily Do Object Detection on Drone Imagery Using Deep Learning", in *Medium*, 6 giugno 2018, https://link.medium.com/gtrECBmtO3; Fintan Corrigan, "12 Top Collision Avoidance Drones and Obstacle Detection Explained", in *DroneZon*, 28 ottobre 2019, https://www.dronezon.com/learn-about-drones-quadcopters/top-drones-with-obstacle-detection-collision-avoidance-sensors-explained.


ISSN 2280-6164

Gli avanzamenti tecnologici registrati nelle capacità di volo autonomo sono ovviamente stati pensati e implementati per facilitarne l'impiego a scopi civili e, grazie al livello tecnologico raggiunto, questi UAS possono essere ad oggi utilizzati per molteplici attività[114]. Tuttavia, esse pongono nuove sfide per quanto riguarda le tecniche di contrasto ai droni duali. In primo luogo, va notato come l'autonomia dei droni aumenti la segretezza dell'operazione e favorisca il mantenimento dell'anonimato dell'operatore, rendendo quindi l'impiego di questi prodotti per finalità illecite ancor più vantaggioso dal punto di vista di un potenziale operatore malintenzionato. Inoltre, la possibilità di pianificare una missione di volo nelle fasi precedenti al decollo esclude il contatto tra il drone e l'operatore, via radiofrequenze o connessioni Wi-Fi, impedendo la *detection* del velivolo basata su sensori che monitorino le frequenze standardizzate sulle quali avvengono tali comunicazioni. Allo stesso modo, anche le tecniche di *interdiction* basate sul disturbo delle comunicazioni tra drone e operatore risultano meno efficaci. Nel caso in cui le operazioni di volo autonome si basino su componenti VIO e quindi non prevedano l'elaborazione di dati GPS, anche l'inibizione di questo tipo di segnali non sarebbe in grado di impedire al drone il compimento della sua missione attivando le funzioni di *freeze*, *fail safe* o *return home*. Tutto ciò riduce ulteriormente le possibilità d'ingaggio in ambito urbano e, indipendentemente dalla maggiore libertà d'impiego di mezzi cinetici, riduce le possibilità di contrasto anche nei teatri operativi per via delle difficoltà di rilevare e tracciare il drone. Infine, con particolare riferimento ai teatri operativi, le specifiche tecniche delle nuove videocamere installate sui droni permettono ai loro utilizzatori di avvalersi di dati qualitativamente migliori per le funzioni ISTAR descritte nel paragrafo precedente.

Il terzo trend di evoluzione tecnologica è quello che ha interessato la capacità dei droni di agire in sciami. Il termine sciami si riferisce a gruppi di UAS guidati da AI e capaci di comunicare tra loro durante le operazioni di volo, caratteristiche che li rendono in grado di rispondere autonomamente a eventuali cambiamenti che dovessero presentarsi nell'ambiente circostante[115]. Proprio il ruolo dell'AI e dell'autonomia degli UAV che volano in maniera cooperativa differenziano gli *swarm* da gruppi di droni che agiscono in maniera coordinata. A differenza degli sciami cooperativi, quelli che operano in modo coordinato non scambiano informazioni tra loro ma si attengono al piano di volo assegnato ad ognuno dei singoli droni che compongono lo sciame[116].

Gli sciami possono anche essere classificati a seconda del loro livello di autonomia rispetto all'operatore e all'interdipendenza di ogni drone che compone lo sciame

[114] Sam Daley, "Fighting Fires and Saving Elephants: How 12 Companies Are Using the AI Drone to Solve Big Problems", in *Built In*, 22 ottobre 2019, https://builtin.com/artificial-intelligence/drones-ai-companies.

[115] Iván Maza et al., "Multi-UAV Cooperation", in *Encyclopedia of Aerospace Engineering*, Chichester/Hoboken, Wiley, 2015, https://personal.us.es/imaza/papers/book_chapters/maza_eae15/maza_eae15_web.pdf.

[116] Tim Wright, "When Is a Drone Swarm Not a Swarm?", in *Air & Space Magazine*, 12 gennaio 2018, https://www.airspacemag.com/daily-planet/when-drone-swarm-not-swarm-180967820.


ISSN 2280-6164

rispetto agli altri. In particolare, si parla di sciami autonomi nel caso in cui le loro operazioni di volo successive al decollo non dipendano in alcun modo da un operatore, o semi-autonomi qualora il ruolo dell'operatore, seppur limitato, sia presente durante volo[117]. Nel primo caso, gli *swarm* vengono lanciati con una missione di volo preconfigurata e, una volta in volo, acquisiscono ed elaborano informazioni dall'ambiente circostante per poi farle circolare all'interno dello sciame al fine di raggiungere l'obiettivo in modo cooperativo[118]. Nel secondo, invece, i droni che compongono lo sciame sono in grado di elaborare e reagire in maniera cooperativa ai comandi ricevuti dall'operatore, e l'interfaccia autonoma con l'ambiente circostante si presenta in maniera leggermente ridotta[119].

Un'altra possibile classificazione riguarda il livello di autonomia che lo sciame può raggiungere nello scambio di informazioni tra i vari UAS che lo compongono. Gli *swarm* che presentano un livello di autonomia pressoché totale tra i singoli componenti vengono definiti *single-layered* e, grazie all'AI, sono in grado di prendere decisioni in autonomia al fine di svolgere la missione in maniera cooperativa, scambiando comunque informazioni con gli altri velivoli. Si parla invece di *multi-layered swarm* quando gli sciami sono divisi in sottogruppi ognuno dotato di un "leader" che guida l'operazione, mentre i membri del sottogruppo seguono i comandi del drone "leader"[120]. Negli sciami *single-layered* ogni drone può avere un obiettivo finale diverso, ma possono essere coordinati tramite AI per quanto riguarda i fattori spazio-temporali. Negli sciami di tipo *multi-layered* è invece il drone "leader" che determina la posizione degli altri droni, i quali solitamente calcolano le proprie azioni e traiettorie in relazione a quelle del "leader". Ciononostante, anche in questi ultimi tipi di sciami, tutti i droni possono avere obiettivi finali diversi, ma a determinare la coordinazione spazio-temporale è il drone "leader" tramite lo scambio di informazioni con gli altri UAV[121].

Un aspetto essenziale da tenere in considerazione quando si parla di sciami cooperativi è rappresentato dalla connettività, intesa come la capacità dei singoli droni di comunicare con l'operatore (in caso di sciami semi-autonomi) o tra i singoli droni che lo compongono (in caso di sciami autonomi). Indipendentemente dalla presenza o meno di un drone "leader", infatti, questi velivoli devono essere in grado di scambiare informazioni tra loro in maniera sicura, affidabile ed efficace[122].

[117] Anam Tahir et al., "Swarms of Unmanned Aerial Vehicles – A Survey", in *Journal of Industrial Information Integration*, Vol. 16, Art. 100106, dicembre 2019, https://www.sciencedirect.com/science/article/pii/S2452414X18300086.

[118] Embetion, *Drone Swarm Performance and Applications*, 28 giugno 2019, https://www.embention.com/news/drone-swarm-performance-and-applications.

[119] Stav Dimitropoulos, "If One Drone Isn't Enough, Try a Drone Swarm", cit.

[120] Anam Tahir et al., "Swarms of Unmanned Aerial Vehicles – A Survey", cit.

[121] Mehmet Cagri Kose, "Monarchy in the Swarm, Drone Swarm with Predetermined Leader", in *Medium*, 3 giugno 2019, https://link.medium.com/al4gXZcvO3.

[122] Bin Li, Zesong Fei, Yan Zhang, "UAV Communications for 5G and Beyond: Recent Advances and Future Trends", in *IEEE Internet of Things Journal*, Vol. 6, No. 2, aprile 2019, p. 2241-2263, https://arxiv.org/abs/1901.06637.


ISSN 2280-6164

Finora le comunicazioni sono avvenute su radiofrequenze o tramite connessioni Wi-Fi che per loro natura presentano un raggio piuttosto ridotto, limitando quindi la distanza massima tra l'operatore e gli sciami o tra i singoli UAV che li compongono. Lo sviluppo del 5G potrebbe permettere di abbattere le barriere rappresentate dai raggi massimi di copertura delle tecnologie utilizzate, dando agli sciami la possibilità di distribuirsi su aree molto più ampie rispetto a quanto non venga fatto oggi, mantenendo però elevati livelli di connettività. In presenza di tali tecnologie, lo scambio di informazioni tra i singoli UAV di uno sciame cooperativo potrebbe avvenire in tempo reale anche a distanze chilometriche[123].

I possibili sviluppi degli sciami di droni, così come l'utilizzo di tecnologie 5G, sono, però, ancora in fase di sperimentazione e la possibilità di far operare droni duali facilmente reperibili in commercio in maniera cooperativa e autonoma non appare di semplice realizzazione. Inoltre, la realizzazione di uno sciame richiede competenze informatiche piuttosto marcate e l'acquisizione di un numero di droni sufficiente a costituire uno sciame aumenta esponenzialmente il costo che un eventuale operatore malintenzionato dovrebbe sostenere. Questi fattori potrebbero potenzialmente ridurre la propensione di singoli individui o organizzazioni non particolarmente strutturate a ricorrere a sciami per portare a compimento attacchi terroristici.

Tuttavia, sono già stati sviluppati software che, se implementati su componenti hardware già presenti in commercio e installati su droni duali *off-the-shelf*, potrebbero permettere la realizzazione di sciami cooperativi[124]. Inoltre, secondo uno studio pubblicato nel 2018 dalla National Academies of Science, Engineering, and Medicine di Washington, le tecnologie necessarie per sviluppare sciami di droni che prevedano l'impiego di centinaia di UAS saranno ampiamente disponibili sul mercato entro il 2025[125].

Gli *swarm* possono rappresentare una minaccia più grave rispetto a quella portata da un singolo drone tanto alla sicurezza nazionale quanto ai contingenti dispiegati in missioni fuori area principalmente a causa del numero maggiore di bersagli che si devono contrastare in caso di intromissioni malevole. Si pensi, ad esempio, ad uno sciame coordinato di diversi droni armati con esplosivi o materiali CBRN che, decollando da punti diversi, mirino tutti su uno stesso obiettivo sensibile. Gli strumenti da mettere in campo per contrastare efficacemente questa minaccia andrebbero moltiplicati e posizionati in zone anche molto distanti tra loro per ridurre le possibilità d'errore, ma aumenterebbero il numero di mezzi e risorse

[123] Guang Yang et al., *A Telecom Perspective on the Internet of Drones: From LTE-Advanced to 5G*, eprint arXiv:1803.11048, marzo 2018, https://arxiv.org/abs/1803.11048.

[124] Vivek Shankar Varadharajan et al., *A Software Ecosystem for Autonomous UAV Swarms*, International Symposium on Aerial Robotics, Philadelphia, 11-12 giugno 2017, https://www.bib.irb.hr/888549?rad=888549.

[125] National Academies of Sciences, *Engineering, and Medicine, Counter-Unmanned Aircraft System (CUAS) Capability for Battalion-and-Below Operations. Abbreviated Version of a Restricted Report*, Washington, The National Academies Press, 2018, https://doi.org/10.17226/24747.


ISSN 2280-6164

necessari al contrasto della minaccia.

Un ulteriore esempio di minaccia portata dagli *swarm* può essere identificata con la possibilità che essi siano composti da un solo drone armato, mentre gli altri potrebbero agire come "esche" mirando a confondere gli strumenti per la *detection* al fine di far concentrare le risorse messe in campo su punti diversi da quelli interessati dalla traiettoria di volo del drone armato. Mentre il primo esempio appare particolarmente sofisticato e di difficile realizzazione, il secondo potrebbe rappresentare una situazione ben più imminente e realizzabile tramite l'impiego di micro droni acquistabili per poche centinaia di euro.

Complessivamente la minaccia rappresentata dai droni duali appare, quindi, reale e attuale e le tecniche di contrasto risultano complesse per via del livello di avanzamento tecnologico raggiunto da questi prodotti e connotate da una profonda asimmetria. A queste difficoltà si aggiungono anche barriere e vuoti normativi dipendenti dal fatto che la minaccia sia emersa in tempi molto recenti e che rischiano di limitare le capacità di contrasto.


ISSN 2280-6164

## 2. Contesto giuridico e istituzionale nazionale

di Rachele de Rosa[126]

### *2.1 Normativa attuale nel controllo e nel contrasto*

L'uso sempre più diffuso dei droni duali non è stato normato sin dall'inizio, in parte perché era un fenomeno molto più ristretto rispetto a quanto non sia oggi, in parte perché non erano state previste dal legislatore nazionale, né da quello europeo, le possibili conseguenze di un loro impiego a fini illeciti. Il problema del vuoto normativo è duplice. Da un lato, la non chiara definizione di quelle che possono essere le attività lecite rende difficile tutelare sia l'utilizzatore del drone, che potrebbe ricadere nell'illegalità, sia il cittadino, al quale potrebbe essere arrecato un danno. Dall'altro, non vengono previste le attività di risposta all'atto illecito che, se intenzionale, potrebbe rientrare in un quadro più ampio che è quello della minaccia ibrida nei confronti dello Stato.

Con la revisione della parte aeronautica del Codice della Navigazione aerea (CdN) a norma dell'art. 2 della legge 9 novembre 2004, n. 265[127], i mezzi aeromobili a pilotaggio remoto (APR) sono considerati "aeromobili" ai sensi del novellato art. 743 del CdN rubricato "Nozione di aeromobile"[128]. Il disposto normativo aggiunge che gli APR sono definiti come tali dalle leggi speciali, dai regolamenti dell'Ente Nazionale per l'Aviazione Civile (ENAC) e, per quelli militari, dai decreti del Ministero della Difesa.

Se da un punto di vista giuridico gli UAS sono considerati aeromobili, in Italia, in Europa e in quasi tutti i Paesi aderenti all'Organizzazione internazionale per l'Aviazione civile (International Civil Aviation Organisation, ICAO), non possono ancora essere integrati nel traffico aereo generale, sebbene l'UE si sia posta questo obiettivo per gli anni a venire. Al momento gli UAS volano ancora prevalentemente in via sperimentale e con molte limitazioni d'impiego per non interferire con il traffico aereo generale. Il volo, per poter aver luogo in modo lecito, deve ricevere specifiche autorizzazioni dall'ENAC, in coordinamento con l'Ente Nazionale per l'Assistenza al Volo (ENAV) e l'Aeronautica Militare (AMI), anche al fine di evitare sconfinamenti in spazi o corridoi aerei riservati o ristretti al sorvolo.

[126] Rachele de Rosa è avvocato e collaboratrice della Rivista Aeronautica.

[127] Legge n. 256 del 9 novembre 2004: *Conversione in legge, con modificazioni, del decreto-legge 8 settembre 2004, n. 237, recante interventi urgenti nel settore dell'aviazione civile. Delega al Governo per l'emanazione di disposizioni correttive ed integrative del codice della navigazione*, in Gazzetta ufficiale n. 264 del 10 novembre 2004, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2004;265.

[128] Vedi Art. 743: Nozione di aeromobile, in *Codice della navigazione*, Parte seconda: Della navigazione aerea, Titolo V: Del regime amministrativo degli aeromobili, http://www.fog.it/legislaz/cn-0743-0775.htm.

ISSN 2280-6164

Il principio fondamentale della piena ed esclusiva sovranità di ogni Stato sullo spazio aereo sancito nell'art. 1 della Convenzione di Chicago del 1944 si applica anche al profilo di volo degli UAS, come specificato nell'art. 8 della Convenzione. Questo articolo impone il divieto di sorvolo, sul territorio di un altro Stato contraente, agli aeromobili senza pilota a bordo, se non con preventiva autorizzazione da parte di questo Stato.

In tale contesto, l'autorità preposta alla formulazione della normativa civile sui droni è l'ENAC che deve recepire i regolamenti e le direttive emanate a livello europeo per le materie di sua competenza. Nell'ambito delle funzioni di vigilanza della navigazione aerea, il disposto dell'art. 793 del CdN, stabilisce che l'ENAC può vietare il sorvolo su determinate zone del territorio nazionale italiano per motivi di sicurezza o di ordine pubblico, sia civili che militari[129]. Inoltre, secondo gli artt. 749 e 750 del CdN, l'ammissione degli UAV alla navigazione è possibile previa iscrizione nel Registro aeronautico nazionale tenuto dall'ENAC e con l'identificazione degli aeromobili, che può avvenire tramite l'apposizione sul velivolo delle marche di nazionalità. Queste ultime permettono una più facile individuazione del velivolo, della sua tipologia e caratteristiche principali, nonché delle generalità del proprietario e delle altre indicazioni richieste dai regolamenti dell'ENAC. Inoltre secondo le Condizioni di navigabilità dell'aeromobile[130], il velivolo deve essere munito di certificato di navigabilità e deve essere adibito soltanto all'impiego al quale è destinato. L'inosservanza delle norme di sicurezza durante lo svolgimento delle operazioni comporta l'applicazione delle sanzioni previste dalla legge[131]. Ciononostante, riguardo il profilo della responsabilità dei danni a terzi sulla superfice, esiste in dottrina una grossa diatriba. Diversi autori prevedono l'applicazione della Convenzione di Roma del 1952[132], di contro, alcuni altri addetti al settore, appellandosi al fatto che la Convenzione è stata ratificata solo da alcuni Paesi dell'UE (Italia, Belgio, Lussemburgo e Spagna), ritengono che la norma non possa disciplinare la fattispecie, auspicando l'elaborazione di provvedimenti riconosciuti a livello UE.

[129] Il Ministero delle Infrastrutture e dei trasporti (MIT) può, altresì, vietare la navigazione aerea su tutto il territorio nazionale, per eccezionali motivi di interesse pubblico.

[130] Le condizioni di navigabilità sono indicate agli articoli 763 e 764 del CdN.

[131] Nello specifico, il CdN all'art. 1228, comma 1 rubricato "Sorvolo di centri abitati", prevede sanzioni come arresto o ammenda in caso di sorvolo di centri abitati, assembramenti di persone, o aeroporti, senza osservare le prescrizioni del regolamento o gli ordini dell'autorità competente. Una simile sanzione è altresì prevista dall'art. 1231 CdN in caso di inosservanza di norme, disposizione di legge o di regolamento sulla sicurezza della navigazione. L'art. 1216 CdN contempla la sanzione per l'esercente che impiega un aeromobile non abilitato alla navigazione, ovvero con certificato di navigabilità che non sia in vigore. L'art. 1174 CdN prevede una sanzione amministrativa per l'inosservanza di un provvedimento legalmente dato dall'autorità competente in materia di polizia degli aeroporti.

[132] Convenzione di Roma del 1952 in seguito modificata con il protocollo aggiuntivo di Montreal del 23 settembre 1978 relativa ai danni causati alla superfice da aerei stranieri.

© 2020 IAI ISSN 2280-6164 DOCUMENTI IAI 20 | 04 - MARZO 2020

I principi enunciati nel Diritto della Navigazione hanno rappresentato uno strumento fondamentale per l'elaborazione della prima edizione del Regolamento emanato dall'ENAC[133], diretto a stabilire un quadro giuridico alla base dell'impiego e della circolazione dei droni. Il Regolamento, recentemente emendato con l'edizione n. 3 dell'11 novembre 2019[134], è entrato in vigore il 15 dicembre dello stesso anno. Esso ha l'obiettivo di includere nella regolamentazione nazionale alcuni requisiti derivanti dalla nuova normativa europea sugli UAS, la quale dovrà essere trasposta e applicata totalmente in tutti i Paesi membri dell'Unione europea a partire dal 1° luglio 2020. La normativa europea è costituita dal Regolamento di esecuzione dell'UE, n. 947 del 24 maggio 2019[135], che stabilisce procedure dettagliate per l'esercizio dei sistemi a pilotaggio remoto e dal Regolamento delegato UE 2019/945 che detta requisiti di progettazione e di fabbricazione[136].

Il primo regolamento suddivide gli UAS in cinque classi definite *Open Category*[137], da C0 a C4, che variano in base alla massa, alle specifiche tecniche, alle funzionalità automatiche e alle prestazioni del velivolo. La sicurezza delle operazioni che coinvolgono tali velivoli è garantita attraverso limitazioni operative specifiche e controlli di conformità agli standard industriali per la sicurezza dei prodotti. Pertanto, l'operatore che utilizza un drone *Open Category* dovrà rispettare le regole di circolazione aeronautica oltre che eventuali disposizioni di pubblica sicurezza dirette a interdire zone di volo.

Una novità introdotta con il nuovo regolamento europeo è l'equiparazione fra droni utilizzati a fini ricreativi e quelli ad uso professionale, facendo però una netta distinzione tra le operazioni specializzate e quelle non specializzate. Secondo quanto definito nell'art. 5, le operazioni specializzate sono riconducibili anche all'utenza professionale e sono attività che prevedono l'effettuazione, con un drone, di un servizio a titolo oneroso o meno. Di contro, le operazioni non specializzate sono intese come le attività ricreative effettuate con un UAS a scopo ludico o sportivo, da parte di un soggetto non configurabile come aeromodellista. In merito, il documento dell'ENAC ha stabilito una nuova classificazione di aeromodelli caratterizzati dall'assenza di sistemi automatici e/o autonomi, esentati dalla registrazione e dall'effettuazione di test online da parte degli operatori. Pertanto, gli aeromodelli sono definiti dalla normativa come una nuova classe di

[133] *Regolamento Mezzi Aerei a Pilotaggio Remoto*, Edizione n. 1 del 16 dicembre 2013, https://www.enac.gov.it/ContentManagement/information/N122671512/Regolamento_APR_ed.1.pdf.

[134] *Regolamento Mezzi Aerei a Pilotaggio Remoto*, Edizione n. 3 dell'11 novembre 2019, https://www.enac.gov.it/node/25825.

[135] *Regolamento di Esecuzione (UE) 2019/947 della Commissione del 24 maggio 2019 relativo a norme e procedure per l'esercizio di aeromobili senza equipaggio*, in Gazzetta ufficiale dell'Unione europea, 11 giugno 2019, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32019R0947 (entrato in vigore il 1° luglio 2019).

[136] *Regolamento Delegato (UE) 2019/945 della Commissione del 12 marzo 2019 relativo ai sistemi aeromobili senza equipaggio e agli operatori di paesi terzi di sistemi aeromobili senza equipaggio*, in Gazzetta ufficiale dell'Unione europea, 11 giugno 2019, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32019R0945.

[137] Nella *Open Category* rientrano i droni con peso massimo al decollo inferiore o uguale ai 25 kg.


ISSN 2280-6164

droni impiegabili unicamente a scopi ricreativi.

Tra gli obiettivi principali della terza edizione del regolamento nazionale c'è l'aumento del livello di sicurezza dell'UAV durante l'operazione. L'art. 33 rubricato *Security* stabilisce misure preventive contro atti illeciti sul normale svolgimento delle operazioni di volo, che possono essere rappresentati da interferenze volontarie sulle comunicazioni radio tra il drone e l'operatore. Tale normativa, inoltre, contempla l'elaborazione di procedure per impedire l'accesso di personale non autorizzato all'area delle operazioni e la possibilità di comunicare alle autorità di pubblica sicurezza i dati forniti all'ENAC dai Centri di Addestramento APR di cui all'art. 23, c. 3 del Regolamento.

Di conseguenza, i requisiti generali (art. 8) hanno lo scopo di ampliare la possibilità di identificare il proprietario del drone ed il profilo di volo, aumentando il rateo di tracciabilità dell'oggetto. Pertanto, chiunque utilizzi un drone, di qualsiasi peso e a scopo professionale, ha l'obbligo di registrarsi su portale *d-flight*[138] e di apporre un dispositivo di identificazione elettronica sull'UAV secondo le disposizioni di cui all'art. 37. L'applicazione al drone di un sistema elettronico di identificazione (*transponder*) che serva a trasmettere in tempo reale la posizione, direzione e velocità degli UAS è fondamentale soprattutto per le autorità competenti. Infatti, la necessità di avere un quadro *real-time* accurato è funzionale poiché permette all'autorità competente di verificare che gli UAS operino all'interno delle attività consentite dalla legge, ed è prerequisito per attività di contrasto in caso di un alto livello di rischio.

La norma prevede che il personale interessato a poter condurre operazioni non critiche (art. 9), ossia quelle attività condotte in *Visual Line of Sight* (VLOS) che non prevedono il sorvolo di aree congestionate, assembramenti di persone o agglomerati urbani, consegua un attestato di competenza rilasciato a seguito del completamento di un corso online e del superamento di un esame[139].

Di contro, per poter svolgere operazioni critiche – che secondo quanto stabilito dall'art. 10 non rispettano i limiti appena indicati e sono autorizzate dall'ENAC sulla base di accertamenti che tengono conto della complessità dei sistemi e della criticità degli scenari operativi – è necessario seguire un percorso di formazione presso uno dei centri di addestramento presenti a livello nazionale e autorizzati dall'ENAC. Al termine del percorso la modalità d'esame differisce in parte da quella prevista per le operazioni non critiche[140].

[138] Sito web consultabile al link: https://www.d-flight.it/portal.

[139] L'esame, previsto dall'art. 21 par. 1 del regolamento, deve svolgersi sul portale web dedicato dell'ENAC e prevede 40 domande a risposta multipla.

[140] L'esame prevede 30 domande a risposta multipla e una prova pratica con apposito esaminatore (art. 22).


ISSN 2280-6164

Una tipologia di drone che non è soggetta al preventivo ottenimento di un attestato per l'uso è rappresentata dai droni con un peso inferiore a 250 gr ad uso ricreativo. Tuttavia, nella regolamentazione ENAC è prevista la registrazione di quei droni che, sebbene abbiano peso inferiore a questa soglia, sono dotati di un dispositivo in grado di captare dati personali. Invece, droni dotati di telecamera ad uso ricreativo vengono esclusi dall'obbligo di registrazione e devono rispettare i dettami delle operazioni non critiche. La norma specifica, inoltre, che il volo deve essere condotto a vista, ad una distanza di sicurezza di almeno 150 m dalle aree congestionate e ad almeno 50 metri dalle persone che non siano sotto il diretto controllo dell'operatore. In tale contesto, vige il divieto di sorvolo di assembramenti di persone, agglomerati urbani e infrastrutture sensibili ad un'altezza rispetto al suolo non superiore ai 120 metri, rispettando le aeree indicate sul sito *d-flight* e quindi anche all'interno degli spazi aerei controllati (*Control Zone*, CTR)[141] e della zona di traffico di aeroporto (*Aerodrome Traffic Zone*, ATZ)[142].

La facoltà di condurre operazioni critiche e non, con un UAS dal peso compreso tra 250 gr e 25 kg, è supportata dalla stipula obbligatoria di un'assicurazione concernente la responsabilità verso terzi e adeguata allo scopo, secondo la previsione dettata dall'art. 32 della norma.

In tale contesto, l'art. 24 della regolamentazione ENAC prevede l'applicazione delle procedure stabilite nelle circolari *Air Traffic Management* (ATM) pubblicate dall'ENAC nelle aree del sedime aeroportuale e nelle vicinanze degli aeroporti (incluse le aviosuperfici) e degli eliporti/elisuperfici, all'interno dell'ATZ e della CTR. In particolare, il paragrafo 6 stabilisce la possibilità di istituire zone con divieto temporaneo di sorvolo agli APR ("*no fly zone*") su richiesta dell'Amministrazione competente per motivi di ordine pubblico e sicurezza. Esse sono pubblicate esclusivamente sul sito *d-flight*, e, pertanto, ai sensi dall'art. 33 paragrafo 4 è rimessa agli operatori la responsabilità di verificare l'esistenza di eventuali disposizioni relative al divieto di sorvolo emanate dalla Autorità di pubblica sicurezza per le aree interessate dalle operazioni.

Il periodo di allineamento completo con il Regolamento europeo è supportato dalla Circolare ATM-09 del 24 maggio 2019 rubricata "Aeromobili a Pilotaggio Remoto, criteri di utilizzo dello spazio aereo" entrata in vigore il 1° Luglio 2019[143]. La Circolare definisce specifici criteri di utilizzo dello spazio aereo, allo scopo di semplificare le procedure di richiesta da parte degli operatori e di ottimizzare il processo di valutazione e rilascio del nulla osta da parte dell'ENAC o dell'AMI a

[141] La CTR è uno spazio aereo controllato che si estende verso l'alto dalla superfice terrestre fino ad un determinato livello superiore, con la funzione di proteggere il traffico con procedura strumentale (*Instrument Flight Rules*, IFR) in avvicinamento e in partenza da un aeroporto.

[142] L'ATZ, è uno spazio aereo nelle vicinanze di un aerodromo istituito allo scopo di contenere e proteggere il traffico d'aeroporto.

[143] Circolare ATM-09 del 24 maggio 2019: *Aeromobili a pilotaggio remoto. Criteri di utilizzo dello spazio aereo*, https://www.enac.gov.it/la-normativa/normativa-enac/circolari/serie-atm/circolare-atm-09.

DOCUMENTI IAI 20 | 04 - MARZO 2020 ISSN 2280-6164

seconda dei casi. La normativa ridefinisce le procedure per l'utilizzo degli spazi aerei segregati e non segregati da parte degli APR e contestualmente aggiorna le quote e le distanze per voli effettuati con i droni a vista.

Nello specifico, l'ATM-09 al paragrafo 7 regola le operazioni VLOS ed *Extended-VLOS* (EVLOS), per APR con massa operativa al decollo minore di 25 kg, in prossimità degli aeroporti all'interno dell'ATZ e del CRT in cui non si richiede riserva di spazio aereo, differenziando tra aeroporti civili e militari. In entrambi i contesti, si diversificano delle zone in cui sono consentite le operazioni dei droni, a seconda della loro vicinanza al punto di riferimento aeroportuale (*Aerodrome Reference Point*, ARP) considerato. Le zone più vicine all'ARP sono identificate come "aree rosse" perché più a rischio. A seconda che l'aeroporto civile sia dotato o meno di procedure strumentali di volo[144], cambiano le distanze di riferimento, fermo restando che nelle aree rosse non sono generalmente consentite attività con gli APR. Nelle vicinanze degli aeroporti militari l'area rossa, in cui non sono consentite operazioni con APR, si estende entro un raggio di 6 km dall'ARP ed entro i limiti dell'ATZ, ferma restando la necessità di un nulla osta dell'Aeronautica Militare.

Parlando di aeroporti civili, le indicazioni inerenti alle distanze riportate nel paragrafo 7 si riferiscono all'ARP e si applicano a tutte le piste del territorio nazionale[145]. Prendendo a riferimento le aree indicate nel documento, le altezze massime possono essere aumentate fino al più alto "ostacolo" (si può trattare anche di un'infrastruttura) presente nel raggio di 50 metri dalla posizione dell'APR e che, se le aree indicate superano l'estensione del CRT, i loro limiti spaziali laterali devono essere ridotti ai limiti laterali dello stesso CRT, dal momento che non interessano lo spazio aereo non controllato. Nel caso, invece, in cui le aree in cui opera l'APR si sovrappongano a zone vietate, pericolose e regolamentate, nelle porzioni comuni di spazio aereo, le operazioni non sono consentite, a meno che non vi sia una specifica deroga da parte dell'ENAC[146]. In caso, invece, di aeroporti limitrofi fa fede il criterio più restrittivo.

Pertanto, l'attività dell'ente regolatore è diretta a stabilire un'azione preventiva al fine di garantire la sicurezza prima che l'effettiva minaccia si presenti in aeroporto. A tale proposito, l'ENAC sta lavorando alla definizione di direttive che regolino le attività di contrasto ai droni duali, andando a identificare sia le autorità preposte che le modalità e gli strumenti con i quali effettuare tali operazioni. La stesura di un simile documento normativo rappresenterebbe una novità nel panorama

[144] Nel primo caso l'area rossa si estende fino a 6 km dall'ARP longitudinalmente in entrambe le direzioni di pista e fino a 2,5 km lateralmente dalla pista (par. 7.8 della Circolare ATM-09 del 24 maggio 2019, cit.). Mentre negli aeroporti civili senza procedure strumentali di volo l'area rossa si estende fino a 3 km dall'ARP longitudinalmente in entrambe le direzioni di pista e fino a 1 km lateralmente dalla pista.

[145] Fa eccezione la pista 16L134R dell'aeroporto di Roma/Fiumicino per la quale le distanze sono calcolate in modo differente.

[146] Par. 6.4 della Circolare ATM-09 del 24 maggio 2019, cit.


ISSN 2280-6164

europeo e potrebbe fissare delle linee guida per successivi regolamenti anche a livello comunitario.

### *2.2 Responsabilità operative e istituzionali*

La proliferazione di droni duali connotati da caratteristiche tecnologiche che ne rendono possibile l'impiego per svariati scopi illeciti, ha reso sempre più impellente la necessità di dotarsi di adeguate procedure atte al loro contrasto. Pertanto, si impone la necessità di normare le operazioni di contrasto alla minaccia che i droni duali possono rappresentare sia per la sicurezza nazionale, che per quanto concerne i contingenti civili e militari impiegati in missioni fuori area.

In quest'ottica, risulta necessario analizzare quali siano gli organi preposti al contrasto dei droni duali a seconda dell'ambito in cui la minaccia si verifica, sia esso nazionale o afferente ai teatri operativi. In secondo luogo vanno identificati i limiti previsti dalla normativa vigente per quanto riguarda le tecniche di contrasto implementabili e la loro entità. Da ultimo, risulta di particolare rilievo l'analisi della disciplina riguardante la responsabilità dell'operatore preposto a effettuare il contrasto dei droni ostili, legata a eventuali effetti collaterali (danni a terzi) cagionati durante l'operazione. Proprio quest'ultima tematica risulta di fondamentale importanza al fine di tutelare anche l'operatore preposto al contrasto della minaccia dalle ripercussioni giuridiche di possibili effetti collaterali causati dal suo operato, qualora esso fosse condotto entro i limiti fissati dalle normative vigenti. A tal proposito, appare indispensabile analizzare le cause di esenzione della pena desumibili dal Codice penale (C.P.), dal Codice penale militare di pace (C.P.M.P.) e dal Codice penale militare di guerra (C.P.M.G.) a seconda che la condotta sanzionabile sia attribuita a un funzionario di pubblica sicurezza, o a un operatore militare che agisca sul territorio nazionale in supporto alle autorità civili, o che quest'ultimo si muova nei teatri operativi. Vanno dunque tenute in considerazione tanto la normativa che autorizza il funzionario al servizio d'ordine sul territorio nazionale ad agire in caso di necessità, quanto il quadro giuridico nazionale ed internazionale che legittima e disciplina l'impiego delle Forze Armate (FF.AA.) in teatro operativo.

Per quanto riguarda le operazioni di contrasto a un'eventuale minaccia alla sicurezza nazionale effettuata con droni duali, lo strumento giuridico di riferimento per individuare l'autorità responsabile dell'azione degli operatori preposti è la Legge 1° Aprile 1981, n. 121, "Nuovo ordinamento dell'Amministrazione della pubblica sicurezza"[147].

[147] Legge n. 121 del 1 aprile 1981: *Nuovo ordinamento dell'Amministrazione della pubblica sicurezza*, in Gazzetta ufficiale n. 100 del 10 aprile 1981, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1981-04-01;121.


ISSN 2280-6164

ISSN 2280-6164

Ai sensi dell'art. 1 di detta legge, la responsabilità della tutela dell'ordine e della sicurezza pubblica è attribuita al ministro dell'Interno in concerto con l'amministrazione della pubblica sicurezza. Nello specifico secondo l'art. 13 della legge n. 121 le attività degli ufficiali e agenti di pubblica sicurezza nella provincia sono coordinate dal Prefetto, il quale si avvale del Comitato provinciale per l'ordine e la sicurezza pubblica in caso di adozione di misure occorrenti alla previsione dei reati, come è stabilito nell'art. 20. Ciononostante, nello svolgimento delle sue mansioni, la Forza pubblica è autorizzata dal Questore che ha la responsabilità e il coordinamento a livello tecnico-operativo del servizio di ordine e sicurezza pubblica.

Nella normativa vigente sono previsti casi nei quali gli operatori di pubblica sicurezza possono essere coadiuvati da personale delle FF.AA. al fine di garantire una migliore protezione della popolazione o delle infrastrutture verso le quali potrebbero essere veicolate minacce, comprese quelle portate da impieghi illeciti dei droni duali. Infatti, in alcune operazioni nazionali/critiche come, ad esempio, quelle che riguardano grandi eventi caratterizzati da agglomerati di persone anche in ambito urbano, le FF.AA. sono chiamate a supporto delle Forze di pubblica sicurezza solitamente preposte allo svolgimento delle necessarie attività. Con particolare riferimento alle minacce portate dai droni duali, la necessità di prevedere il supporto delle FF.AA. è motivata da due fattori: la natura della minaccia e le peculiari competenze sviluppate in ambito militare per svolgere le attività di contrasto[148]. Avvalendosi di un approccio interforze e in maniera sinergica con il mondo civile, sia l'Esercito Italiano (EI) che l'AMI sono attualmente impegnate nello sviluppo di procedure e sistemi volti al contrasto dei droni duali[149]. Personale di queste FF.AA. è già stato impiegato in supporto agli operatori di pubblica sicurezza in concomitanza con eventi di grande rilevanza pubblica verificatisi sul suolo nazionale.

Per quanto concerne i disposti normativi che definiscono le possibilità di risposta ad eventuali minacce portate da droni duali, nonché le limitazioni previste all'uso legittimo della forza da parte delle autorità, si registra un *vacuum* normativo sia a livello italiano che europeo e internazionale. A tal proposito, a livello italiano, la legge *in fieri*, nell'intento di definire la natura giuridica della minaccia proveniente dagli UAS, contempla due tipi di norme: una atta a disciplinare le modalità per contrastarla e a stabilire un'escalation di sistemi cinetici idonei ad abbattere il drone, l'altra con l'obiettivo di stabilire i mezzi tecnici attraverso i quali sarà possibile abbattere il drone. In tale contesto saranno stabilite aree *buffer*, corridoi di volo e *no-fly zone* in prossimità di aree e infrastrutture sottoposte a protezione. Nell'elaborazione del testo della legge, la disciplina di riferimento richiamata in

[148] Ministero della Difesa, *Festività natalizie, Operazione Strade Sicure: continua impegno del personale dell'AM a presidio di importanti aeroporti nazionali*, 24 dicembre 2018, http://www.aeronautica.difesa.it/comunicazione/notizie/Pagine/20181224_20181224_FestivitaNatalizie_Aeroporti_StradeSicure.aspx.

[149] Per una descrizione dettagliata delle iniziative portate avanti da entrambe le Forze Armate qui citate si rimanda al paragrafo 3.2 del presente studio.

caso di violazione delle zone interdette al volo è l'art. 965 della parte seconda del CdN[150].

Pertanto, la normativa prevede che all'operatore siano fornite adeguate conoscenze necessarie a valutare quale sistema anti-drone, cinetico o meno, sia possibile utilizzare per meglio contrastare la minaccia e limitare eventuali danni collaterali.

La minimizzazione degli effetti collaterali è uno dei punti sui quali la legislazione in divenire si sta concentrando in maniera più consistente. Tuttavia, stante la natura della minaccia, rimane la possibilità che questi si verifichino. Vanno dunque ampliati i disposti legislativi a tutela dell'operatore di pubblica sicurezza, o del militare in suo supporto, che, pur rispettando i termini e le limitazioni previste dalla normativa in materia di contrasto dei droni duali, dovesse trovarsi ad arrecare danni a terzi. In merito, il quadro giuridico è costituito dai disposti normativi del C.P.[151] e del C.P.M.P.[152]. I due regimi giuridici partono da presupposti diversi per affrontare simili problematiche.

Nel caso in cui un operatore di pubblica sicurezza causi danni collaterali durante le operazioni di contrasto di droni malevoli, si nota che, in maniera analoga a quanto accade in altre fattispecie, la prassi preveda l'apertura di un fascicolo giudiziario presso la Procura della Repubblica competente. La procedura è volta a valutare in termini penali, amministrativi e disciplinari la sussistenza o meno della responsabilità giuridica del soggetto indagato. Nello specifico, il Pubblico ministero (PM), quale organo deputato all'indagine, avuto formalmente conoscenza del verificarsi del fatto che può essere oggetto dell'azione penale lo iscrive immediatamente nell'apposito registro per verificare l'eventuale responsabilità dell'operatore.

Tuttavia, la vigente legislazione prevede motivi di esenzione dalla responsabilità per i danni a terzi inavvertitamente causati durante operazioni che prevedano l'uso legittimo della forza, a condizione che questo rispetti i limiti previsti dalla legge. L'art. 51 C.P. rubricato "Esercizio di un diritto o adempimento di un dovere", recita al primo comma "L'esercizio di un diritto o l'adempimento di un dovere imposto da una norma giuridica o da un ordine legittimo della pubblica autorità, esclude la punibilità". Inoltre, gli articoli 52, 53 e 54 del C.P. forniscono ulteriori scriminanti a tutela dell'operatore. In particolare, l'art 52 C.P. codifica la legittima

[150] Art. 965: Responsabilità dell'esercente per danni a terzi sulla superficie, in *Codice della Navigazione*, Parte seconda: Della navigazione aerea, Titolo II: Della responsabilità per danni a terzi sulla superficie e per danni da urto, aggiornata al decreto legislativo 15 marzo 2006 n.151, http://www.fog.it/legislaz/cn-0965-0980.htm.

[151] Regio Decreto n.1398 del 19 ottobre 1930: *Approvazione del testo definitivo del Codice Penale*, in Gazzetta ufficiale n. 251 del 26 ottobre 1930, provvedimento entrato in vigore il 1 luglio 1931, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1930-10-19;1398.

[152] Regio Decreto n.303 del 20 febbraio 1941: *Codici penali militari di pace e di guerra*, in Gazzetta ufficiale n. 107 del 6 maggio 1941, provvedimento entrato in vigore il 21 maggio 1941, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:relazione.e.regio.decreto:1941-02-20;303.

ISSN 2280-6164

difesa, stabilendo che non è punibile chi ha commesso il fatto per esservi stato costretto dall'impellente necessità di difendersi contro un'offesa ingiusta. L'art. 53 C.P. disciplina l'uso legittimo delle armi, stabilendo che "non è punibile il Pubblico Ufficiale che, al fine di adempiere a un dovere del proprio ufficio, fa uso, ovvero ordina di far uso, delle armi o di altro mezzo di coazione fisica quando vi è costretto dalla necessità di respingere una violenza o di vincere una resistenza all'autorità e comunque di impedire la consumazione di delitti di strage". La stessa disposizione si applica a qualsiasi persona che, legalmente richiesta dal pubblico ufficiale gli presti assistenza. L'art. 54 regola lo stato di necessità, secondo cui non è possibile punire chi ha commesso un reato se è stato costretto dalla necessità di salvare sé o altri.

Dalla lettura integrata degli art. 51 e 54 C.P., il comportamento che ha cagionato l'effetto lesivo sarebbe scriminato dall'adempimento di un dovere per ordine impartito da un'autorità sovraordinata ed escluso alla stregua dello stato di necessità. Tale cornice giuridica può essere integrata dal divieto di sorvolo stabilito dall'art. 793 della parte seconda del CdN.

Secondo l'attuale quadro normativo nazionale, l'ENAC ha il potere di vietare il sorvolo su determinate zone del territorio nazionale per motivi di sicurezza o di ordine pubblico[153] su richiesta della competente amministrazione. Nella fattispecie, il divieto, esteso all'utilizzo di UAS, è istituito a seguito di richiesta da parte della Prefettura presso l'ufficio territoriale del Governo della città interessata dall'evento. Pertanto, anche in caso di abbattimento di un drone che, pur non risultando armato, si trovasse a sorvolare aree precluse da apposita decisione dell'amministrazione competente, esisterebbero gli estremi per una esclusione di responsabilità per l'operatore che dovesse causare danni a terzi. Ciò è motivato dal fatto che, pur potendo risultare la difesa sproporzionata rispetto all'offesa, conoscere in anticipo l'effettiva entità della minaccia sia particolarmente complicato. Inoltre, in caso di zona interdetta al sorvolo vi sarebbe una violazione che può essere ritenuta minacciosa per definizione.

Per quanto concerne l'eventualità che sia un appartenente alle FF.AA. posto a supporto delle autorità civili di pubblica sicurezza a causare danni a terzi tramite l'abbattimento di un drone, la norma prevede che venga aperto un fascicolo giudiziario presso la Procura Militare civile e penale di Roma. All'apertura del fascicolo segue la formazione di un costrutto legale con l'obiettivo di accertare la sussistenza o meno della responsabilità oggettiva del Comandante, e della responsabilità soggettiva dell'operatore materiale. In questa circostanza è applicata in primo luogo la normativa stabilita nel C.P. e nel Codice civile (C.C.). Solo in seconda istanza si applica la disciplina prevista dal C.P.M.P.

[153] Si parla in questi casi di *NOtice to AirMen* (NOTAM).


ISSN 2280-6164

Considerando il caso in specie, ossia l'abbattimento di un drone duale ostile o potenzialmente tale che dovesse trovarsi a sorvolare aree interdette, la tutela della responsabilità del militare sottoposto ad indagine è auspicabile richiamando la disciplina che contempla le cause di giustificazione dell'uso della forza. Infatti, ai sensi dell'art. 42 C.P.M.P., per i reati militari non è punibile chi è costretto a compiere un reato militare, se costretto dallo stato di necessità, sempre che la difesa sia stata proporzionata all'offesa.

Per quanto riguarda il contrasto alla minaccia afferente all'uso illecito di droni duali che si verifichi in teatri operativi, le normative vigenti sono profondamente diverse sia per quanto riguarda l'autorità preposta alla difesa, sia per ciò che concerne il quadro giuridico e le limitazioni all'uso della forza. Per contro, il costrutto normativo che riguarda la tutela dell'operatore in caso di danno a terzi si presenta sostanzialmente identico.

Per meglio comprendere i suddetti punti, è necessario partire dai disposti del diritto internazionale umanitario (DIU), analizzando anche le prassi normative internazionali relative ai conflitti armati.

Nelle operazioni di *Military Operations Other Than War* (MOOTW)[154], l'impiego delle FF.AA. ha l'obiettivo di evitare lo scoppio o il perpetuarsi di un conflitto, la promozione della pace e il supporto alle autorità civili in risposta a crisi di ordine interno. In questo contesto, un elemento fondamentale da considerare è che l'invio all'estero dei contingenti militari italiani è disciplinato da due fondamentali previsioni legislative: l'art. 1 c. 1, Legge 14 novembre 2000, n. 331[155], rubricato Compiti delle Forze Armate e gli artt. 3 c. 3 e 7 c. 1, Legge 18 febbraio 1997, n. 25[156]. L'art. 1 c. 1, Legge 14 novembre 2000, n. 331, menziona, tra gli altri, il compito di operare al fine della realizzazione della pace e della sicurezza, in conformità alle regole del diritto internazionale ed alle determinazioni delle organizzazioni internazionali delle quali l'Italia fa parte, mentre gli artt. 3 c. 3 e 7 c. 1, Legge 18 febbraio 1997, n. 25, assegnano al Capo di Stato Maggiore della Difesa l'impiego delle Forze Armate.

Inoltre, la conduzione delle operazioni militari ostili è disciplinata dal DIU, detto anche diritto dei conflitti armati. Secondo i principi fondamentali di *necessità*, *proporzionalità* e *distinzione* sanciti nel disposto normativo, l'impiego della forza deve essere necessario, sotto il profilo militare, e proporzionato all'obiettivo. Pertanto, sono vietati mezzi e metodi di combattimento che, per la loro natura, possano causare danni collaterali eccessivi rispetto all'entità dell'attacco o alla

[154] In questa categorie rientrano operazioni di *peace keeping*, *peace building*, e *peace enforcement*.

[155] Legge n. 331 del 14 novembre 2000: *Norme per l'istituzione del servizio militare professionale*, in Gazzetta ufficiale n. 269 del 17 novembre 2000, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2000-11-14;331.

[156] Legge n. 25 del 18 febbraio 1997: *Attribuzioni del Ministro della difesa, ristrutturazione dei vertici delle Forze armate e dell'Amministrazione della difesa*, in Gazzetta ufficiale n. 45 del 24 febbraio 1997, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1997-02-18;25.

DOCUMENTI IAI 20 | 04 - MARZO 2020 ISSN 2280-6164

necessità di difendersi da determinati attacchi. I militari sono altresì obbligati a dirigere le azioni di contrasto esclusivamente contro obiettivi militari per il principio di distinzione fissato dal DIU. Dunque, pur rimanendo ben saldo l'imprescindibile diritto del personale militare impegnato in missioni fuori area di difendersi da un attacco armato attuale o imminente, le normative internazionali limitano le possibilità di risposta ad esso. Queste regole sono fissate al fine di mantenere un bilanciamento tra offesa e difesa, anche qualora essa prendesse le sembianze di una contro-offensiva.

In particolare, le regole che autorizzano l'uso della forza in teatro operativo, nel rispetto del diritto internazionale, del DIU, nonché delle leggi e regolamenti nazionali in vigore sono le regole d'ingaggio (*Rules of Engagement*, ROE), la cui formazione ha inizio dal più alto livello della catena gerarchica, ovvero quello politico-militare, per scendere poi attraverso il livello strategico, operativo e tattico, fino al militare in campo e sono diramate dalle competenti autorità militari in base al tipo di missione da portare a compimento.

Nel caso italiano, l'elenco delle ROE ritenute necessarie per l'assolvimento della missione è predisposto dal Comando Operativo di Vertice Interforze (COI), in coordinamento con le varie FF.AA. In seguito le norme sono presentate tramite il Capo di Stato Maggiore della Difesa al ministro della Difesa, per poi essere poste al vaglio del Parlamento per l'approvazione finale. L'autorizzazione parlamentare della missione include anche l'accettazione implicita delle regole scelte. Tuttavia, il Governo si fa carico di garantire il rispetto dei principi irrinunciabili dell'ordinamento nazionale, inserendo eventualmente i *caveat*, ossia riserve che derogano al testo delle ROE stabilite a livello di coalizione/internazionale, in modo tale da armonizzarle con le leggi nazionali, e mantenendo come cardine il rispetto dei principi costituzionali.

Tuttavia, le azioni di un'unità impiegata all'estero dipendono dalle disposizioni del Comando superiore che varia in base alla tipologia delle operazioni da condurre in teatro. A seconda dell'operazione, si attiva il livello di comando dedicato a cui è attribuita la responsabilità dell'intera operazione che può essere nazionale, di coalizione, NATO e che si suddivide nei tre livelli strategico, operativo e tattico.

Inoltre, al fine di permettere di raggiungere gli obiettivi della missione senza operare in contrasto con i regolamenti internazionali e la normativa che regola l'impiego delle FF.AA. è stata istituita la figura del *Legal Advisor*. In teatro, secondo quanto stabilito dall'art. 82 del 1° Protocollo addizionale del 1977 alle quattro Convenzioni di Ginevra sul DIU[157], i *Legal Advisor* hanno un doppio ruolo. Da una parte, essi fungono da consulenti per i comandanti militari in merito ad una

[157] Protocollo aggiuntivo alle Convenzioni di Ginevra del 12 agosto 1949 relativo alla Protezione delle vittime dei conflitti armati internazionali, adottato a Ginevra l'8 giugno 1977, ratificato dall'Italia con legge 11 dicembre 1985, n. 762 (in Suppl. ordinario alla Gazzetta ufficiale n. 303 del 27 dicembre 1985), https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1985-12-11;762.


ISSN 2280-6164

corretta ed effettiva applicazione delle convenzioni e relativi protocolli; dall'altra supportano i comandanti militari nell'insegnamento dei disposti normativi al personale militare per il quale sono responsabili. Il *Legal Advisor* è informato sui dettagli dell'operazione e consiglia al militare quali ROE applicare per l'assolvimento dei compiti assegnati dall'autorità gerarchicamente superiore. Nello specifico, può consentire o negare determinate azioni in modo da permettere il pieno raggiungimento degli obiettivi della missione senza agire in contrasto con quanto previsto dal diritto.

Tuttavia, vanno fatte delle distinzioni tra quelle che sono le caratteristiche delle operazioni di contrasto ad una minaccia convenzionale o non-convenzionale. Infatti, le operazioni relative al contrasto della minaccia convenzionale contemplano un flusso decisionale che va dall'autorità più alta gerarchicamente fino al preposto all'operazione, con tempistiche adeguate e in un'ottica di reazione proporzionata (come, ad esempio, la procedura di difesa aerea con decollo su allarme *scramble*)[158]. Di contro, nel caso di minaccia non convenzionale, asimmetrica e difficilmente contrastabile con i mezzi di cui le FF.AA. sono solitamente dotate, come quella proveniente da un drone duale, la compressione del tempo di reazione richiede una procedura pre-autorizzata. Sulla base di quest'ultima, l'operatore è autorizzato a neutralizzare la minaccia senza contattare il superiore, se ciò è quanto permesso. Pertanto, i contingenti militari impiegati in missioni fuori area sono addestrati e opportunatamente informati in merito all'attività di contrasto di UAS duali, principalmente afferenti alle categorie micro e mini, con sistemi di rilevamento, identificazione, tracciamento e interdizione specifici per contrastarla.

In caso di danni collaterali cagionati in risposta a un atto ostile, indipendentemente se questo si verifichi durante operazioni militari in teatro o sul territorio nazionale, la norma prevede l'avvio dell'iter già descritto in precedenza relativo all'apertura del fascicolo giudiziario presso la Procura Militare civile e penale di Roma.

La cornice giuridico/operativa evidenzia che le scriminanti a tutela della responsabilità dell'operatore sono stabilite da profili normativi predefiniti. In particolare, anche per effetti collaterali causati dall'operato di personale militare impegnato in missioni fuori area, le scriminanti possono essere ritrovate nel già citato art. 42 C.P.M.P. Pertanto, qualora l'operazione che causi danni a terzi sia condotta nel rispetto delle norme che regolano l'impiego delle FF.AA. in campo internazionale, l'esenzione dalla responsabilità dell'operatore sarebbe garantita dal quadro giuridico esistente.

Riguardo la difesa anti-drone degli aeroporti civili e assimilati, si riscontra come questa sia ad oggi nelle mani della società di gestione dell'aeroporto. Infatti, alla luce del Regolamento europeo 2018/1139, le società di gestione sono responsabili per il mantenimento della *safety* degli aeroporti e delle zone limitrofe da eventuali

[158] Davide Bartoccini, "Cos'è la procedura di 'Scramble' che difende i cieli dell'Italia", in *InsideOver*, 22 luglio 2018, https://www.insideover.com/?p=167617.


ISSN 2280-6164

pericoli, siano essi fissi o mobili[159]. Pertanto, l'azione preventiva volta a garantire la sicurezza dell'infrastruttura e delle sue attività deve essere pianificata e condotta dai gestori degli aeroporti, i quali sono supportati e guidati dall'ENAC anche alla luce della prossima uscita del regolamento sulle procedure e strumenti per il contrasto ai droni duali al quale si è già fatto riferimento in precedenza. Tuttavia, nel caso in cui venissero registrate frequenti attività potenzialmente minacciose, o qualora la minaccia veicolata a mezzo droni dovesse avere implicazioni sulla *security*, le autorità aeroportuali possono richiedere il supporto della Polizia di Stato, o un intervento diretto da parte del personale di quest'ultima. Anche personale delle FF.AA. potrebbe essere impiegato per i medesimi scopi.

Per la stipula di misure e procedure volte a salvaguardare la *safety* dell'infrastruttura e delle sue attività, le società di gestione degli aeroporti, in collaborazione con personale dell'ENAC, si avvalgono dei Comitati di Sicurezza aeroportuale (CSA)[160]. Nei CSA è solitamente prevista anche la partecipazione di funzionari della Polizia di Stato al fine di stabilire misure e procedure di sicurezza preventiva in maniera efficace e sinergica. Pertanto, è lecito affermare che la Polizia di Stato giochi un ruolo nella garanzia della sicurezza degli aeroporti, anche se in maniera prettamente consultiva e intesa per la pianificazione *ex-ante*. Per contro, non è prevista la presenza in pianta stabile all'interno delle infrastrutture aeroportuali di personale della Polizia di Stato o delle FF.AA. che potrebbero garantire una repentina ed efficace risposta in caso di minacce afferenti alla sfera della *security* veicolate con droni appositamente modificati e, potenzialmente, armati.

Per quanto riguarda l'attribuzione di responsabilità in caso di danno a terzi causato durante operazioni di contrasto ai droni duali all'interno o in prossimità degli aeroporti, è importante notare come questa ricadrebbe sulla società di gestione e, qualora si registrassero atti che prevarichino i limiti previsti dalla legislazione vigente, sul singolo operatore. Allo stato attuale, le scriminanti a tutela di società e operatore, sia esso interno al personale della società di gestione o un membro della Polizia di Stato o delle FF.AA., risultano essere le stesse descritte in precedenza per operazioni dello stesso tipo condotte in altri contesti sul territorio nazionale. Tuttavia, lo sforzo normativo già in atto presso ENAC per definire procedure e misure volte a garantire la sicurezza degli aeroporti potrebbe portare ad una definizione più chiara e dettagliata delle procedure e misure lecite al fine di garantire la sicurezza in tali infrastrutture.

Indipendentemente dalla possibilità di trovare nel quadro giuridico esistente tanto le definizioni degli operatori incaricati a contrastare la minaccia rappresentata dall'impiego illecito di droni duali, che i limiti alle tecniche di contrasto e le

[159] *Regolamento (UE) 2018/1139 del del 4 luglio 2018, recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea...*, in Gazzetta ufficiale dell'Unione europea, 22 agosto 2018, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32018R1139.

[160] I CSA sono stati istituiti nel 1971 in riferimento alle disposizioni contenute nell'Annesso 17 della Convenzione di Chicago.

© 2020 IAI
ISSN 2280-6164
DOCUMENTI IAI 20 | 04 - MARZO 2020

scriminanti per gli operatori, appare necessaria la stesura di nuove regole che normino unicamente e specificatamente queste tematiche. Infatti, il vuoto normativo riscontrato in termini di regole che affrontino la questione in maniera strutturata e onnicomprensiva apre a problemi interpretativi, legando alle singole fattispecie il ruolo delle autorità preposte al loro contrasto. Allo stesso modo, anche le scriminanti a tutela dell'operatore potrebbero risultare aperte all'interpretazione e legate alle particolari dinamiche dei singoli casi. La rilevanza che la minaccia portata dai droni duali ha assunto negli ultimi anni impone pertanto al legislatore, sia nazionale che internazionale, di definire con chiarezza le normative che ne regolino il contrasto.

Concludendo, dall'analisi effettuata nel documento sugli aspetti giuridici connessi allo svolgimento delle missioni fuori area e in territorio nazionale, emerge la delicata questione della necessità di definire rapidamente la posizione degli operatori eventualmente coinvolti in un'indagine sui "danni collaterali" di un'operazione anti-drone.

Alcuni fatti di cronaca[161] registrati in passato hanno già evidenziato come incerte definizioni circa le autorità competenti e i limiti previsti dalla legge entro i quali una qualsivoglia azione debba mantenersi possano avere ripercussioni considerevoli sugli operatori impegnati in attività di contrasto. Uno degli eventi più esplicativi di tale dinamica è rappresentato dalla cosiddetta Tragedia di Otranto del 1997, dove in seguito ad uno scontro tra la corvetta Sibilla della Marina Militare e un natante con a bordo numerosi migranti partiti dalle coste albanesi si registrò il decesso di 81 persone. L'iter giudiziario successivo vide in un primo momento l'apertura di un fascicolo a carico dei vertici della Marina che avevano impartito le ROE per ostacolare gli sbarchi. Questa venne in seguito archiviata, rimanendo sul banco degli imputati solo l'ufficiale incaricato di eseguire gli ordini che prevedevano le manovre di dissuasione divenute fatali per l'imbarcazione con a bordo i migranti[162]. In seguito al processo[163], durato 17 anni, l'ufficiale in questione fu condannato a due anni di carcere nel 2014. Similmente, nel 2013 i quattro ufficiali in servizio sul pattugliatore Libra vennero accusati dal Giudice per le indagini preliminari (GIP) di Palermo e Agrigento del reato di omicidio con dolo eventuale ai sensi dell'art. 40 C.P.[164]. In questa circostanza, il capo d'accusa fu inerente a una omissione di soccorso nelle circostanze del naufragio di un'imbarcazione di fortuna partita dalle coste libiche con a bordo più di 200 migranti. Per competenza, la causa passò poi al GIP del Tribunale di Roma che dispose di non dare seguito alla richiesta di archiviazione avanzata dalla Procura della Repubblica. Pertanto, i fatti sono ancora

[161] I più famosi sono quelli della nave Sibilla nel marzo 1997 con profughi dall'Albania e della nave Libra nell'ottobre 2013 con i profughi dalla Libia.

[162] Attualmente le ROE sono diverse in quanto non si dissuade, si soccorre.

[163] "Naufragio canale d'Otranto: 108 morti, condanne confermate", in *Ansa*, 30 giugno 2011, https://www.ansa.it/mare/notizie/rubriche/uominiemare/2011/06/30/visualizza_new.html_811011463.html.

[164] La circostanza infatti configura l'ipotesi di dolo eventuale che s'innesta sulla causazione dell'evento (art. 40 C.P.).


ISSN 2280-6164

oggi sottoposti a procedimento penale e non si è ancora giunti ad una sentenza definitiva di alcun tipo[165].

L'eccessiva lunghezza dei periodi necessari non solo per l'emissione di una sentenza, ma anche per la mera decisione sull'apertura di una procedura giudiziaria a carico degli operatori, impedisce a questi ultimi di poter svolgere pienamente le loro funzioni nelle fasi in cui sono in corso le indagini preliminari, bloccandone a fini cautelativi anche eventuali avanzamenti di carriera. Il rischio di vedere compromessa la propria carriera in maniera irreversibile, anche qualora si dovesse risultare innocenti o non dovesse essere aperta una procedura processuale, è ben risaputo dagli ufficiali e altri operatori preposti al contrasto e ciò potrebbe incidere sulla loro valutazione del rischio.

Quindi è opportuno un impegno congiunto del legislatore e della magistratura per trovare in tempi brevi una soluzione adeguata. Una procedura accelerata, fermo restando il principio fondamentale della necessità della magistratura di poter disporre delle tempistiche necessarie a supporto della fase istruttoria, potrebbe consentire di arrivare alle decisioni del caso in tempi rapidi, senza creare interferenze potenzialmente dannose nelle procedure di avanzamento di carriera dei predetti soggetti.

Alla luce di quanto precedentemente illustrato, in caso di contrasto della minaccia proveniente dai droni si può sostenere con forza l'urgenza di stabilire le regole da applicare a tutela dell'ufficiale incaricato di obbedire agli ordini. In tal modo la professionalità dell'operatore non dovrebbe rischiare d'incorrere in avvenimenti gravi e pregiudizievoli per la sua carriera.

[165] Open Migration, *Naufragio dei bambini: dopo sei anni un processo per accertare le responsabilità*, 11 ottobre 2019, https://openmigration.org/analisi/naufragio-dei-bambini-dopo-sei-anni-un-processo-per-accertare-le-responsabilita.


ISSN 2280-6164

## 3. Contrasto delle nuove minacce

di Ester Sabatino

### *3.1 I sistemi di contrasto*

L'entità della minaccia rappresentata dall'uso illecito dei droni duali ha portato i principali attori del settore aereo[166], così come le organizzazioni di difesa e sicurezza nazionale e regionale, a pensare a soluzioni *ad hoc* per il loro contrasto. Dando uno sguardo alla grandezza del mercato dei sistemi anti-drone (Counter-UAS o C-UAS) è possibile comprendere come la minaccia dei droni duali sia diventata di grande interesse non solo per le forze armate, ma anche per attori civili e privati.

Secondo alcune analisi, il mercato mondiale dei sistemi anti-drone è destinato a raggiungere un market value di circa 2 miliardi di dollari nel 2024[167]. Questo dato rappresenta un tasso annuo di crescita composto del 16,83 per cento nel periodo 2019-2024[168]. La rapida espansione del mercato dei sistemi anti-drone evidenzia come la minaccia portata dai droni sia diventata non solo più tangibile rispetto a pochi anni fa, ma anche più probabile. La crescente disponibilità e accessibilità dei droni, soprattutto di piccole dimensioni e tecnologicamente avanzati che possono essere utilizzati per usi illeciti, ha innescato a sua volta una richiesta sempre più pronunciata di sistemi in grado di contrastarli. Inoltre, droni di piccole dimensioni tenderanno ad essere sempre più integrati nei sistemi d'arma convenzionali, come può essere il caso dell'aereo da combattimento di sesta generazione, o il carro armato di quinta generazione, ampliando la necessità, per le forze armate, di dotarsi di sistemi C-UAS, sia fissi che mobili[169] e di integrare una capacità di difesa anti-drone nei sistemi principali.

Dal momento che la tipologia della minaccia, sebbene non più "nuova", può comunque essere considerata recente, le possibilità di contrasto dei droni duali devono sperimentare ancora una fase di evoluzione e definizione per quanto riguarda i requisiti necessari per sistemi C-UAS civili e militari. Questo processo, a causa delle caratteristiche della minaccia, così come del quadro giuridico di

[166] Durante la 40a assemblea generale triennale dell'ICAO è stato presentato un documento che sottolinea l'importanza di arrivare alla definizione di standard e procedure congiunte per limitare e mitigare i danni derivanti dall'uso improprio di droni. Per maggiori informazioni si veda: Airports Council International (ACI) et al., *The Need for Standards and Guidance to Mitigate the Risks of, and to Improve Response to Unauthorized UAS Operations* (A40-WP/196), 1 agosto 2019, https://www.icao.int/Meetings/a40/Lists/WorkingPapers/DispForm.aspx?ID=236.

[167] Frost & Sullivan, *Global Market for Counter Unmanned Aircraft Systems to Exceed $2 billion by 2024*, 25 ottobre 2019, https://ww2.frost.com/news/press-releases/global-market-for-counter-unmanned-aircraft-systems-to-exceed-2-billion-by-2024.

[168] BIS Research, *Global Counter-UAS (Anti-Drone) Market: Focus on Technology... Analysis and Forecast 2019-2024*, 2019, https://bisresearch.com/industry-report/counter-uas-market.html.

[169] Leonardo DRS, "Vehicle Platform Integration: Where Technologies Become Capabilities", in *Breaking Defense*, 14 ottobre 2019, https://breakingdefense.com/?p=79967.


ISSN 2280-6164

riferimento ancora in fase di definizione e implementazione[170], genera delle criticità sotto diversi aspetti.

Partendo da un punto di vista economico, i sistemi anti-drone hanno un costo decisamente più elevato rispetto ai sistemi che sono chiamati a dover contrastare[171]. Un drone duale dotato di caratteristiche tecniche sufficientemente elevate da poter rappresentare una minaccia, può essere facilmente acquistabile sul mercato per poche migliaia di euro, mentre un sistema di contrasto può arrivare a costare diversi milioni di euro. Nonostante il costo di un sistema C-UAS quanto più completo possibile sia considerevolmente minore rispetto ad altri tipi di armamenti, la spesa per la loro acquisizione risulta comunque sproporzionata se considerata in relazione al costo potenziale della minaccia, aumentandone l'asimmetricità. Inoltre, il fatto che essa possa essere generata anche quando l'intenzione dell'operatore non è quella di arrecare danno o di portare a termine un attentato terroristico, induce gli operatori di pubblica sicurezza a dover intervenire in ogni caso, per limitare possibili danni a cose e persone, che possono essere causati anche involontariamente dall'operatore.

Per comprendere eventuali danni causati anche da un semplice hobbista che sconfina in zone interdette al volo è sufficiente pensare ai danni, economici e non, causati dall'incidente di Gatwick del dicembre 2018[172]. A seguito dell'evento e con il fine di limitare episodi di questo tipo, il Regno Unito si è dotato di una strategia nazionale che mira a delineare in maniera netta i limiti di utilizzo dei droni duali e che integra le disposizioni della recente normativa europea.

Considerando che la maggior parte degli sconfinamenti in zone interdette al sorvolo, o delle violazioni di privacy e proprietà privata, è effettuata da singoli cittadini che ignorano le limitazioni della normativa vigente, vi è la necessità di considerare il contrasto della minaccia dei droni duali da diverse prospettive, che partono dalla sensibilizzazione e formazione degli operatori dei droni, per arrivare alle misure di contrasto attivo del drone malevolo. In senso ampio, è quindi possibile intendere il contrasto all'uso illecito dei droni duali come quell'insieme di attività, strumenti e contromisure necessari in primo luogo a ridurre il numero di violazioni delle limitazioni all'uso e, in secondo luogo, a mitigare possibili danni derivanti da un uso malevolo degli UAS. La riduzione delle violazioni di legge per non conoscenza delle stesse è un aspetto piuttosto importante da dover tenere in considerazione, dal momento che andrebbe a ridurre il numero totale di violazioni che vengono effettuate, permettendo una concentrazione migliore e più accurata degli assetti per il contrasto dei droni duali impiegati a fini illeciti.

[170] Per maggiori informazioni si veda il capitolo 2 del presente studio.

[171] National Academies of Sciences, Engineering, and Medicine, *Counter-Unmanned Aircraft System (CUAS) Capability for Battalion-and-Below Operations*, cit.

[172] Per maggiori informazioni si veda il paragrafo 1.1 del presente studio.



ISSN 2280-6164

L'asimmetricità della minaccia è resa evidente anche dalla difficoltà di definire con anticipo se eventuali intromissioni in uno spazio aereo interdetto al sorvolo di droni duali, o operazioni condotte nelle immediate vicinanze di zone sensibili per la sicurezza pubblica, siano di tipo involontario o siano effettuate volontariamente da operatori sofisticati con droni dotati di armi, piuttosto che di altro materiale. La presenza del codice identificativo sul drone è certamente un buono strumento per effettuare l'identificazione elettronica[173] del drone e del suo proprietario, ma la sua presenza non garantisce che il fine di utilizzo del drone sia personale o commerciale e non illecito. Pertanto, ogni violazione della normativa deve essere considerata con attenzione, indipendentemente se si tratta di una minaccia effettiva o potenziale. Allo stato attuale della tecnologia, per poter avere la certezza che il drone non sia dotato di *payload* ostile, è necessario attendere che il drone si trovi abbastanza vicino alle postazioni preposte al contrasto della minaccia, ossia ad una distanza che potrebbe essere troppo ridotta per poterla contrastare efficacemente e limitarne i possibili danni.

Partendo dalle attività di sensibilizzazione e formazione degli operatori, la normativa europea, che sarà pienamente operativa in ogni Stato membro a partire da luglio 2020, introduce l'obbligo di registrazione del drone indipendentemente dalla sua grandezza e dell'ottenimento di un patentino per gli operatori[174]. La formulazione della normativa è un primo passo per limitare la minaccia dei droni duali usati in modo improprio, ma deve essere integrata da altre iniziative e strumenti. La formazione, così come la sensibilizzazione tramite media, o l'installazione di cartellonistica in prossimità delle zone interdette al sorvolo[175], dovrebbero essere parte integrante della strategia di contrasto dell'uso improprio e illecito dei droni che ad oggi è portata avanti tramite l'uso congiunto di sistemi di rilevamento e interdizione.

La tempestività nel rilevamento e nell'individuazione di un drone di piccole dimensioni è una delle caratteristiche principali che deve essere assicurata da un sistema C-UAS efficace. I droni duali che ricadono nelle categorie mini e micro possono essere fatti decollare o essere lanciati da una distanza molto ravvicinata rispetto all'obiettivo, fattore che, se considerato congiuntamente alla loro velocità, causa una significativa riduzione del tempo a disposizione per poter reagire efficacemente.

Il contrasto può avvenire tramite molteplici e differenti modalità, le cui performance cambiano in relazione alle caratteristiche tecniche dei droni. Ciononostante, dal momento che UAS di grandezza compresa tra i 25 kg e i 150 kg sono ancora di

[173] Con identificazione elettronica si fa riferimento alla possibilità di accesso remoto alle informazioni del drone, quali posizione, tipo di modello, nome dell'operatore, numero di registrazione del drone.

[174] EASA, *EU Wide Rules on Drones Published*, 11 giugno 2019, https://www.easa.europa.eu/node/98754.

[175] Stefano Orsi, "Come funziona un sistema anti drone per identificare e bloccare i droni sopra agli aeroporti", in *Dronezine*, 26 aprile 2019, https://www.dronezine.it/76331.

ISSN 2280-6164

difficile reperimento sul mercato, a causa degli elevati costi e delle complessità afferenti alle operazioni di volo, la minaccia maggiore è rappresentata dai droni con peso compreso tra i 250 gr e i 25 kg. Le piccole dimensioni e pesi dei droni si ripercuotono sulla necessità di doversi dotate in primo luogo di sistemi in grado di contrastare droni di piccola taglia, pur sempre tenendo presente la necessità di effettuare ricerche per il contrasto degli APR di medie dimensioni, che potrebbero diventare più accessibili nel prossimo futuro. Altra caratteristica da dover tenere in considerazione nella scelta delle modalità più adeguate al contrasto dei droni duali, è la tipologia dell'ambiente circostante. Il range di soluzioni da poter attuare, a seconda che la minaccia si presenti in ambiente urbano, in zone aeroportuali, in prossimità di infrastrutture critiche, o in teatro operativo, varia considerevolmente.

Nel caso di contrasto in ambiente urbano, un drone malevolo difficilmente potrebbe essere neutralizzato tramite abbattimento compiuto per mezzo di armi convenzionali[176]. Qualora abbattuto con armi cinetiche, la possibile presenza di esplosivo, armi o di materiale CBRN sul drone potrebbe causare danni equiparabili a quelli che l'attore malevolo avrebbe voluto causare. Inoltre, anche qualora il drone non autorizzato o impiegato in maniera malevola non trasportasse cariche pericolose, la sua distruzione in ambiente urbano potrebbe causare danni collaterali su edifici e persone. L'utilizzo di armi ad energia diretta in grado di "vaporizzare" drone e carico, ovvero di danneggiarlo, non è, invece, praticabile per diverse ragioni: potenza assorbita, ingombro, peso, costo, operatività del sistema. Pertanto, a seconda della gravità della minaccia presentata, potrebbe essere meno problematico utilizzare soluzioni riconducibili allo spettro elettromagnetico sia in contesto urbano che in casi in cui la loro vaporizzazione o danneggiamento potrebbe causare danni elevati[177], come ad esempio in prossimità delle infrastrutture critiche o degli aeroporti[178]. In quest'ultimo caso, se un drone sconfina, anche se per errore del pilota, nelle zone aeroportuali o ad esso limitrofe, è necessario dover sventare qualsiasi possibilità di collisione con aerei o elicotteri[179]. Il loro impatto causerebbe danni così elevati, che potrebbero potenzialmente portare anche alla perdita di controllo e caduta del velivolo, con possibile conseguente perdita di vite umane e ingenti danni collaterali[180].

[176] Si veda il capitolo 18 in Randall K. Nichols et al., *Unmanned Aircraft Systems in the Cyber Domain*, 2a ed., Manhattan, New Prairie Press, 2019, https://kstatelibraries.pressbooks.pub/unmannedaircraftsystems/?p=321.

[177] Wayne A. Schroeder, *NATO at Seventy: Filling NATO's Critical Defense-Capability Gaps*, Washington, Atlantic Council, aprile 2019, https://www.atlanticcouncil.org/?p=129320.

[178] Per una disamina delle possibili conseguenze relative ad un attacco alle infrastrutture critiche e agli aeroporti civili, si veda il paragrafo 1.1 del presente studio.

[179] Casi di collisione tra un drone e un altro velivolo si sono già verificati e sono stati oggetto anche di studi sulle possibili ripercussioni dell'urto. Si veda ad esempio: Pamela Gregg, "Risk in the Sky? Impact Tests Prove Large Aircraft Won't Always Win in Collision with Small Drones", in *UDRI News*, 13 settembre 2018, https://udayton.edu/udri/news/18-09-13-risk-in-the-sky.php.

[180] Ashley May, "Drones Can Do Serious Damage to Airplanes, Video Shows", in *USA Today*, 17 ottobre 2018, https://eu.usatoday.com/story/travel/nation-now/2018/10/17/drones-crashing-into-airplanes-quadcopters-damage-video/1657112002.


ISSN 2280-6164

Diverso è il caso del contrasto dei droni in teatro operativo. Soluzioni cinetiche potrebbero trovare più facile applicazione nei teatri operativi in cui si trovano le nostre forze armate, dove, generalmente, la distruzione del drone è una soluzione più praticabile e che genera minori ripercussioni[181]. In questi contesti, il rilevamento deve essere effettuato a distanze maggiori rispetto a quanto non avvenga in contesto urbano – grazie alla possibilità di perimetrare aree più estese e di utilizzare dispositivi con capacità di rilevamento e tracciamento più elevate – e l'abbattimento, se avviene ad una distanza consona dal contingente, comporta danni collaterali trascurabili. In teatro operativo, la valutazione dei danni che possono derivare dall'abbattimento del drone, anche se in prossimità o all'interno del compound, è differente rispetto al caso precedente, essendo essi tollerati se dettati dallo stato di necessità.

Prima di poter procedere all'interdizione del drone ostile è necessario riuscire a rilevarlo e tracciarlo. Con rilevazione si fa riferimento non solo alla capacità di rilevare la presenza del drone, ma anche alla capacità del sistema anti-drone di identificarlo, categorizzarlo come ostile e di rilevare l'eventuale tipologia di minaccia ad esso collegata.

Data la grande varietà di droni disponibili sul mercato in termini non solo di dimensioni, ma anche di caratteristiche tecniche, i sistemi anti-drone, per garantire elevati standard di protezione, dovrebbero essere modulari[182]. La modularità di questi sistemi permetterebbe un loro costante aggiornamento di pari passo con lo sviluppo della tecnologia dei droni duali e permetterebbe di contrastare questi ultimi tramite l'utilizzo e l'integrazione di diverse tecnologie. L'integrazione di diversi sistemi di *detection and tracking* permette di ridurre la possibilità che il sistema generi "falsi negativi" o "falsi positivi". La generazione di "falsi", ossia di errori, inficia la capacità di protezione del sistema anti-drone, dal momento che esso non riesce ad individuare correttamente la minaccia. Con l'espressione falso negativo si fa infatti riferimento all'erronea non individuazione del drone malevolo, mentre, nel caso di falso positivo, il sistema C-UAS individua come drone anche ciò che drone non è, scambiando, ad esempio, un volatile per un SAPR.

Il rilevamento del drone è effettuato tramite diverse tecnologie e la complementarietà dei vari sistemi permette una maggiore capacità di successo anche qualora l'UAS abbia subìto modifiche, o in casi di ridotta visibilità. Un metodo utilizzato convenzionalmente per il rilevamento di velivoli, come il radar, può essere utilizzato anche per rilevare droni duali. In questo caso però, è necessario che il radar sia pensato per il rilevamento di droni o velivoli di piccole dimensioni, con ridotta segnatura, che volano a bassa quota, su aree abitate e a velocità ridotta[183].

[181] Wayne A. Schroeder, *NATO at Seventy*, cit.

[182] Marian Buric, Geert De Cubber, "Counter Remotely Piloted Aircraft Systems", in *MTA Review*, Vol. 27, No. 1, giugno 2017, p. 9-18, https://journal.mta.ro/articole/39/Counter%20Remotely%20Piloted%20Aircraft%20Systems.pdf.

[183] Arthur Holland Michel, *Counter-Drone Systems*, Washington, Center for the Study of the Drone


ISSN 2280-6164

Qualora ciò non avvenisse, il sistema radar non sarebbe in grado di rilevare la loro presenza. Infatti, i radar utilizzati per contrastare aerei militari con equipaggio sono settati su frequenze diverse che servono per il rilevamento di aerei o sistemi di grandi dimensioni, a media e alta quota e a velocità sostenuta[184]. Con lo scopo di rilevare droni ostili possono essere utilizzati anche i sistemi *Counter-Rocket Artillery and Mortar* (C-RAM) che, sebbene inizialmente pensati per altri scopi, sono dotati di caratteristiche tecniche tali da permettere il rilevamento di droni duali[185].

L'utilizzo del solo sistema radar non è tuttavia sufficiente, dal momento che possono esserci diversi fattori che ne inibiscono le capacità di rilevamento. In primo luogo vi è una difficoltà legata alla necessità, in contesto urbano, di dover montare un numero elevato di antenne a quote relativamente alte, per poter permettere una copertura quanto più completa possibile del raggio del radar, ma l'orografia urbana, a differenza di quanto non avvenga per gran parte dei teatri operativi, non favorisce un rilevamento centralizzato. In secondo luogo, la capacità di rilevamento di droni dipende anche dal tipo di materiale con il quale i droni sono costruiti. Una conseguenza della miniaturizzazione dei droni duali è quella di aver portato ad un utilizzo sempre più diffuso di materiali plastici per la costruzione dei droni, materiali che non sono facilmente rilevabili dai sistemi radar[186]. Un ulteriore problema legato all'utilizzo del radar per effettuare la *detection* è rappresentato dall'ampiezza del lobo cieco, ossia della porzione di area, a partire dal radar stesso, che non risulta inclusa nell'area coperta dallo spettro.

Oltre al sistema radar, il rilevamento è effettuato anche tramite sistemi di rilevamento passivi, come sistemi basati su radio frequenze, sistemi elettro-ottici/infrarossi (EO/IR), o acustici.

Con i primi, si ha la possibilità di rilevare la presenza di un drone tramite lo scanning delle frequenze radio generalmente utilizzate per le comunicazioni tra il velivolo e l'operatore. Questo sistema di rilevamento passivo[187] presenta tuttavia la difficoltà nell'individuazione di un drone che sia pilotato tramite l'utilizzo di frequenze radio non autorizzate, o generalmente non impiegate a tal fine. I sistemi che si basano su sensori EO/IR prevedono invece lo sfruttamento della segnatura ottica dei droni. Integrando sensori EO e IR si ha la possibilità di effettuare controllo passivo sia

at Bard College, febbraio 2018, https://dronecenter.bard.edu/counter-drone-systems.

184 Fraunhofer Institute for High Frequency Physics and Radar Techniques FHR, *Detection of Small Drones with Millimeter Wave Radar*, 15 marzo 2019, https://www.fhr.fraunhofer.de/en/businessunits/security/Detection-of-small-drones-with-millimeter-wave-radar.html.

185 Kris Osborn, "Army C-RAM Base Defense Will Destroy Drones", in *Warrior Maven*, 28 November 2017, https://defensemaven.io/warriormaven/land/army-c-ram-base-defense-will-destroy-drones-iERxJDqgmkuuz67ZO4y4ZA.

186 Veselin Demirev, "Drone Detection in Urban Environment – The New Challenge for the Radar Systems Designers", in *Security & Future*, Vol. 1, No. 3, 2017, p. 114-116, https://stumejournals.com/journals/confsec/2017/3/114.

187 Martins Ezuma et al., *Micro-UAV Detenction and Classification from RF Fingerprints Using Machine Learning Techniques*, eprint arXiv:1901.07703, 10 aprile 2019, https://arxiv.org/abs/1901.07703.


ISSN 2280-6164

nelle ore diurne che notturne[188], ma come accade per i sistemi a radio frequenze, è necessario che ci sia un'adeguata VLOS per rilevare la presenza del drone e questo diventa complesso in ambiente urbano. Un ulteriore metodo per il rilevamento droni prevede l'utilizzo di sensori acustici. I suoni registrati dai microfoni di questo sistema vengono confrontati con quelli inseriti in una banca dati contenente i suoni generalmente emessi dai droni. La localizzazione del drone tramite l'utilizzo di questa tecnica risente tuttavia di diversi problemi. La morfologia del territorio sul quale il drone opera, così come l'inquinamento sonoro limitano la capacità dei sensori acustici. Inoltre, la banca dati di riferimento utilizzata potrebbe non essere completa dei suoni emessi dagli ultimi modelli di UAS, rendendo questo sistema inefficace[189]. Questo limite, se da un lato può essere arginato dall'obbligo per le case produttrici di fornire i dati sui suoni emessi dai droni, dall'altro non può essere completamente eliminato se i droni utilizzati vengono modificati artigianalmente. Data la fallibilità sia dei sistemi acustici ed EO, questi due particolari tipi di sistemi di rilevamento potrebbero essere utilizzati per integrare e validare una prima rilevazione effettuata tramite l'uso dei sensori radar e frequenzimetri[190].

I diversi sensori presentano ognuno delle limitazioni che possono essere superate dall'utilizzo congiunto e integrato dei vari sistemi di rilevamento. L'importanza della loro integrazione è duplice. In primo luogo, oltre a subentrare a quei sistemi che poco o difficilmente si adattano all'ambiente circostante, i diversi sistemi di rilevamento sono in grado di coprire distanze diverse tra loro. Queste distanze possono variare dal raggio di qualche km per radar con sensori particolarmente avanzati, fino a distanze ridotte a qualche centinaio di metri per i sensori acustici, passando per la distanza intermedia dei sensori EO/IR. In questo modo, indipendentemente dalla distanza o vicinanza all'obiettivo dalla quale il drone decolla o è lanciato, l'uso congiunto dei diversi sistemi assicura una maggiore percentuale di successo nell'attività di rilevamento. In secondo luogo, nel caso di attacchi da sciami di droni provenienti da diversi punti, si ha la necessità di poter attuare ingaggi multipli non solo al fine del rilevamento, ma anche nelle fasi successive del tracciamento e contrasto dei droni.

Una volta rilevata la presenza di droni ostili, è necessario passare al loro tracciamento e interdizione. Il tracciamento del drone è necessario a definire se l'UAV, che si trova in zone interdette al sorvolo o in prossimità di punti di interesse strategici, possa rappresentare un'effettiva minaccia e aiuta a determinare la tipologia di reazione da dover attuare. Avere contezza della rotta del drone, della velocità di avvicinamento e del numero di target potenziali, possibile solo grazie all'impiego di diversi sistemi di *detection*, aiuta l'operatore preposto al contrasto dei droni duali ad attuare il tipo di interdizione più appropriato al livello della

188 FLIR, *What Is EO/IR?*, 26 luglio 2019, https://www.flir.com/discover/rd-science/what-is-eoir.

189 Arthur Holland Michel, *Counter-Drone Systems*, cit.

190 Federal Aviation Administration (FAA), *Unmanned Aircraft System Detection - Technical Considerations*, 26 marzo 2019, https://www.faa.gov/airports/airport_safety/media/Attachment-3-UAS-Detection-Technical-Considerations.pdf.


ISSN 2280-6164

minaccia e all'ambiente circostante[191]. Il livello di invasività delle diverse tecniche di interdizione varia in relazione al grado di potenzialità negativa della minaccia. In altri termini, maggiore è il rischio di arrecare danni a persone e cose, maggiore sarà l'invasività dei sistemi di contrasto, che possono essere suddivisi in sistemi non cinetici e sistemi cinetici.

Tra i sistemi non cinetici, il livello minore di interdizione attuabile è rappresentato dai sistemi di *geo-fencing*, ossia da sistemi, integrati direttamente sul drone, che impediscono all'UAV di entrare in aree di volo interdette. Il *geo-fencing* può essere un valido supporto all'interdizione di intromissioni involontarie, ma non dà nessuna garanzia di successo in caso di intromissioni volontarie effettuate da operatori sofisticati. Sono infatti presenti sul mercato delle soluzioni software che permettono di eliminare il sistema di *geo-fencing*, di fatto rendendo questa soluzione impraticabile[192].

Un ulteriore metodo C-UAS non cinetico è dato dall'interdizione del drone tramite l'uso di un *jammer*, ossia di un disturbatore di frequenze radio. L'azione di *jamming* prevede l'intromissione nella trasmissione del segnale radio o GPS tra il comando e controllo (C2) del drone e il velivolo. Ad interruzione del segnale radio, generalmente il drone effettua il *safe-return-home*, anche se ci possono essere casi in cui questa funzione non sia prevista per il velivolo sottoposto a questo tipo di interdizione, o che le coordinate impostate per questa funzione siano esattamente quelle del bersaglio verso il quale dirigersi[193]. In questi casi l'impiego del *jammer* potrebbe risultare non efficace o addirittura controproducente. È probabile, infatti, che il drone utilizzato per compiere attacchi sia dotato di rotte di volo pre-impostate, che permetterebbero al drone di proseguire il volo senza la necessità del mantenimento del *data link* con la stazione di controllo tramite le radio frequenze. È, inoltre, possibile che il drone abbia subìto modifiche inerenti alle modalità di reazione alla perdita della comunicazione con il pilota e che reagisca con la caduta al suolo all'interruzione del segnale radio[194]: in contesti urbani, questa possibilità costringerebbe alla ricerca di altre soluzioni.

Un altro problema del sistema di *jamming* è dato dall'emissione di un'elevata potenza elettromagnetica, che può causare ripercussioni all'ambiente circostante. Gli attuali sistemi permettono il direzionamento dell'onda elettromagnetica, proprio per ridurre al minimo possibili interferenze sui sistemi di comunicazione telefonica e sul corretto funzionamento di apparecchiature elettroniche che dovessero trovarsi in prossimità del raggio d'azione del *jammer*. Ciononostante, l'uso di tali sistemi nelle zone aeroportuali potrebbe non esse attuabile, dal momento che le

191 Marian Buric, Geert De Cubber, "Counter Remotely Piloted Aircraft Systems", cit.

192 Ibid.

193 Arthur Holland Michel, *Counter-Drone Systems*, cit.

194 Daniela Pistoia, "Sensors and Effectors against an Asymmetric Threat, Detecting and Neutralizing Micro-Drones", in *JAPCC Journal*, No. 25, inverno 2017/2018, p. 81-86, https://www.japcc.org/detecting-and-neutralizing-mini-drones.


ISSN 2280-6164

onde elettromagnetiche del sistema C-UAS potrebbero causare l'interruzione delle operazioni del sistema di gestione del traffico aereo[195]. Inoltre, nel caso di sciami di droni, il direzionamento dell'onda elettromagnetica potrebbe rappresentare più un problema al contrasto che non un vantaggio in quanto all'aumentare del numero di droni da dover contrastare, anche la quantità di energia necessaria al contrasto aumenterebbe. Per di più, nel caso di utilizzo di *jammer* con onda direzionata, vi sarebbe l'esigenza di utilizzare diversi *jammer* contemporaneamente e, quindi, di impiegare un numero maggiore di operatori.

Tra le forme di contrasto non cinetico rientra anche lo spoofing del segnale GPS. Lo spoofing è una tecnica attraverso la quale vengono inviati al drone dei falsi segnali GPS[196]. In altre parole, questo tipo di interdizione consiste nel far credere all'UAV che la sua posizione sia diversa rispetto a quella reale. Il problema di questo tipo di soluzione è però duplice. Da un lato esso può essere utilizzato solo se il drone basa la sua navigazione sul sistema satellitare; dall'altro il drone potrebbe avere dei sistemi di protezione del segnale GPS (*anti-spoofing*) o avere capacità di AI tali da permettere al drone di comprendere l'inganno dello spoofing e continuare la propria missione.

I sistemi di interdizione non cinetici sono tanto più efficaci quanto maggiore è la qualità dei sensori che utilizzano, ma il costante sviluppo tecnologico impone una loro continua evoluzione. I sistemi non cinetici descritti in precedenza non sono efficaci se i droni duali basano la loro navigazione su sistemi INS o VIO. In questi casi, gli UAV sono immuni alle false trasmissioni e al disturbo elettronico e rendono questa tipologia di risposta inappropriata.

Tutte le problematiche descritte in precedenza dimostrano quanto gli strumenti di contrasto afferenti esclusivamente al campo elettromagnetico possano risultare inefficaci. Pertanto, si rende necessaria l'integrazione di questi sistemi con altri tipi di risposta, come quelli cinetici.

Nel considerare la risposta cinetica, va sottolineata l'importanza dell'ambiente circostante e dell'entità di eventuali danni collaterali. La ponderazione di questi aspetti, soprattutto se ci si trova in zone urbane o in prossimità di assembramenti di persone, potrebbe non permettere l'impiego di determinate contromisure. Oltre a ciò, riflessioni di carattere economico potrebbero precludere l'utilizzo di alcuni sistemi piuttosto che permetterne altri, pur sempre tenendo presente che ogni sistema di risposta cinetica presenta delle criticità.

[195] Arthur Holland Michel, *Counter-Drone Systems*, cit.

[196] Luca Mella, "Attacchi ai sistemi GPS: cosa sono e come difendersi", in *Cybersecurity360*, 2 settembre 2019, https://www.cybersecurity360.it/?p=33618.


ISSN 2280-6164

Tra le soluzioni cinetiche è possibile considerare, in via potenziale, anche l'utilizzo di tradizionali sistemi di difesa aerea. L'utilizzo di questi sistemi[197] è stato però finora piuttosto contenuto dato il costo elevato che li caratterizza e la sproporzionalità della risposta ad un attacco effettuato da un drone di piccole dimensioni. Questo tipo di soluzione risulta poco sostenibile economicamente, sebbene possibile. Tra le altre armi cinetiche è possibile impiegare fucili, sistemi laser, fucili ad aria compressa, munizioni a scoppio programmabile.

L'abbattimento del drone ostile per mezzo di fucili[198] è tra i sistemi di contrasto meno costosi. Tuttavia, è necessario tenere in considerazione il tipo di materiale di cui è composto il drone – generalmente plastiche dure e affusolate – per decidere la tipologia di munizione più appropriata che un tiratore esperto può utilizzare. La buona riuscita dell'abbattimento del drone tramite questo tipo di risposta necessita di particolari competenze tecniche del tiratore e di consistenti processi addestrativi.

Un ulteriore sistema C-UAS è rappresentato dall'utilizzo di raggi laser ad alta intensità. Questo sistema, caratterizzato da costi piuttosto contenuti[199], può essere mobile e può avere una capacità di risposta anche prolungata. Infatti, oltre alla carica di cui il laser è dotato, è generalmente possibile aumentare la capacità del laser abbinandolo ad un generatore di energia. Ciò aumenta le possibilità di buona riuscita dell'operazione di contrasto, dal momento che il raggio del laser, per poter ottenere gli effetti sperati, deve essere direzionato in maniera continuativa sul bersaglio, mantenendo l'ingaggio per diversi secondi[200]. Questa necessità riduce tuttavia il grado di successo del sistema per diversi motivi. Innanzitutto, qualora dovessero esserci delle condizioni meteorologiche avverse, il raggio laser potrebbe non raggiungere l'obiettivo o riflettersi altrove. In secondo luogo, il materiale di cui è composto il drone influenza il tempo necessario all'abbattimento dello stesso[201]. Un ulteriore fattore che influenza la buona riuscita dell'operazione di contrasto è il movimento del drone, dal momento che potrebbe essere difficoltoso riuscire a mantenere il contatto diretto del laser. Questa necessità prevede un'ottima capacità dell'operatore preposto all'attività di contrasto che, tuttavia, potrebbe non essere sufficiente se, ad esempio in contesto urbano, il drone volasse nel cosiddetto canyon cittadino e, quindi, fuori dalla VLOS.

[197] Judah Ari Gross, "To Rule Out a Russian Link, IDF Waited 16 Minutes Before Downing Syrian Drone", in *Times of Israel*, 11 luglio 2018, https://www.timesofisrael.com/to-rule-out-a-russian-link-idf-waited-16-minutes-before-downing-syrian-drone.

[198] I fucili generalmente utilizzati per questo scopo sono quelli di calibro 12mm.

[199] Anatolii S. Dudush et al., "State of the Art and Problems of Defeat of Low, Slow, and Small Unmanned Aerial Vehicles", in *Advances in Military Technology*, Vol. 13, No. 2, 2018, p. 157-171, http://aimt.unob.cz/articles/18_02/1233.pdf.

[200] "Raytheon Delivers C-UAS Laser System to USAF", in *Shephard News*, 23 ottobre 2019, https://www.shephardmedia.com/news/landwarfareintl/raytheon-delivers-c-uas-laser-system-usaf.

[201] Anatolii S. Dudush et al., "State of the Art and Problems of Defeat ...", cit.

© 2020 IAI ISSN 2280-6164 DOCUMENTI IAI 20 | 04 - MARZO 2020

Se il drone si trova a distanza ravvicinata, è possibile utilizzare anche fucili ad aria compressa. Questi fucili, dalla forma che richiama un cannone portatile, sparano una rete, alla quale può essere abbinato un paracadute che forza il drone "catturato" a planare al suolo[202]. Il range entro il quale è possibile utilizzare questo tipo di soluzione varia da sistema a sistema, ma generalmente essi sono dotati di un dispositivo che calcola la distanza presente tra il drone e l'operatore, permettendo a quest'ultimo di valutare la fattibilità dell'impiego di questo tipo di C-UAS. Tuttavia, il lancio della rete può risentire delle condizioni atmosferiche nelle quali l'operatore si trova a dover agire e non può essere utilizzato se tra il drone e l'operatore preposto al suo contrasto sono presenti ostacoli fisici.

Un'ulteriore possibilità di contrasto dei droni è data dall'utilizzo di fucili dotati di munizioni a scoppio programmabile. Queste munizioni possono essere programmate elettronicamente per esplodere dopo aver percorso una certa distanza, o in prossimità del bersaglio[203]. La caratteristica principale di questo tipo di soluzione C-UAS è rappresentata dal fatto che queste munizioni offrono la possibilità di adeguare il numero e la tipologia di carica in relazione all'obiettivo. Inoltre, rispetto all'utilizzo di normali fucili, l'impiego di munizioni a scoppio programmabile aumenta la probabilità di contrasto dell'UAV. La carica, esplodendo in prossimità del drone ostile lancia un numero elevato di proiettili causando impatti multipli con il bersaglio, aumentando le possibilità di centramento. Ogni soluzione C-UAS è una soluzione parziale e la possibilità di utilizzo varia a seconda di diversi fattori, che possono essere legati alla caratteristica della minaccia, alla sua effettiva pericolosità, all'ambiente circostanze e alle condizioni atmosferiche. Pertanto, nessun sistema di contrasto è totalmente efficace, ma bisognerebbe pensare all'integrazione dei vari sistemi per assicurare la flessibilità necessaria ad un contrasto efficace. Inoltre, il rapido avanzamento tecnologico nel campo dei droni causa la necessità di dover essere costantemente alla frontiera tecnologica in ambito C-UAS e di avere la capacità di prevedere le caratteristiche dei droni di nuova generazione e il loro potenziale utilizzo al fine di non trovarsi a dover fronteggiare minacce per le quali non siano già state elaborate apposite contromisure.

In parte per rispondere a quest'esigenza, si sta sperimentando l'utilizzo di droni e di sciami di droni come misure di contrasto. La convenienza derivante dall'utilizzo dei droni a questo scopo risiede nella loro modularità, nonché nel loro costo più contenuto. A seconda della tipologia di scopo o di bersaglio della missione nella quale vengono impiegati, i droni possono essere integrati, ad esempio, con sistemi di rilevamento, piuttosto che con armi anti-drone, cinetiche e non, permettendo il contrasto di differenti tipologie di minacce[204]. Il loro utilizzo può essere impiegato anche come supporto all'attività di rilevamento della minaccia compiendo sia

[202] "Mobile Drone-Catcher [DSEI19D4]", in *Jane's 360*, 13 settembre 2019, https://www.janes.com/article/91202.

[203] Anatolii S. Dudush et al., "State of the Art and Problems of Defeat ...", cit.

[204] Zachary Kallenborn, "The Era of the Drone Swarm Is Coming, and We Need to Be Ready for It", in *Modern War Institute Commentary & Analysis*, 25 ottobre 2018, https://mwi.usma.edu/?p=9924.


ISSN 2280-6164

azioni di sorveglianza che di *early warning* in caso di presenza di droni non autorizzati nel perimetro di loro pertinenza. Sono già molti gli impieghi di droni di piccole dimensioni a questi scopi sia da parte di agenti di pubblica sicurezza[205] che da parte di aziende o attori privati[206].

Oltre alla fase di *detection* del drone ostile, i droni possono essere impiegati per categorizzare la tipologia della minaccia tramite l'invio di immagini del drone ostile riprese a distanza ravvicinata, o inviando dati specifici sulle caratteristiche tecniche e di *payload* del drone ostile. Grazie all'installazione di particolari sistemi di rilevamento di esplosivi o di componenti CBRN un drone così configurato è in grado di inviare i relativi dati alla stazione di C2[207]. Ciò permetterebbe di comprendere con maggiore anticipo la natura della minaccia e, di conseguenza, la tipologia di risposta da attuare[208]. In questo contesto, è da dover essere presa in considerazione la possibilità che droni o sciami di droni possano essere impiegati anche come droni kamikaze o essere dotati di armi cinetiche per l'abbattimento del proprio bersaglio. In uno scontro di questo tipo, che, sebbene possa sembrare futuristico, è potenzialmente attuabile anche con l'attuale tecnologia disponibile, possono scaturire danni collaterali dal loro impatto o scontro. Nel contrasto ai droni duali, la sfida non è rappresentata solamente dalla necessità di dover trovare dei sistemi efficaci di rilevamento e interdizione, ma anche dalla capacità dell'utilizzatore. Infatti, mentre sono già disponibili sul mercato sistemi C-UAS tecnologicamente avanzati, meno diffusi sono gli operatori effettivamente in grado di utilizzare con precisione questi sistemi, carenza che è rilevata anche a livello regionale NATO[209]. La formazione del personale per il contrasto dei droni duali è un aspetto fondamentale, non solo perché ci sarà una necessità crescente di personale specializzato, ma anche perché le tempistiche necessarie per poter attuare il tipo di risposta più appropriato è in netta diminuzione rispetto a quanto non avvenga per gli altri sistemi di difesa.

Per questo motivo la creazione di un sistema C-UAS quanto più automatizzato e integrato possibile è da preferire a soluzioni che prevedono la loro attivazione tramite un ruolo più pronunciato del man-in-the-loop. Un sistema che sia in grado di effettuare le funzioni di *detection and tracking* ad ampio spettro e in modo costante è indispensabile per avere una protezione continua degli assetti

[205] "Droni a supporto delle Forze di Polizia", in *Drone Blog News*, 23 ottobre 2019, https://www.droneblog.news/droni-a-supporto-delle-forze-di-polizia.

[206] Danilo Scarato, "ENAC autorizza 'ad hoc' i voli del drone autonomo/automatico Percepto sulla centrale ENEL di Civitavecchia", in *Quadricottero News*, 3 giugno 2019, https://www.quadricottero.com/2019/06/enac-autorizza-ad-hoc-i-voli-del-drone.html.

[207] "Explosives Detection: The World's First Sniffer Drone", in *Army Technology*, 31 gennaio 2017, https://www.army-technology.com/?p=18120.

[208] Mandeep Singh, "Drone Swarms: The Emerging Air Threat", in *Indian Defence Review*, Vol. 33, No. 4, ottobre-dicembre 2018, p. 33-37, http://www.indiandefencereview.com/?p=46121.

[209] European Air Group (EAG), Joint Air Power Competence Centre (JAPCC), "The Implications for Force Protection Practitioners of Having to Counter Unmanned Systems. A Think-Piece", in *JAPCC White Papers*, 2019, https://www.japcc.org/portfolio/counter-uas-think-piece.


ISSN 2280-6164

strategici nazionali o in occasione di grandi eventi, così come per la protezione delle truppe e dei mezzi dispiegati nei teatri operativi. Automatizzare la parte di *detection and tracking* non necessariamente porta all'esclusione del fattore umano nel *sensor to shooting cycle*, anzi ne amplifica il ruolo. Con *sensor to shooting cycle* si fa riferimento al processo attraverso il quale un obiettivo, in questo caso un drone potenzialmente minaccioso, viene rilevato, identificato, reso prioritario e infine presentato all'operatore il quale ha l'onere di dover decidere quale tipo di reazione mettere in atto. In questo ciclo, il fattore umano è gravato dalla responsabilità di dover efficientare e velocizzare la propria risposta al dato fornito dall'apparecchiatura a suo supporto[210].

In questo processo, dato l'avanzamento tecnologico esponenziale, la prontezza dell'intervento umano è determinante. Per comprendere l'importanza di un *sensor to shooting cycle* il più lineare e celere possibile, basti pensare che la crescente velocità di crociera dei droni duali implica tempi di reazione molto più ristretti. Tempi che, per essere efficaci, devono essere largamente inferiori ai 60 secondi. Ciò implica anche tempi di autorizzazione a procedere per i piloti che mal si integrano con le tradizionali procedure.

Un'ulteriore problematica che potrebbe presentarsi nell'ambito C-UAS riguarda le differenti modalità e standard presenti a livello internazionale. Dal momento che lo sviluppo dei sistemi C-UAS ha sperimentato un'impennata negli ultimi anni, non si è ancora arrivati né a livello nazionale, né internazionale, alla definizione di standard condivisi che regolino le modalità di impiego e le regole di ingaggio per l'uso dei sistemi anti-drone.

### *3.2 Il contesto NATO*

Il contrasto della minaccia rappresentata da un possibile uso illecito dei droni duali è un argomento che ha interessato la NATO sin dall'inizio degli anni 2000 e che continua ad essere oggetto di attenzione e ricerca per arrivare alla definizione di standard, procedure e modalità di contrasto condivise. La possibilità di utilizzo di droni di piccole dimensioni da parte di gruppi terroristici strutturati o di singoli individui è infatti sempre più consistente, anche in virtù della velocità del loro sviluppo tecnologico. Questo fattore, inoltre, apre sempre di più le porte all'eventualità che, in un futuro prossimo, questo tipo di droni, così come il loro utilizzo in sciami, diventi parte integrante degli scontri convenzionali.

All'interno della NATO sono in corso studi e sperimentazioni che porteranno gli Alleati ad essere dotati di capacità di contrasto sempre più sofisticate e performanti, in grado di garantire un'elevata probabilità di successo. Benché finora gli sforzi siano stati frammentati, le varie iniziative portate avanti in seno all'Alleanza costituiscono delle valide opportunità di confronto sia tra gli Stati, per la definizione

[210] Sydney J. Freedberg, "Exclusive: Pentagon's AI Problem Is 'Dirty' Data: Lt. Gen. Shanahan", in *Breaking Defense*, 13 novembre 2019, https://breakingdefense.com/?p=83723.


ISSN 2280-6164

delle priorità nazionali e dell'intera NATO, sia sul versante industriale, per meglio comprendere i requisiti richiesti.

Fino alla fine del 2018, lo studio dei droni duali e delle capacità necessarie al loro contrasto è stato effettuato da una varietà di gruppi e agenzie in capo alla NATO. Ad esempio, all'interno del Programma di lavoro per la difesa contro il terrorismo (Defence Against Terrorism Programme of Work, DAT POW)[211], nella sezione riguardante la protezione e la sopravvivenza delle forze c'è un'azione dedicata alla dimostrazione della capacità di contrasto di UAS LSS con armi non letali[212]. Nello stesso anno, il DAT POW ha sponsorizzato il NATO Non-Lethal Technology Exercise Counter-UAS (NNTEX-18C), ossia una dimostrazione dello stato dello sviluppo tecnologico per il contrasto dei droni di piccole dimensioni con armi non letali, che è stata il frutto di una collaborazione iniziata nel 2015 tra NATO, Stati Uniti e alcuni degli Alleati[213]. La dimostrazione è stata solo una parte del lavoro svolto, che ha interessato anche l'analisi preventiva di quelle che possono essere le necessità operative delle forze armate. In particolare, le riflessioni hanno tenuto conto sia del costante sviluppo tecnologico dei droni duali, che della necessità di avere soluzioni di contrasto non letali e con limitati danni collaterali, soprattutto nel caso in cui dovessero essere utilizzate in contesti urbani. La dimostrazione ha interessato diversi scenari tra cui anche attacchi CBRN in contesti con un'alta concentrazione di persone o contro *high level target*.

L'interesse dimostrato dalla NATO verso tecnologie preposte al contrasto dei droni è evidenziato anche dall'attività svolta dal programma Science for Peace and Security (SPS)[214] o quelle del Joint Air Power Competence Center (JAPCC)[215]. Il JAPCC ha istituito nel 2019 un Counter-UAS Focus Group (CUASFG) con l'obiettivo di mettere insieme esperti di vari settori e arrivare, entro il 2020, al completamento di uno studio che tenga in considerazione le difficoltà delle agenzie di law enforcement in materia di contrasto dei droni[216]. Infatti, una delle criticità riscontrate nel contrasto ai droni di piccole dimensioni riguarda i diversi approcci normativi e procedurali, laddove presenti, tra i vari Stati membri.

[211] NATO, *Defence Against Terrorism Programme of Work (DAT POW)*, 3 luglio 2018, https://www.nato.int/cps/en/natohq/topics_50313.htm.

[212] Con armi non letali si fa riferimento a soluzioni che causano o possono causare solo danni collaterali limitati. Nel caso specifico del C-UAS, questo fa riferimento a *jammer*, alcune delle soluzioni cinetiche e soluzioni di cattura a rete. Si veda NATO Industrial Advisory Group, *Proposals for Advisory Studies by the NIAG in Budget Year 2020*, 16 ottobre 2019, Annex 2, p. 13-14, https://www.bdsv.eu/über-uns/nato-industrial-advisory-group.html?file=files/ueber-uns/niag/AC_259-D(2019)0029_INV_2020_STUDIES.pdf.

[213] United States Marine Corps, *NATO Non-Lethal Technology Exercise Counter-UAS (NNTEX-18C)*, 7 dicembre 2018, https://www.dvidshub.net/webcast/17908.

[214] NATO SPS, *Special Call for Proposals on Security-Related Advanced Technologies*, 18 ottobre 2019, https://www.nato.int/cps/en/natolive/87129.htm.

[215] Il JAPCC è stato istituito da un MoU ed è sponsorizzato da 16 Paesi NATO. Per maggiori informazioni si veda il sito ufficiale: https://www.japcc.org.

[216] André Haider, "A Comprehensive Approach to Countering Unmanned Aircraft Systems", cit.


ISSN 2280-6164

Il supporto del JAPCC è stato anche richiesto dal Quartier generale supremo delle potenze alleate in Europa (Supreme Headquarters Allied Powers Europe, SHAPE) nella sua veste di Chair della NATO Force Protection Working Group (FPWG) nel 2017. In tale contesto, il supporto del centro è stato richiesto per analizzare le possibili implicazioni sulle modalità di risposta alla minaccia, derivanti da un uso illecito di droni duali e arrivare alla definizione di un requisito operativo urgente di risposta alle crisi (*Crisis Response Urgent Operational Requirement*, CUR)[217]. Il lavoro del JAPCC, con il fine di coordinare al meglio le necessità degli attori a vari livelli, ha un approccio complessivo e non si limita al solo dominio aereo, ma interessa i sistemi autonomi in generale. Infatti, è prevedibile che la minaccia, sebbene venga intesa al momento come proveniente principalmente dal dominio aereo, possa interessare anche gli altri domini negli anni a venire. Inoltre, viste le conseguenze che una minaccia aerea può causare, risulta necessaria la cooperazione non solo delle varie agenzie NATO, ma anche tra i vari Alleati, nonché l'utilizzo di diversi sistemi di contrasto che dovrebbero essere definiti, anche al fine di una loro inclusione nel NATO Defence Planning Process (NDPP).

Il JAPCC supporta altresì le attività portate avanti dal NATO Science and Technology Organisation (STO) Study SCI-301 per la formulazione di raccomandazioni per un sistema C-UAS integrato di seconda generazione[218].

Nonostante lo sforzo profuso sia stato considerevole negli anni passati, un *Practical Framework* tra i vari gruppi e agenzie NATO è stato istituito solo di recente. La decisione inerente alla creazione del *Practical Framework* è stata presa dal Consiglio e reiterata dai ministri della Difesa dei 29 Paesi NATO riuniti durante il summit di febbraio 2019[219]. Il NATO C-UAS *Practical Framework*, guidato dall'Emerging Security Challenges Division (ESCD) e operando insieme alla Defence Investment Division afferente al NATO International Staff, avrà l'obiettivo di porsi come una piattaforma di cooperazione comune, adottando un approccio quanto più comprensivo e trasversale possibile, per mezzo del NATO C-UAS Working Group[220]. L'ESCD è anche supportata dal Supreme Allied Comand Transformation (ACT) che ha inserito lo sviluppo di capacità C-UAS per droni di piccole dimensioni nell'agenda di sviluppo per la guerra (*warfare development agenda*) e nel programma di lavoro 2019-2020 per lo sviluppo e la sperimentazione (Concept Development and Experimentation – CD&E)[221]. Tra gli scopi del programma di lavoro in ambito C-UAS c'è la definizione di un manuale[222] per arrivare ad una comprensione condivisa della minaccia, delle

[217] EAG, JAPCC, "The Implications for Force Protection Practitioners...", cit.

[218] JAPCC, *Annual Report 2018*, gennaio 2019, https://www.japcc.org/portfolio/annual-report-2018.

[219] NATO Air and Missile Defence Committee, *Countering Class I Unmanned Aerial Systems. Practical Framework Outline* (AC/336-D(2018)0014-REV1), 2018.

[220] André Haider, "A Comprehensive Approach to Countering Unmanned Aircraft Systems", cit.

[221] Il CD&E promuove un approccio collaborativo di definizione e sviluppo delle capacità militari. Per maggiori informazioni si veda il sito di NATO ACT: *International Concept Development & Experimentation Conference*, https://www.act.nato.int/cde-conf.

[222] NATO Allied Command Transformation, *Countering Small Unmanned Aircraft Systems (C-sUAS). Fact Sheet*, giugno 2019, https://www.act.nato.int/images/stories/media/opex/2019_CsUAS.pdf.


ISSN 2280-6164

sue ripercussioni sulla popolazione e sugli aspetti militari e di *law enforcement* ad essa connessi. Il manuale raggrupperà i risultati dei lavori del NATO ESCD e del NATO C-sUAS (Countering Small Unmanned Aircraft Systems).

È da notare che, al momento, la NATO non ha incluso la capacità di contrasto dei droni duali tra quelle incluse nel NDPP[223], sebbene il loro sviluppo permanga tra i principali obiettivi capacitivi che l'Alleanza si è posta. L'inserimento dei sistemi C-UAS all'interno dell'NDPP è importante per promuovere uno sviluppo più armonizzato delle capacità di contrasto dei droni duali tra i Paesi membri della NATO, nonché per arrivare a delle tempistiche maggiormente definite.

L'inclusione del C-UAS nel NDPP è possibile, ma deve seguire delle tempistiche ben delineate. Infatti, i cinque cicli[224] di cui è composto hanno durata di quattro anni ognuno e, per includere il C-UAS nell'attuale processo di pianificazione, è necessario che tra la fine del 2020 e l'inizio del 2021 la fase della definizione dei requisiti necessari per un C-UAS efficace sia pronta per essere integrata nella fase di definizione dei requisiti capacitivi all'interno del processo[225]. Un'eventuale inclusione in corso d'opera è possibile grazie alla previsione da parte degli organi NATO della natura mutevole e altamente tecnologica che caratterizza le capacità di difesa attuali e alla conseguente possibilità di modificare e aggiungere determinate capacità prevista nei documenti che regolano il funzionamento del NDPP[226]. Lo sforzo del gruppo di lavoro NATO è particolarmente complesso e per arrivare ad una definizione dei requisiti è previsto che le forze impiegate nelle operazioni a rotazione come quelle della missione Resolute Support o nell'Enhanced Forward Presence testino le attuali capacità[227].

Ulteriori test che potranno essere utilizzati a complemento delle attività preparatorie per l'inclusione del C-UAS nel processo dell'NDPP sono quelli svolti nell'ambito del programma SET-260 della NATO STO[228]. Questo programma ha una durata triennale e si pone l'obiettivo di valutare tecnologie EO/IR per il rilevamento di droni entro il 2021. A differenza di altre iniziative svolte in ambito NATO, i test condotti dal SET-260 sono stati svolti in contesto urbano, in previsione di un loro utilizzo in tali contesti.

[223] EAG, JAPCC, "The Implications for Force Protection Practitioners...", cit.

[224] Definire una guideline politica, determinare i requisiti, definire i target, facilitare l'implementazione delle attività necessarie, esaminare i risultati. Si veda: NATO, *NATO Defence Planning Process*, 28 giugno 2018, https://www.nato.int/cps/en/natohq/topics_49202.htm.

[225] NATO Air and Missile Defence Committee, *Countering Class I Unmanned Aerial Systems*, cit.

[226] NATO, *NATO Defence Planning Process*, cit.

[227] NATO Air and Missile Defence Committee, *Countering Class I Unmanned Aerial Systems*, cit.

[228] "NATO Tests Passive and Active Tracking of Small UAVs in Urban Environments", in *Unmanned Airspace*, 14 agosto 2019, https://www.unmannedairspace.info/?p=5361.


ISSN 2280-6164

Oltre a cercare di definire i requisiti operativi e tecnici dei sistemi di rilevamento e contrasto dei droni duali, la NATO, tramite la NATO Communications and Information (NCI) Agency sta provvedendo all'acquisizione di capacità C-UAS[229] in capo alla NATO, per testare e sviluppare ulteriormente le capacità di contrasto in teatri operativi.

### *3.3 Il contesto europeo*

A livello europeo sono state avviate una serie di iniziative con un duplice scopo. Da un lato, gli sforzi sono stati rivolti alla definizione di un quadro regolatorio completo per un corretto utilizzo dei droni in vista di una loro integrazione nei sistemi di gestione del traffico aereo, mentre dall'altra l'UE si è mossa al fine di standardizzare l'approccio e le procedure per l'implementazione dei sistemi C-UAS sia in contesti civili che in ambito militare. Da un punto di vista civile, infatti, il sempre crescente numero di UAS duali porterà ad un loro crescente utilizzo da parte di industrie, professionisti, e singoli utilizzatori. Pertanto, la loro integrazione nello spazio aereo civile sarà uno degli aspetti da dover considerare e normare con la dovuta attenzione per evitare che il loro utilizzo lecito possa inficiare la sicurezza di cittadini, proprietà private e dell'aviazione civile[230]. A conferma di ciò, un gran numero di iniziative a livello europeo è volto a definire standard per le operazioni di volo di UAV, nell'ottica di una loro integrazione crescente nello spazio aereo civile[231].

L'attenzione posta a livello politico sulla necessità di avere le capacità di contrasto dei droni duali è molto alta. Nell'ottobre 2019 la Commissione europea ha organizzato una conferenza internazionale a cui hanno partecipato gli Stati membri, le industrie, i principali stakeholder, organizzazioni internazionali operanti nel settore e Paesi terzi. All'iniziativa è poi seguito un incontro a livello UE per meglio considerare il contrasto della minaccia posta da un uso malevolo dei droni duali[232]. Dall'incontro è emersa la necessità per l'UE e i suoi Stati membri di dotarsi di capacità di rilevamento continuo, di arrivare alla formulazione di procedure di valutazione del rischio armonizzate, di aumentare la resilienza cibernetica delle infrastrutture critiche e di sviluppare capacità di contrasto che siano alla frontiera dell'innovazione tecnologica. Per poter raggiungere tali obiettivi, l'Europa riconosce la necessità di incrementare le attività in corso e di crearne di nuove, mettendo anche a disposizione la nuova European Drone Investment – Advisory Platform[233].

[229] NATO NCI, *NCI Agency Releases Invitation for Bid for Counter-Drone Capability*, 1 luglio 2019, https://www.ncia.nato.int/NewsRoom/Pages/20190701-NCI-Agency-releases-Invitation-for-Bid-for-counter-drone-capability.aspx.

[230] Per una breve panoramica sul quadro normativo attuale si veda il capitolo 2 del presente studio.

[231] A tal proposito si vedano le attività del SESAR Joint Undertaking: *Full Speed Ahead for Drone Traffic Integration: SESAR Establishes U-space Demonstrators across Europe*, 19 ottobre 2018, https://www.sesarju.eu/node/3091.

[232] Commissione europea, *Commission Hosted a High-Level International Conference on Countering the Threats Posed by Drones*, 7 novembre 2019, https://europa.eu/!rc44rm.

[233] Commissione europea, *Drones: European Commission Hosts an International Conference*


ISSN 2280-6164

Tra le attività promosse in ambito civile per il rilevamento dei droni duali, l'Organizzazione europea per le Apparecchiature dell'Aviazione civile (European Organisation for Civil Aviation Equipment, EUROCAE) ha recentemente creato il Working Group 115 on Counter-UAS[234] che si pone l'obiettivo di definire il livello minimo di capacità di rilevamento di un sistema C-UAS in ambienti aeroportuali e di definire un *action plan*. I lavori del WG-115 dovrebbero portare alla definizione di standard condivisi per i sistemi C-UAS che potrebbero essere applicati anche in un contesto urbano, per svolgere principalmente operazioni di rilevamento e sorveglianza[235]. L'approccio promosso dall'EUROCAE intende arrivare alla formulazione di requisiti tecnici dei sistemi C-UAS che permettano quanto più possibile alla comunicazione e navigabilità aeree di non subire variazioni rilevanti e che tengano in considerazione anche gli avanzamenti in ambito NATO per assicurare l'interoperabilità dei sistemi[236].

Per ciò che concerne lo sviluppo delle capacità di contrasto, l'UE ha supportato diverse iniziative che rientrano tra le azioni della Commissione europea e tra quelle della Cooperazione strutturata e permanente (Permanent Structured Cooperation, PeSCo)[237].

Tra le iniziative in capo alla Commissione, quelle sul C-UAS ricadono sia tra i progetti Horizon 2020, che tra quelli del Programma europeo di sviluppo del settore industriale della difesa (European Defence Industrial Development Programme, EDIDP). Il progetto Advanced hoListic Adverse Drone Detection, Identification and Neutralization (ALADDIN) nel quadro dei finanziamenti Horizon 2020[238] mette insieme industrie e istituti di ricerca per la creazione di un sistema di riconoscimento, identificazione e neutralizzazione dei droni duali in grado di rispondere sia a minacce attive che a intrusioni involontarie in zone ristrette al sorvolo. I 16,5 milioni di euro messi a disposizione per questo progetto[239] dovranno portare alla sperimentazione del primo sistema di rilevamento completamente integrato e dotato di diverse capacità di contrasto. Stando a quanto previsto dal progetto, queste ultime potranno essere utilizzate a seconda dell'ambiente circostante e di una valutazione dei possibili danni collaterali a persone e cose[240].

*on Drone Threats and Announces Support for Innovative Projects*, 17 ottobre 2019, https://europa.eu/!mJ79mN. Si veda inoltre: Commissione europea, *European Commission and European Investment Bank Announce Launch of "European Drone Investment - Advisory Platform"*, cit.

234 Si veda il sito di EUROCAE: *Working Groups*, https://eurocae.net/about-us/working-groups.

235 "EUROCAE Creates C-UAS Working Group", in *UAS Vision*, 13 novembre 2019, https://www.uasvision.com/2019/11/13/eurocae-creates-c-uas-working-group.

236 EUROCAE, *Technical Work Programme, Edition 2020*, 25 ottobre 2019, p. 39, https://www.eurocae.net/media/1636/eurocae-twp-2020-public-version.pdf.

237 Il progetto PeSCo sul C-UAS verrà considerato nel paragrafo 3.4 del presente studio.

238 Si veda il sito ufficiale di ALADDIN: *Project*, https://aladdin2020.eu/project.

239 Commissione europea, *Funding & Tender Opportunities: Technologies for Prevention, Investigation, and Mitigation in the Context of Fight Against Crime and Terrorism* (ID: SEC-12-FCT-2016-2017), ottobre 2015, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/sec-12-fct-2016-2017.

240 Si veda il sito di ALADDIN: *Outcomes*, https://aladdin2020.eu/outcomes.


ISSN 2280-6164

Allo sviluppo di capacità di contrasto modulari, scalabili e interoperabili per il contrasto dei droni duali e a protezione delle forze armate dispiegate, delle infrastrutture critiche e delle informazioni sensibili, è dedicato un bando con un finanziamento previsto di 13,5 milioni di euro, rientranti nell'ambito delle azioni dell'EDIDP per il 2019-2020[241]. L'EDIDP pone inoltre particolare enfasi allo sviluppo di capacità di rilevamento, tracciamento e contrasto dei droni duali per mezzo di sciami di droni rientranti nella categoria mini. In quest'ottica, a livello europeo vi è la consapevolezza che gran parte degli sviluppi tecnologici funzionali allo scopo preposto provengono dalle PMI, alle quali è riservata la *call for proposal* riguardante lo sviluppo di sciami composti da droni di categoria mini.

Passando alle attività promosse nel quadro dei progetti PeSCo, il progetto Counter Unmanned Aerial System (C-UAS), a guida italiana, mira a sviluppare un efficiente sistema di sistemi dotato di un'architettura C2 in grado di contrastare la minaccia rappresentata dai mini e micro droni[242]. Il progetto rientra tra quelli adottati durante la seconda ondata di progetti PeSCo approvati nel 2018[243] e al momento vede la partecipazione di Italia e Repubblica Ceca. Dovesse il progetto estendersi anche ad altri Paesi, se presentato nell'ambito del Fondo europeo per la Difesa (European Defence Fund, EDF) potrebbe beneficiare dei fondi stanziati dall'EDF, potendo anche contare sulla "premialità" derivante dalla PeSCo. La tematica dei droni è stata oggetto anche di un ulteriore progetto PeSCo, approvato con la terza ondata di progetti del 2019. Il progetto European Global RPAS Insertion Architecture System[244], anch'esso a guida italiana, prevede la creazione di un centro di competenza multinazionale per sviluppare una dottrina comune europea circa i sistemi *unmanned* e gli assetti volti al loro contrasto.

### *3.4 Il contesto nazionale*

La capacità di difendersi da potenziali attacchi perpetuati dai droni è considerata dalle forze di sicurezza e di difesa italiane un requisito di primaria importanza. All'interno del Rapporto Esercito[245], rapporto annuale sulle attività, i programmi e i progetti delle FF.AA., la necessità di dotarsi di un sistema di contrasto dei droni duali è una costante delle ultime due edizioni. Nell'edizione del 2017 il Rapporto rendeva nota la creazione di un progetto per acquisire un sistema in grado di

[241] Si veda Annex, p. 5, in Commissione europea, *Commission Implementing Decision of 19.3.2019 on the Financing of the European Defence Industrial Development Programme and the Adoption of the Work Programme for the Years 2019 and 2020* (C/2019/2205), https://ec.europa.eu/docsroom/documents/34515.

[242] Si veda il sito di PESCO: *Counter Unmanned Aerial System (C-UAS)*, https://pesco.europa.eu/?p=800.

[243] Emma Marty, "Another 17 PESCO Projects Approved", in *Finabel Info Flash*, 12 dicembre 2018, https://wp.me/paDUqP-cm.

[244] Si veda il sito di PESCO: *European Global RPAS Insertion Architecture System*, https://pesco.europa.eu/?p=1772.

[245] Disponibile nel sito dell'Esercito Italiano: *Rapporto Esercito*, http://www.esercito.difesa.it/Rapporto-Esercito.


ISSN 2280-6164

contrastare i droni duali da dare in dotazione delle unità di artiglieria contraerea[246]. Mentre in quell'occasione veniva fatto riferimento unicamente alla creazione del progetto, è dall'edizione del 2018 che il livello di concentrazione degli sforzi che le FF.AA. stanno compiendo in ambito C-UAS è risultato evidente.

Nelle priorità di ammodernamento del 2018[247] si fa riferimento all'elaborazione di concrete misure per acquisire la capacità C-UAS. Tali capacità devono essere in grado di garantire la protezione delle truppe in teatri operativi, e devono poter essere poste a supporto delle altre misure di sicurezza in occasione di eventi pubblici sul territorio nazionale. Nel rapporto 2018 si fa, inoltre, riferimento alla conclusione della fase di sperimentazione dei prototipi che verranno assegnati al 17° reggimento a. c/c Sforzesca, in capo al Comando di Artiglieria Controaerei (COMACA) di Sabaudia.

Anche analizzando il Documento programmatico pluriennale per la Difesa (DPP) 2019-2021 è possibile rilevare che la dotazione di questi sistemi è prevista per assicurare la Difesa Aerea e Missilistica Integrata (DAMI)[248]. I fondi del DPP per il C-UAS rientrano nei principali interventi svolti con il supporto del Fondo per il rilancio degli investimenti delle amministrazioni centrali e dello Stato che prevede uno stanziamento di 16 milioni di euro per questa capacità.

L'importanza di doversi dotare di un sistema di contrasto alla minaccia dei droni, che sia utilizzabile dalle diverse Forze Armate, è rappresentata dalla costituzione di un Centro di eccellenza Counter Mini/Micro Aeromobili a Pilotaggio Remoto (CDE C-M/M APR) a valenza interforze[249] presso il COMACA. A seguito di un anno di sperimentazioni in ambito C-UAS al COMACA è stato ufficialmente affidato nel 2016 il mandato di studio e realizzazione di capacità di contrasto dei droni di piccola taglia, come iniziale soluzione di *gap-filler* capacitivo[250]. Tra i compiti del Centro compaiono quelli di studio, ricerca, sviluppo concettuale, tecnico e dottrinale per un contrasto quanto più efficace possibile. Il CDE C-M/M APR insieme ai Fucilieri dell'Aria del 16° Stormo, in capo all'Aeronautica Militare, svolgono anche altre attività di studio e sperimentazione di tecniche, procedure e sistemi di contrasto di mini/micro APR[251].

[246] Stato Maggiore dell'Esercito, *Rapporto Esercito 2017*, gennaio 2018, p. 74, http://www.esercito.difesa.it/Rapporto-Esercito/Documents/RE17%203101%20MEDIUM%20PER%20INTERNET.pdf.

[247] Stato Maggiore dell'Esercito, *Rapporto Esercito 2018*, marzo 2019, p. 68, http://www.esercito.difesa.it/Rapporto-Esercito/Documents/RE-2018-rid-190329.pdf.

[248] Ministero della Difesa, *Documento programmatico pluriennale per la Difesa per il triennio 2019-2021*, luglio 2019, p. 26, https://www.difesa.it/Content/Documents/Documento_Programmatico_Pluriennale_(DPP)_2019_2021_digit.pdf.

[249] Esercito Italiano, *Centro di eccellenza antidrone al COMACA*, 11 marzo 2019, http://www.esercito.difesa.it/comunicazione/Pagine/Centro_di_eccellenza_antidrone_al_COMACA-190311.aspx.

[250] Roberto Baldisseri, intervento al convegno *La neutralizzazione della minaccia drone: una sfida da vincere*, 22 novembre 2017 (video), https://www.afcearoma.it/eventi/anno-2017/93.

[251] Aeronautica Militare, *Al Centro di Eccellenza di Amendola i futuri Operatori APR*, 26 febbraio 2019, http://www.aeronautica.difesa.it/comunicazione/notizie/Pagine/mini-e-micro-apr.aspx.


ISSN 2280-6164

Nonostante il CDE C-M/M APR sia di recente costituzione, la formazione di personale specializzato preposto alle attività di contrasto dei droni duali utilizzati per scopi illeciti è in corso in Italia già da tempo. La prima qualifica di operatore *Counter-UAS* è stata rilasciata, infatti, già nel 2018 sfruttando le competenze acquisite nei teatri operativi[252]. Con la costituzione del CDE C-M/M APR la formazione ha assunto valenza ancora più centrale, dal momento che il COMACA ha formulato e implementato un *business plan* dedicato alla formazione del personale[253]. Le capacità degli operatori vengono completate con le qualifiche di *Slow Mover Interceptor Operator* (SMIO) ottenute dai Fucilieri del 9° Stormo di Grazzanise per intercettare e contrastare velivoli dalle dimensioni ridotte[254].

L'approccio che il Governo italiano intende seguire sembra essere quello a caratteristica interforze, che ben si adatta all'ampio spettro di applicazione dei droni utilizzabili a scopi illeciti e alle loro caratteristiche. Questi sono dei dispositivi che, sebbene possano essere applicati in teatri diversi e con specifiche tecniche differenti, utilizzano lo stesso ventaglio di tecnologia di base.

Da diversi anni le FF.AA. sono impegnate in un programma di definizione dei requisiti e delle necessità numeriche di un sistema C-UAS nell'ambito di un piano di ammodernamento e rinnovamento avviato dallo Stato Maggiore della Difesa (SMD)[255]. A livello italiano si è proceduto, in un primo momento, alla sperimentazione in ambito C-UAS per l'individuazione delle possibili soluzioni di contrasto dei droni di piccoli dimensioni attraverso l'utilizzo di capacità già a disposizione delle FF.AA.[256]. Il passo successivo previsto sarà la definizione, tramite un tavolo tecnico interforze, dei requisiti dei sistemi di contrasto *ad hoc*, che sia possibile modificare e aggiornare costantemente, a seconda dell'evoluzione tecnologica disponibile. Tuttavia, allo stato attuale EI e AMI sono dotati di sistemi di C-UAS[257] che sono il frutto di iniziative differenti. Stando alla Relazione sullo stato di attuazione dei programmi di ammodernamento e rinnovamento di mezzi, impianti e sistemi per l'anno 2018[258] presentata dal ministro della Difesa Guerini,

[252] Aeronautica Militare, *Al 16° Stormo il 1° corso operatore C-UAS*, 8 novembre 2018, http://www.aeronautica.difesa.it/comunicazione/notizie/Pagine/AL-16°-STORMO-IL-1°-CORSO-OPERATORE-C-UAS.aspx.

[253] Ministero della Difesa, *Antidrone: la nuova capacità dell'Esercito Italiano a Matera*, settembre 2019, https://www.difesa.it/Content/Manifestazioni/Matera_2019/Pagine/Antidrone_la_nuova_capacita_del_Esercito_Italiano_a_Matera.aspx.

[254] "Aeronautica Militare, aumenta la capacità della Forza Armata nel contrasto alle minacce derivanti dall'utilizzo di droni…", in *Report Difesa*, 4 gennaio 2019, http://www.reportdifesa.it/?p=25160.

[255] Glauco Luigi Mora, intervento al convegno *La neutralizzazione della minaccia drone: una sfida da vincere*, 22 novembre 2017 (video), https://www.afcearoma.it/eventi/anno-2017/93.

[256] Roberto Baldisseri, intervento al convegno *La neutralizzazione della minaccia drone*, cit.

[257] Leonardo, *La Royal Air Force sceglie Leonardo come partner per il programma di ricerca anti-drone*, 11 settembre 2019, https://www.leonardocompany.com/it/press-release-detail/-/detail/11-09-19-2-royal-air-force-selects-leonardo-for-counter-drone-research-programme.

[258] Ministero della Difesa, *Relazione sullo stato di attuazione dei programmi di ammodernamento e rinnovamento di mezzi impianti e sistemi (anno 2018)* (Doc. CCIX n.2), 23 ottobre 2019, http://www.


ISSN 2280-6164

l'AMI ha sostenuto una spesa di 4,8 milioni di euro per "l'acquisizione delle capacità di contrasto alla minaccia portata da mini/micro APR". Dal canto suo, l'EI si è dotato autonomamente di un sistema di C-UAS.

Soprattutto dopo gli avvenimenti verificatisi ai pozzi di petrolio in Arabia Saudita[259] è diventata più realistica la necessità di pensare anche alla protezione dai droni di dimensioni superiori ai 20 kg, ma non rientranti nella categoria dei droni militari. Questo tipo di difesa, già nota alle FF.AA.[260], potrebbe essere effettuata tramite l'integrazione dei vari sistemi di difesa aerea, dai sistemi *ground-based air defence* e la difesa aerea tradizionale, ai sistemi C-UAS. Il raggio delle soluzioni per il contrasto degli UAV deve essere all'avanguardia tecnologica che sia in grado di contrastare la maggior parte possibile delle potenziali minacce e nei vari contesti nazionali e in teatro operativo. In quest'ultimo contesto, è necessario sottolineare come la protezione delle FF.AA. italiane impiegate nei teatri operativi debba essere assicurata anche a livello di convoglio e non solo di basi militari.

La sinergia derivante dalla collaborazione tra le varie Forze Armate e gli operatori di pubblica sicurezza è stata testata già in diverse occasioni. A titolo di esempio, durante la visita del Presidente della Federazione Russa Vladimir Putin a Roma dello scorso 4 luglio 2019 sono stati utilizzati assetti anti-drone[261] del CDE C-M/M APR insieme a quelli dell'Operazione Strade Sicure. Inoltre, nell'ambito di quest'ultima operazione, dal settembre 2018 vengono impiegati anche i Fucilieri del 16° e del 9° Stormo a protezione dei principali aeroporti italiani[262].

Oltre alla cooperazione tra i vari corpi d'arma e alla cooperazione tra i vari uffici, l'Italia è promotrice di una maggiore cooperazione internazionale sul tema, particolarmente a livello europeo. Il già citato progetto PeSCo C-UAS a guida italiana è stato ufficialmente avviato con il primo incontro del progetto svoltosi a Sabaudia nel settembre 2019, al quale erano presenti anche rappresentanti di 5 Paesi europei[263] e durante il quale sono state presentate le potenzialità dei sistemi al momento in dotazione in Italia. Anche per quanto concerne lo sviluppo o il progetto PeSCo European Global RPAS Insertion Architecture System approvato nel novembre 2019[264].

senato.it/service/PDF/PDFServer/DF/348064.pdf.

259 Sissi Bellomo, "Attacco con droni al petrolio saudita: fermata metà della produzione", in *Il Sole 24 Ore*, 14 settembre 2019, https://www.ilsole24ore.com/art/nuovo-attentato-petrolio-saudita-droni-contro-due-impianti-AC6HXQk.

260 Glauco Luigi Mora, intervento al convegno *La neutralizzazione della minaccia drone*, cit.

261 Ministero della Difesa, *Le Forze Armate concorrono alla cornice di sicurezza per la visita del Presidente Putin*, 4 luglio 2019, https://www.difesa.it/SMD_/Eventi/Pagine/Forze_Armate_concorrono_alla_sicurezza_per_la_visita_presidente_Putin.aspx.

262 Ministero della Difesa, *Festività natalizie, Operazione Strade Sicure*..., cit.

263 Ministero della Difesa, *PeSCO: avviato il progetto per il contrasto ai droni*, 18 settembre 2019, https://www.difesa.it/SMD_/Eventi/Pagine/Pesco_avviato_il_progetto_per_il_contrasto_ai_droni.aspx.

264 Il progetto prevede la partecipazione, oltre all'Italia, di Francia e Romania.

DOCUMENTI IAI 20 | 04 - MARZO 2020 ISSN 2280-6164

## Conclusioni

di Ester Sabatino e Michele Nones[265]

Negli ultimi decenni i droni duali (in particolare di dimensioni ridotte) sono stati oggetto di importanti innovazioni tecnologiche che, unitamente ad un costo contenuto, hanno reso la loro acquisizione e il loro utilizzo molto più accessibile di quanto non avvenisse in passato. I vantaggi in termini di costo-efficienza hanno fatto sì che gli utilizzatori privati iniziassero ad utilizzarli per scopi commerciali e ricreativi. Parimenti però, anche attori non statali, gruppi terroristici e singoli individui li hanno impiegati per scopi illeciti di varia natura, rendendo più impellente la ricerca di soluzioni atte al loro contrasto.

Tra le ragioni che hanno portato all'inclusione dei droni duali tra i possibili mezzi di una minaccia ibrida, un ruolo determinante è stato giocato dal loro sviluppo tecnologico che ha seguito tre trend principali, incrementando le difficoltà di contrasto della minaccia:

1. La costante tendenza alla miniaturizzazione delle componentistiche ha aumentato non solo la possibilità di un uso più agevole dei droni, ma ne ha di pari passo accresciuto le potenzialità di utilizzo e di personalizzazione. Grazie a materiali leggeri e resistenti è possibile mantenere una capacità di *payload* elevata e le possibilità di montaggio di componenti aggiuntive sono tendenzialmente illimitate, se si considera la possibilità della loro fabbricazione tramite l'*additive manufacturing*.

2. L'impiego di tecnologie quali i sistemi INS e VIO, svincolate dai tradizionali sistemi di guida basati su segnali GPS o Wi-Fi, aumentano l'autonomia del drone rispetto all'operatore, oltre a rendere più sicura la buona riuscita dell'operazione. Ciò ha incrementato le possibilità di anonimato dell'operatore, che può limitare la sua azione all'impostazione del piano di volo o delle coordinate del bersaglio ed essere geograficamente molto distante dal drone, specialmente se fossero impiegate tecnologie 5G.

3. Sebbene ancora in fase di sperimentazione, gli sciami di droni sono in grado di operare in modo autonomo rispetto all'operatore e di rispondere in modo coordinato e/o cooperativo ad eventuali interferenze esterne, grazie all'utilizzo dell'Intelligenza Artificiale. L'uso degli sciami amplifica la portata della minaccia, non solo perché bisogna contrastare più droni allo stesso momento, ma anche perché essi possono confondere l'operatore dei sistemi di difesa C-UAS, inducendolo a concentrarsi su bersagli esca.

[265] Michele Nones è vicepresidente dello IAI.


ISSN 2280-6164

La minaccia portata dai droni duali è ad oggi rappresentata anche da un uso improprio non intenzionale. Ciò può essere causato sia da una non curanza dell'operatore delle linee guida da dover seguire, sia dalla mancanza di un quadro regolatorio e legislativo chiaro e definito. Il crescente utilizzo dei droni anche da parte di amatori e hobbisti non è stato infatti accompagnato da una normativa adeguata che ne definisse le possibilità di impiego e i relativi limiti. Le novità introdotte dalla terza edizione del Regolamento ENAC Mezzi Aerei a Pilotaggio Remoto, in applicazione del Regolamento di esecuzione (UE) 2019/947 potrebbero portare a una maggiore consapevolezza dell'uso lecito dei droni di piccole dimensioni. Potrebbe, quindi, risultare più semplice per gli operatori di pubblica sicurezza e per il personale delle FF.AA., impiegate a supporto dei primi, concentrarsi maggiormente sull'identificazione e il contrasto di attacchi volontari veicolati a mezzo drone.

Nonostante gli sforzi compiuti nel definire i limiti all'impiego dei droni duali, rimane ancora la mancanza di una definizione univoca degli organi preposti al loro contrasto. In particolare, ad oggi non risulta chiaramente definito quale sia l'autorità competente ad intervenire in relazione all'ambito in cui la minaccia si verifichi, sia essa in territorio nazionale o afferente ai teatri operativi. Anche le eventuali responsabilità dell'operatore preposto al contrasto, in caso di danni collaterali causati durante l'operazione, non sono determinate in modo tale da limitare eventuali ripercussioni sull'operatore. Si è riscontrata, in questo contesto, la necessità di dover snellire e velocizzare le tempistiche per la determinazione della responsabilità dell'operatore, altrimenti non adeguatamente tutelato.

Contrastare la minaccia dei droni duali presenta delle difficoltà sotto diversi aspetti. Il carattere asimmetrico è amplificato dalla limitata possibilità di definire con congruo anticipo se eventuali intromissioni in spazi aerei limitati, o con divieto di sorvolo, siano attacchi volontari o meno. Inoltre, con la tecnologia attualmente a disposizione, è possibile verificare l'eventuale presenza di *payload* ostile solo a distanze piuttosto ravvicinate (se ci si riesce), con la conseguente compressione del tempo a disposizione dell'operatore per poter decidere e attuare la tipologia di contrasto più consona. Di qui l'esigenza di essere dotati di un sistema C-UAS che operi autonomamente nelle fasi di rilevamento e tracciamento del drone e che mantenga il *man-in-the-loop* nella sola fase di ingaggio. Inoltre, considerato che i diversi sensori e attuatori C-UAS sono in grado di rilevare, tracciare e contrastare i droni con modalità differenti, la modularità di questi sistemi è di fondamentale importanza per assicurare la buona riuscita dell'operazione. Un sistema di contrasto modulare permette, altresì, il possibile impiego di diverse soluzioni di contrasto a seconda che obiettivo dell'attacco sia un centro abitato, un assembramento di persone, un'infrastruttura critica o un contingente impiegato in teatro operativo.

Il costante avanzamento tecnologico dei droni duali determina la necessità di una pianificazione *forward looking* delle capacità di contrasto. Diversamente da quanto avviene per gli altri sistemi d'arma, la catena produttiva dei sistemi C-UAS non può avere le stesse logiche e tempistiche che hanno caratterizzato la progettazione e lo sviluppo degli armamenti convenzionali: l'elevata capacità di


ISSN 2280-6164

adattamento dei droni duali allo sviluppo delle capacità di contrasto, sta portando i *decision-maker* a considerare l'impiego di droni e di sciami di droni come parte delle soluzioni C-UAS. In questo modo l'*early warning* avvantaggia l'operatore di pubblica sicurezza e delle FF.AA. aumentando la prontezza non solo nei confronti dell'eventuale presenza di *payload* ostile, ma dell'effettiva entità della minaccia, senza dover necessariamente aspettare l'avvicinamento del drone ostile al target. Risulta ancora incerto, tuttavia, in quale misura droni o sciami di droni possano essere impiegati anche nella fase di contrasto della minaccia e come gestire gli eventuali danni collaterali.

La possibilità che droni duali possano diventare parte integrante dei futuri scontri convenzionali ha portato le più importanti organizzazioni internazionali attive nel campo della sicurezza a considerare la definizione di standard e procedure condivisi, nonché lo sviluppo di capacità C-UAS tra le loro priorità principali. La molteplicità delle iniziative portate avanti sia a livello NATO che a livello europeo è sintomatico della crescente attenzione posta ai droni duali e delle differenti angolature da cui la minaccia può essere considerata. Tuttavia, la messa a sistema di tali iniziative e la condivisione dei risultati raggiunti potrebbero accelerare il raggiungimento degli obiettivi preposti e assicurare maggiori livelli di sicurezza e di capacità di difesa, anche in ottica cooperativa.

Il rafforzamento delle capacità di difesa dai droni duali è tra gli obiettivi che l'Italia sta perseguendo. La guida di due progetti PeSCo inerenti alle capacità di contrasto dei droni duali, così come la partecipazione del personale italiano ai gruppi di lavoro NATO, confermano la volontà nazionale di essere attivamente presenti anche nelle iniziative internazionali nel campo C-UAS.

Nella stessa direzione va il lavoro interforze del Centro di eccellenza C-M/M APR presso il COMACA. Questo rappresenta la volontà dello Stato Maggiore della Difesa di unificare gli sforzi finora compiuti dalle singole Forze Armate. Proseguire su questa strada mal si adatta, infatti, all'ampio spettro di applicazione dei droni duali.

È, quindi, necessaria una strategia che definisca in modo chiaro le caratteristiche di un sistema di difesa nazionale contro la minaccia proveniente dai droni duali a livello di requisiti operativi, di necessità numeriche e di procedure operative. In particolare dovranno essere definite con maggiore chiarezza le responsabilità dei diversi soggetti coinvolti e le modalità di coordinamento delle loro attività sia addestrative che operative. Altrettanta attenzione andrà posta al piano tecnologico e industriale, assicurando la continuità della ricerca e dello sviluppo in un settore caratterizzato da una rapidissima evoluzione tecnologica e da un mercato fortemente internazionalizzato e, nello stesso tempo, un'adeguata standardizzazione per garantire sia l'interoperabilità di tutti i sistemi C-UAS utilizzati, sia la maturazione industriale necessaria per costruire un mercato sufficientemente attrattivo.

In quest'ottica potrebbe essere utile costruire una cabina di regia interministeriale che, analogamente a quanto avvenuto in altri settori, consenta di costruire una


ISSN 2280-6164

posizione condivisa delle diverse amministrazioni coinvolte e convogliare efficacemente le risorse finanziarie necessarie per migliorare le nostre capacità di difesa di fronte a questa nuova crescente minaccia.

*aggiornato 22 gennaio 2020*


ISSN 2280-6164

## Lista degli acronimi

| | |
|---|---|
| 3D | Tridimensionale |
| 5G | Quinta generazione |
| ACT | Allied Comand Transformation (NATO) |
| AI | Artificial Intelligence |
| ALADDIN | Advanced hoListic Adverse Drone Detection, Identification and Neutralization |
| AMI | Aeronautica Militare |
| APR | Aeromobili a pilotaggio remoto (vedi anche UAV) |
| ARP | Aerodrome Reference Point |
| ATM | Air Traffic Management |
| ATZ | Aerodrome Traffic Zone |
| BVLOS | Beyond Visual Line of Sight |
| CC | Codice civile |
| CP | Codice penale |
| CPMG | Codice penale militare di guerra |
| CPMP | Codice penale militare di pace |
| C2 | Comando e controllo |
| CBRN | Chimici, biologici, radiologici, nucleari |
| CD&E | Concept Development and Experimentation |
| CDE C-M/M APR | Centro di eccellenza Counter Mini/Micro Aeromobili a Pilotaggio Remoto |
| CdN | Codice della Navigazione aerea |
| COI | Comando operativo di vertice interforze |
| COMACA | Comando Artiglieria Controaerei |
| C-RAM | Counter-Rocket Artillery and Mortar |
| CSA | Comitati di Sicurezza aeroportuale |
| C-sUAS | Countering Small Unmanned Aircraft Systems |
| CTR | Control Zone |
| C-UAS | Counter Unmanned Aerial System |
| CUASFG | Counter-UAS Focus Group |
| CUR | Crisis Response Urgent Operational Requirement |
| DAA | Detection and avoid |
| DAMI | Difesa Anti-Missilistica Integrata |
| DAT POW | Defence Against Terrorism Programme of Work |
| DIU | Diritto internazionale umanitario |
| DPP | Documento programmatico pluriennale |
| EDF | European Defence Fund |


ISSN 2280-6164

| | |
|---|---|
| EDIDP | European Defence Industrial Development Programme |
| EI | Esercito Italiano |
| ENAC | Ente Nazionale per l'Aviazione Civile |
| ENAV | Ente Nazionale per l'Assistenza al Volo |
| EO | Elettro-ottico |
| ESCD | Emerging Security Challenges Division |
| EUROCAE | European Organisation for Civil Aviation Equipment |
| EVLOS | Extended-Visual Line of Sight |
| FAA | Federal Aviation Administration |
| FF.AA. | Forze Armate |
| FPWG | Force Protection Working Group (NATO) |
| GIP | Giudice per le indagini preliminari |
| ICAO | International Civil Aviation Organisation |
| ID | Identification Code (Codice identificativo) |
| IED | Improvised Explosive Device |
| IFR | Instrument Flight Rule |
| IMU | Inertial Measurement Unit |
| INS | Inertial Navigation System |
| IO | Infrarossi |
| ISTAR | Intelligence, Surveillance, Target Acquisition and Reconnaissance |
| JAPCC | Joint Air Power Competence Center (NATO) |
| LSS | Low, small and slow |
| MEMS | Micro Electro-Mechanical Systems |
| MIT | Ministero delle Infrastrutture e dei trasporti |
| MOOTW | Military Operations Other Than War |
| NASA | National Aeronautics and Space Administration |
| NCI | NATO Communications and Information |
| NDPP | NATO Defence Planning Process |
| NNTEX-18C | NATO Non-Lethal Technology Exercise Counter-UAS |
| NOTAM | NOtice to AirMen |
| PeSCo | Permanent Structured Cooperation (UE) |
| PM | Pubblico ministero |
| PMI | Piccole e medie imprese |
| RFID | Radio-frequency Identification |
| ROE | Rules of Engagement |
| RPAS | Remotely Piloted Aircraft System (vedi anche SAPR) |
| SAPR | Sistemi aeromobili a pilotaggio remoto (vedi anche RPAS) |
| SESAR | Single European Sky Air Traffic Management Research |
| SHAPE | Supreme Headquarters Allied Powers Europe (NATO) |


ISSN 2280-6164

| | |
|---|---|
| SMD | Stato Maggiore della Difesa |
| SMIO | Slow Mover Interceptor Operator |
| SPS | Science for Peace and Security (NATO) |
| STO | Science and Technology Organisation (NATO) |
| SWaP | Size, weight and power |
| UAS | Unmanned Aerial System |
| UAS | Unmanned Aircraft System |
| UAV | Unmanned Aerial Vehicle (vedi anche APR) |
| UE | Unione europea |
| VIO | Visual-Inertial Odometry |
| VLOS | Visual Line of Sight |


ISSN 2280-6164

ISSN 2280-6164

Istituto Affari Internazionali (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, 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*), tre collane di libri (*Global Politics and Security*, *Quaderni IAI* e *IAI Research Studies*) e varie collane di paper legati ai progetti di ricerca (*Documenti IAI*, *IAI Papers*, ecc.).

Via Angelo Brunetti, 9 - I-00186 Roma, Italia
T +39 06 3224360
F + 39 06 3224363
iai@iai.it
www.iai.it

# Ultimi DOCUMENTI IAI

Direttore: Alessandro Marrone (a.marrone@iai.it)

20 | 04 Ester Sabatino e Francesco Pettinari (a cura di), *La minaccia dei droni duali e le sfide per l'Italia*

20 | 03 Alessandro Marrone e Michele Nones, *Le forze italiane in missione all'estero: trend e rischi*

20 | 02 Jean-Pierre Darnis, Xavier Pasco and Paul Wohrer, *Space and the Future of Europe as a Global Actor: EO as a Key Security Aspect*

20 | 01 Francesco Pettinari, *L'Europa della difesa accelera, e l'Italia?*

19 | 21 Eleonora Poli e Lara Laviola, *Tavola rotonda italo-olandese Van Wittel/Vanvitelli*

19 | 20 Eleonora Poli, Lara Laviola and Laura Sacher, *Central European Initiative Dialogue Forum*

19 | 19 Matteo Bonomi, *Walking the Strategic Talk. A Progressive EU Foreign Policy Agenda. Conference Report*

19 | 18 Margherita Bianchi, *From Findings to Market: Perspectives and Challenges for the Development of Gas Resources in the East Med*

19 | 17 Michele Nones, Paola Sartori e Andrea Aversano Stabile, *La difesa missilistica e l'Italia: vecchie minacce e nuove sfide per la sicurezza nazionale*

19 | 16 Filippo Cutrera, *Priorità italiane dopo 70 anni di Nato*