



White Paper in collaborazione con Robin Radar

Situazione

La grande crescita dell'utilizzo di **droni** ha causato un'impennata nella casistica delle mancate collisioni ed incrementato il rischio che i droni possano interrompere il traffico aereo o addirittura causare collisioni.

I droni "consumer" e commerciali sono normalmente sotto i dieci Kg e nella maggior parte dei casi sotto i 2Kg. Quadcopters con quattro pale rotanti orizzontali sono i più comuni ma ci sono anche droni con piccole ali fisse.

I droni, di norma, contano su un'autonomia di volo di circa 30 minuti, ma con un veloce cambio di batterie e/o con l'utilizzo di droni multipli sono in grado di causare importanti interruzioni del traffico aereo.

Nonostante le limitazioni imposte dai regolamenti i droni sono sicuramente in grado di volare fino ad un'altitudine di 6.000mt e fino ad 8Km dal loro operatore, il che li porta facilmente nello stesso spazio aereo degli aerei in atterraggio o in partenza.

Studi internazionali hanno dimostrato che la collisione di un drone con un aereo può causare danni alla struttura dello stesso maggiori rispetto alla stessa energia prodotta da un impatto con uccelli e che i danni di una collisione di un drone con un aereo può causarne la caduta.

A parte le interruzioni involontarie al traffico aereo o le collisioni, causate da operatori inconsapevoli o che hanno scelto di ignorare le disposizioni di sicurezza vigenti nei pressi di aeroporti, c'è un altro rischio dovuto a coloro che intenzionalmente vogliono causare interruzioni.

Ricordiamo che un piccolo drone "consumer" può sollevare e trasportare un pacchetto di 500gr. e che un drone commerciale può arrivare fino a 6kg. Ove un terrorista volesse far esplodere un aereo passeggeri troverebbe più semplice l'uso di un drone munito di esplosivo piuttosto che cercare di forzare la sicurezza aeroportuale.

Sono disponibili varie tecnologie per il monitoraggio e per l'attivazione di contromisure. Il monitoraggio è consentito e raccomandato. L'abbattimento di droni non è permesso nella maggior parte dei paesi.

Le tecnologie di monitoraggio normalmente comprendono Analizzatori di Radio Frequenza (RF), Sistemi Acustici, Telecamere e Radar. Ciascuna tecnologia ha i propri pro e contro ed è raccomandabile che i sistemi di monitoraggio droni acquistati dagli aeroporti siano un'integrazione di:

- RF, per l'identificazione e triangolazione sia dei droni che del controllore (se sono presenti segnali radio);
- Telecamere, per l'identificazione visuale e la comprensione del pericolo e degli intenti;
- Radar, per il rilevamento a distanza, accurata localizzazione e tracciamento (anche in caso di sciame di droni) e classificazione anche di droni autonomi che non emettono alcun segnale radio.

I radar per il rilevamento di droni, siano essi stand alone o parte di un sistema integrato, dovrebbero essere dotati di tecnologia micro-doppler specificamente predisposta, ed in grado, di distinguere i droni dagli uccelli. La tecnologia micro-doppler è in grado di evitare ed abbattere falsi allarmi causati dagli uccelli, problema assai frequente quando si utilizzano i radar tradizionali.

Le contromisure normalmente comprendono: RF Jammer, GPS Spoofer, Microonde ad alta potenza (HPM), Reti e Fucili per lanciare reti, uccelli rapaci. Secondo la normativa vigente, nessuna di queste contromisure è consentita, ma possono essere richieste deroghe specifiche e motivate.

I fucili con reti hanno un basso rischio di danni collaterali negli aeroporti. RF jamming, GPS spoofing and Electromagnetic Pulses (EMPs), hanno invece un maggiore rischio di danni elettronici collaterali negli aeroporti, ma possono essere usati con successo se coordinati e gestiti correttamente.



Qual è il problema con i droni negli aeroporti?

L'utilizzo di droni sia a scopo amatoriale che commerciale ha avuto una crescita esplosiva negli ultimi anni. Sono diventati economici, facile da ottenere e semplici da usare. Questo ha creato nuove opportunità ma evidenzia anche nuovi pericoli.

La crescita dell'utilizzo di droni ha causato un'ondata di segnalazioni di mancate collisioni ed aumentato il rischio di interruzioni del traffico aereo.

È così difficile interrompere il traffico aereo?

NO, e le cause vanno dal semplice volo in area interdetta all'attentato terroristico.

Basta pensare al drone che si avvicina alle piste, che vola per scattare foto o che trasporta una piccola quantità di esplosivo da far detonare sull'ala di un aeroplano pronto al decollo. Un aereo con il pieno di carburante e con passeggeri a bordo...






Quale tipo di droni rappresentano un problema?

Quando parliamo del rischio **droni** negli aeroporti non ci riferiamo a quelli impiegati negli attacchi in Afghanistan o Pakistan nella guerra al terrorismo.

Parliamo di droni "consumer" e "commerciali" normalmente con peso sotto i 10Kg e nella maggior parte dei casi sotto i 2Kg. Spesso sono Quadcopters con quattro pale rotanti orizzontali ma il termine drone comprende anche velivoli con piccole ali fisse.

Altri nomi per droni sono: Small Unmanned Air Vehicles (SUAVs) e Small Unmanned Air Systems (SUAS). Questi termini sono i più usati nell'industria della difesa.

Alcuni dei più diffusi droni in commercio sono prodotti dalla società DJI. Di seguito sono indicati i modelli più noti e le relative caratteristiche:

	Spark	Mavic	Phantom	Inspire	Matrice 600
					
Dimensions	14x14x6cm	31x24x9cm	29x29x20cm	48x47x32cm	167x152x73cm
Weight	300g	700g	1.4kg	3.4kg	10kg
Max. Flight Time	16 mins	31 mins	30 mins	27 mins	18 mins
Max. Speed	50km/h	72km/h	72km/h	94km/h	65km/h
Max. Altitude	4km	6km	6km		4.5km
Max. Transmission Distance	2km	8km	7km	7km	5km
Max. Recommended Payload	n/a	n/a	n/a	810g	6kg
Autonomous Flight Capable?	Yes	Yes	Yes	Yes	Yes

Source: dji.com

T-Shield Defense S.r.l.

Via Luigi Mainoni d'Intignano, 17/A – 20125 Milano

tel. 02 45482197 – fax 02 84891855 – e-mail info@t-shielddefense.com P.I. 11766490962



Intenzionale interruzione di un aeroporto

La capacità di volo di un drone è relativamente limitata – tra i 15 e i 10 minuti, ma batterie di ricambio possono essere sostituite velocemente (in pochi secondi). Questo significa che il tempo di volo può essere significativamente esteso con frequenti e brevi interruzioni per la sostituzione delle batterie.

Se lo scopo dell'operatore di un drone è quello di fermare un aeroporto questo può essere facilmente raggiunto con un set di batterie di ricambio o facendo volare più droni.

Un aereo può facilmente incontrare un drone in fase di decollo o di atterraggio

Nella maggior parte dei casi i droni sono manovrati da terra e in quasi tutti i paesi non è consentito loro di volare sopra una determinata altezza. Normalmente debbono rimanere sotto i 120 metri. Questo assicura che i droni rimangano parecchio più bassi di un aeroplano. Va però ricordato che i droni possono volare ben al di sopra di detto limite. In alcuni casi fino a 6km. Non certo un pericolo per un aeroplano ad altezza di crociera ma certamente un pericolo nell'avvicinamento alla pista di atterraggio.

Un operatore di droni potrebbe non essere nei pressi dell'aeroporto

Un'altra norma, vigente in molti paesi, prevede che i droni, per poter essere manovrati, debbano essere visibili all'operatore, entro la cosiddetta "line-of sight" (LOS), ovvero entro i 500 metri.

Come si può notare dalla tabella, di nuovo, la capacità di volo di un drone è ben superiore ai limiti stabiliti dalla norma essendo gestibili da una distanza di 7-8km.

Questo significa che l'operatore potrebbe controllare il drone presente nell'aeroporto da parecchi chilometri di distanza, il che fa crescere ulteriormente le difficoltà di identificazione dell'operatore.

Cosa succede se un drone collide con un aereo passeggeri?

Come descritto precedentemente nella tabella i droni "consumer" misurano circa 30x30cm. e pesano mediamente meno di 2 kg. Quelli professionali sono tra i 50cm. e 1,5mt, con un peso tra i 3kg. e 10kg. La maggior parte del peso è dovuto alle batterie.

In uno studio realizzato dalla Università del Dayton Research Institute (DRI), un drone DJI Phantom (30x30cm. e pesante 1,4kg.) è stato lanciato a 250 miglia/ora contro l'ala di un aereo della General Aviation (GA). Il test, condotto in laboratorio, ha simulato le condizioni di un aereo colpito da un drone in fase di atterraggio. Il drone ha colpito e forato l'attaccatura dell'ala ed entrato in profondità nella struttura, deformando un longherone.

Secondo Kevin Poorman, capo del Gruppo di Impatto Fisico di DRI:

"Tutto il peso di un aereo è basato sui longheroni e se uno viene sufficientemente danneggiato non sopravvivrà. L'aeroplano cadrà"

Mentre il test sopradescritto veniva effettuato su una struttura della GA, l'Autorità dell'Aviazione Civile britannica (CAA) ha sdrammatizzato il rischio di danni, almeno per gli aerei più grandi, dovuto al fatto che questi sono costruiti secondo standard più elevati. Ha però specificato che:

"La collisione con un drone può creare maggiori danni strutturali, rispetto a quello con uno stormo di uccelli, a parità di impatto energetico"



Quel drone porta una telecamera, una pizza o una bomba?

Come descritto precedentemente alcuni droni possono portare piccoli carichi. Il DJI Inspire può trasportare circa un chilo. Il DJI Matrice 600 può invece avere un carico di 6Kg; questi valori sono quelli raccomandati ma in realtà possono trasportare pesi maggiori.

Il DJI Phantom, ad esempio, non è stato progettato per avere pesi, è stato però modificato *dall'ISIS* per trasportare e sganciare granate da 400mm dal peso di circa 400g. Centinaia di attacchi mortali, così organizzati, sono stati effettuati in Iraq e Siria.

Due DJI Matrice 600 sono stati usati nel tentativo di assassinare il Presidente del Venezuela Maduro nel 2018. Sebbene l'attentato non sia riuscito, questi droni, capaci di trasportare fino a 6Kg., hanno fatto detonare dell'esplosivo nell'aria in prossimità del Presidente.

Sebbene a tutt'oggi nessun drone con esplosivo sia stato segnalato in un aeroporto (Drone Borne Improvised Explosive Device DBIED), le misure di sicurezza sono basse. È comunque più facile portare un attacco con un drone che riuscire a mettere una bomba a bordo di un aereo con modalità tradizionali.

Sfide aggiuntive per i droni

La maggior parte dei droni sono controllati mediante radio e molto spesso mediante Wi-Fi. Le tipiche frequenze del Wi-Fi sono: da 2.400 a 2.483GHz. oppure da 5.725 a 5.825GHz. Le informazioni sono normalmente inviate in entrambe le direzioni: dal controllore al drone e dal drone al controllore. Entrambi funzionano sia come trasmettente che ricevente.

I dati trasmessi dal drone al controllore spesso contengono la posizione, la velocità, la rotazione e l'altitudine del drone, così come le immagini video in diretta. I segnali video e tutta la telemetria sono normalmente disponibili su un tablet o uno smartphone con cui è connesso l'operatore. Questo permette all'operatore di avere consapevolezza della situazione consentendo inoltre di controllare e manovrare il drone con la massima precisione.

Volo autonomo

L'operatore di un drone normalmente controlla il drone in tempo reale. È però anche possibile impostare la rotta in modo che il drone possa volare autonomamente verso località preimpostate.

Molti droni prevedono una funzione di sicurezza in grado di far volare il drone automaticamente verso una località predefinita anche in caso di problemi come, ad esempio, la perdita del segnale con il controllore.

I droni possono anche essere modificati in modo da non trasmettere alcun dato. Questa tecnica viene usata quando l'operatore vuole evitare che il drone sia intercettato da sistemi di rilevamento radio.

Sciame

Normalmente vengono presi in considerazione singoli droni ma *sciame di droni* sono diventati una più che realistica possibilità.

Ad una manifestazione di droni INTEL ha sincronizzato 1000 droni, tutti pre-programmati e controllati da una singola base.

Una base aerea russa in Siria è stata attaccata da 13 droni pre-programmati armati con esplosivo, l'attacco sciame di droni è stato lanciato da una distanza di 50 Km.



Amico o nemico

I droni sono sempre più spesso usati per attività commerciali e per servizi di emergenza. In un aeroporto è pertanto importante determinare quali droni siano usati legittimamente (come quelli impiegati per le ispezioni degli aeromobili) e quali sono quelli non autorizzati.

Ad esempio, durante l'interruzione delle attività all'aeroporto di Gatwick nel dicembre 2018, alcuni rapporti citano che alcuni degli avvistamenti di droni fossero droni della polizia. La confusione creata potrebbe aver causato la chiusura dell'aeroporto per un tempo più lungo del necessario.

Quali sono le soluzioni disponibili per contrastare i droni non autorizzati negli aeroporti?

Attualmente la maggior parte degli aeroporti si basa sull'avvistamento visuale, sull'allerta dei piloti, del personale di terra e del pubblico.

Questo approccio passivo ha come maggior vantaggio quello di essere gratuito. Almeno fino a quando non succede un incidente come quello di Gatwick nel dicembre 2018 rivelatosi molto costoso. Stime variano da decine a centinaia di milioni di sterline perse a causa della chiusura dell'aeroporto.

La mancanza di un sistema di monitoraggio droni in funzione significa non disporre delle informazioni necessarie per prendere le decisioni, quelle disponibili sono imprevedibili, inaffidabili ed incostanti.

“Domanda: Preferite essere informati dai piloti di eventuali mancate collisioni o preferite informare i piloti della presenza di droni prima che ci sia una mancata collisione?”

Sicurezza e incertezza non legano bene nell'ambiente aeroportuale. Il risultato è che le piste o l'intero aeroporto possono rimanere chiusi per un tempo più lungo del necessario. Questo si traduce in costi non necessari e negativa reputazione.

Negli ultimi anni diversi apparati per contrastare i droni aerei sono stati immessi sul mercato e si possono suddividere in due macrocategorie: Apparati di Monitoraggio e Contromisure.

Apparati per il monitoraggio di droni

Gli apparati di monitoraggio possono essere passivi (semplice osservazione e ascolto) o attivi (invio di segnali e analisi dei ritorni) e possono svolgere parecchie funzioni incluse:

- Rilevazione
- Classificazione o Identificazione
- Localizzazione e tracciamento
- Allerta

Non tutti gli apparati svolgono contemporaneamente le funzioni sopra descritte, i principali tipi di apparati per il monitoraggio droni sono:

- Analizzatori di Radio Frequenza (RF)
- Sensori Acustici (Microfoni)
- Sensori ottici (Telecamere)
- Radar

Analizzatori di radiofrequenze (RF)

T-Shield Defense S.r.l.

Via Luigi Mainoni d'Intignano, 17/A – 20125 Milano

tel. 02 45482197 – fax 02 84891855 – e-mail info@t-shielddefense.com P.I. 11766490962



Gli Analizzatori RF consistono di una o più antenne per ricevere onde radio e di un processore per analizzare lo spettro RF. Sono usati per ricevere le comunicazioni radio tra un drone ed il suo controllore. Alcuni sistemi sono in grado di identificare i più comuni produttori di droni ed i loro modelli. Alcuni possono anche identificare gli indirizzi MAC del drone e del controllore (se il drone usa il Wi-Fi per le comunicazioni).

Questo è particolarmente utile a fini di azioni penali, si può infatti provare a dimostrare che quel particolare drone ed il suo controllore erano “attivi”. Alcuni sistemi di fascia alta possono anche triangolare il drone ed il suo controllore quando usano più unità radio dislocate in lontananza.

Pro: Sono economici, rilevano (e qualche volta identificano) più droni e controllori, sono strumenti passivi e quindi non richiedono permessi, alcuni possono triangolare la posizione del drone e del controllore.

Contro: Non sempre riescono a localizzare e tracciare i droni, non possono individuare droni autonomi, sono meno efficienti in aree già affollate di radiofrequenze e normalmente sono a corto raggio

Sensori acustici (microfoni)

Normalmente un microfono, o un insieme di microfoni identificare il suono prodotto da un drone e calcolarne la direzione. Più insieme di microfoni possono essere usati per una triangolazione di massima.

Pro: Costi medi, normalmente non localizzano ma possono fornire la direzione del drone

Contro: Non funzionano bene in ambienti rumorosi, operano ad un raggio molto corto (massimo 300-500 metri)

Sensori ottici (telecamere)

Sono essenzialmente delle videocamere. Così come le telecamere standard diurne, i sensori ottici possono essere a infrarossi o ad immagini termiche.

Pro: Forniscono immagini visive del drone e (potenzialmente) anche del suo carico, può registrare le immagini come prova in caso di azione penale

Contro: Difficoltà per il rilevamento automatico, alto numero di falsi allarmi, prestazioni modeste in caso di oscurità, nebbia ecc.

Radar

L'apparato utilizza energia radio per rilevare un oggetto. Un radar invia un segnale e ne riceve il riflesso, misurando direzione e distanza (posizione). La maggior parte dei radar inviano i loro segnali radio a raffica e rimangono in attesa di ricevere “l'eco”. La maggior parte dei radar non sono fatti per rilevare piccoli oggetti. Sono fatti per rilevare masse consistenti, come gli aerei.

Pro: Lungo raggio, tracciamento continuo, localizzazione molto accurate, può gestire simultaneamente centinaia di obiettivi, può tracciare tutti i tipi di drone, anche se a volo autonomo ed indipendentemente dalle condizioni di visibilità (diurno, notturno, nebbia ecc.)

Contro: La capacità di rilevamento dipende dalla dimensione del drone, la maggior parte non distingue un drone da un uccello, richiede licenze per l'utilizzo delle frequenze per prevenire interferenze.

Contromisure contro droni

Le contromisure possono essere raggruppate in:

- Fisiche, in grado di distruggere i droni
- Neutralizzare i droni; o

T-Shield Defense S.r.l.

Via Luigi Mainoni d'Intignano, 17/A – 20125 Milano

tel. 02 45482197 – fax 02 84891855 – e-mail info@t-shielddefense.com P.I. 11766490962



- Prenderne il controllo

È importante chiarire che, sebbene le tecnologie siano disponibili, in quasi tutti i paesi è proibito usare le soluzioni sopra riportate. Ci sono ovviamente eccezioni per strutture militari e agenzie governative.

Localizzare e fisicamente arrestare l'operatore del drone

Un metodo consentito alle forze dell'ordine è quello di localizzare e arrestare l'operatore di un drone, forzandolo a far atterrare il drone. Ovviamente è necessario prima trovarlo.

Disturbatori di radio frequenza (RF Jammers)

Un Jammer RF può essere statico, mobile o manuale. Trasmette una gran quantità di energia RF verso il drone, oscurando il segnale del controllore. Questo produce uno dei quattro scenari descritti di seguito in relazione al tipo di drone.

1. Il drone atterra subito in modo controllato
2. Il drone ritorna nella località predefinita
3. Il drone cade a terra in modo incontrollato
4. Il drone vola via in modo incontrollato

Pro: Costi medi, neutralizzazione non cinetica.

Contro: Corto raggio, può disturbare altre comunicazioni radio, può causare imprevedibili comportamenti del drone, può involontariamente condurre il drone verso il suo obiettivo.

GPS Spoofers

Questi apparati inviano un nuovo segnale al drone, sostituendo la comunicazione con quella dei satelliti GPS usati per la navigazione. In questo modo il drone viene "ingannato" facendogli credere di essere qualcos'altro. Alterando dinamicamente in tempo reale le coordinate GPS. La posizione del drone può così essere controllata da chi ha fatto la manomissione (Spoofer). Una volta ottenuto il controllo del drone può essere diretto, ad esempio, verso una "zona sicura".

Pro: Costi medi, neutralizzazione non cinetica.

Contro: Corto raggio, può disturbare altre comunicazioni radio.

Apparati microonde ad alta potenza (hpm)

Gli Apparati Microonde ad Alta Potenza (HPM) generano Impulsi Elettromagnetici (EMP) in grado di distruggere apparati elettronici. Gli EMP interferiscono con i collegamenti radio e interrompe o addirittura distrugge i circuiti elettronici del drone (più ogni altro dispositivo elettronico nei paraggi) a causa del danneggiamento nel voltaggio delle correnti che crea. I dispositivi HPM possono disporre di un'antenna per puntare l'EMP in una certa direzione al fine di limitare i potenziali danni collaterali.

Pro: Entro una certa distanza il drone può effettivamente essere fermato, neutralizzazione non cinetica.

Contro: Alti costi, rischio di involontarie interruzioni o distruzioni di altri dispositivi elettronici nell'area. Il drone cade istantaneamente a terra in modo incontrollato.

Reti & fucili lancia reti

T-Shield Defense S.r.l.

Via Luigi Mainoni d'Intignano, 17/A – 20125 Milano

tel. 02 45482197 – fax 02 84891855 – e-mail info@t-shielddefense.com P.I. 11766490962



Sparare una rete ad un drone, o comunque portare una rete a contatto con un drone, ferma il drone, bloccando le lame del rotore. Principalmente sono di tre tipi:

- Cannoni di reti sparati da terra: possono essere palmari, poggiati su una spalla, o montati su torretta. Funzionanti da 20 a 300 metri. Possono essere usati con o senza paracadute per una discesa controllata a fini di recupero.
- Cannoni di reti sparati da un altro drone: vengono superati i limiti delle reti sparate da terra ma può essere difficile catturare un altro drone in movimento. Vengono normalmente usati con paracadute per una discesa controllata a fini di recupero.
- Reti sospese dispiegate da un apposito drone di rete. Il drone è catturato manovrando opportunamente la rete verso il drone “nemico”. L’apposito drone di rete è normalmente in grado di portare il drone “nemico” in una zona sicura o, se questo è troppo pesante, farlo scendere con o senza paracadute.

Pro: Cattura fisica del drone – ottimo ai fini di un’azione giudiziaria. Le reti lanciate da cannoni di terra sono semi automatiche e molto precise, le reti sospese sono di lungo raggio e con pochi rischi di danni collaterali.

Contro: potrebbe finire in rottami, a seconda se è stato o meno previsto il paracadute. Le reti sospese sono imprecise e richiedono molto tempo per essere riposizionate. Le reti lanciate da terra hanno un corto raggio.

Laser ad alta energia

Trattasi di un potente dispositivo ottico che produce un fascio di luce molto concentrato, o raggio laser. Il laser abbatte il drone distruggendo la struttura e/o l’elettronica.

Pro: Interruzione fisica del drone.

Contro: Alti costi, rischio di danni collaterali, sistemi grandi, tecnologia per lo più sperimentale.

Uccelli predatori

Alcune aquile sono state addestrate per catturare piccoli droni. Questa è sicuramente una soluzione poco tecnica ma che richiede molte ore uomo per l’addestramento (almeno un anno per uccello) oltre al mantenimento dei rapaci. La Polizia olandese aveva creato un apposito gruppo che è stato però dismesso in quanto gli uccelli non sempre erano disposti a catturare i droni a comando.

Pro: se ci sono uccelli addestrati, l’intercettazione di un drone può essere veloce ed accurata, con un basso rischio di danni collaterali.

Contro: Difficile dal punto di vista operativo, gli uccelli non sono sempre disponibili a catturare droni “a comando”. Lungo e costoso addestramento, gli uccelli stessi potrebbero essere un pericolo in un aeroporto.

Raccomandazione

Gli aeroporti richiedono un sistema integrato

Nessuna delle soluzioni sopra descritte può essere considerata una “bacchetta magica”.

Il più efficiente sistema contro i droni è la combinazione di tutte o parte le soluzioni sopradescritte; un sistema di sistemi.

Il responsabile della sicurezza deve decidere se vuole o può (in una cornice operativa di legalità), combinare insieme soluzioni di monitoraggio e contromisure.

Ma qual è il vantaggio di monitorare se poi non si possono usare contromisure?

T-Shield Defense S.r.l.

Via Luigi Mainoni d’Intignano, 17/A – 20125 Milano

tel. 02 45482197 – fax 02 84891855 – e-mail info@t-shielddefense.com P.I. 11766490962



Una domanda: il vostro allarme antincendio di casa spegne anche l'incendio?

Ma voi avete comunque un allarme antincendio. Corretto? Sarebbe irresponsabile e pericoloso rimuoverlo.

È un cliché, ma è la verità; non puoi gestire quello che non misuri.

Il primo passo per contrastare il problema è capirlo: quanto volte accade, dove succede, che tipo di droni si vedono e qual è il loro intento?

Dovrebbe essere attiva una procedura con l'indicazione di cosa fare quando succede, il cui risultato va basato sulle risposte date ai quesiti sopra descritti.

E per fare questo è necessario un efficiente sistema di monitoraggio droni. Per gli aeroporti e per le infrastrutture critiche è raccomandata una soluzione mista che preveda almeno un radar anti-drone, un dispositivo automatico con telecamera ed un dispositivo di contromisura.

Si può così operare a lungo raggio, con preallarme e con il tracciamento assai accurato del radar. Oltre all'identificazione dei droni e dei controllori tramite i dispositivi RF e alla conferma visiva data dalla telecamera.

Un sistema integrato necessita di un radar microdoppler

Venivano prima elencati i Pro e Contro dei radar e le risposte fanno per lo più riferimento a radar tradizionali

I radar tradizionali non sono in grado di rilevare e tracciare i droni. I sistemi radar di ROBIN Radar funzionano con la tecnologia micro-doppler, una speciale tecnologia radar che consente di rilevare, tracciare e, cosa ancora più importante, classificare i droni.

Nel caso di droni, un radar micro-doppler può identificare se sono presenti eliche, anche piccoli oggetti in movimento – rilevando le differenti velocità delle lamine rotanti. Alcune lamine fanno avvicinare il drone verso il radar e altre lo fanno allontanare.

Con questo metodo, gli uccelli sono facilmente ignorati, perché non hanno eliche. Questa tecnica funziona sia per i quadricotteri (con eliche orizzontali) che per i velivoli ad ala fissa (con eliche verticali).

I radar di ROBIN Radar sono specificatamente progettati per rilevare, classificare e tracciare i droni, superando i “contro” sopracitati.

In particolare:

- Alternativa low-cost ai radar tradizionali
- Classificazione automatica dei droni dagli uccelli, in modo da evitare qualsiasi falso allarme.
- Basso voltaggio, pertanto sicuro per gli operatori e facilitata procedura per l'ottenimento delle concessioni.

In aggiunta può:

- Fornire preallarmi con rilevamento a lungo raggio.
- Rilevare e tracciare droni autonomi che non possono essere identificati dai sistemi RF.
- Fornire una copertura a 360° con una singola unità radar.

T-Shield Defense S.r.l.

Via Luigi Mainoni d'Intignano, 17/A – 20125 Milano

tel. 02 45482197 – fax 02 84891855 – e-mail info@t-shielddefense.com P.I. 11766490962



Micro-Doppler Radar 'ELVIRA'® at Berlin Airport During ILA 2018

Photo Credit: ESG

Conclusioni

Studi hanno dimostrato che la collisione tra un drone ed un aeroplano causa maggiori danni rispetto a quella causata da stormi di uccelli a parità di energia prodotta e che la collisione di un drone con un aeroplano può danneggiare la struttura e causarne anche la caduta.

Oltre alle interruzioni o collisioni involontarie, causate da un operatore di droni che non sa o non conosce le regolamentazioni di sicurezza nelle aree aeroportuali, c'è un rischio aggiuntivo dovuto a coloro che volontariamente decidono di causare interruzioni.

Diverse sono le tecnologie disponibili per monitorare e contrastare i droni. Il monitoraggio è consentito e raccomandato. La neutralizzazione di un drone non è legale nella maggior parte dei paesi.

Le più diffuse tecnologie di monitoraggio comprendono analizzatori di Radio Frequenza (RF), Sistemi Acustici, Telecamere e Radar. Ciascuna tecnologia ha i propri “pro e contro” ed è raccomandabile che i sistemi a difesa di Infrastrutture Critiche per il monitoraggio dei droni siano un'integrazione di:

- RF, per l'identificazione e la triangolazione sia del drone che del controllore (se ci sono segnali radio attivi);
- Telecamere, per l'identificazione visiva e la comprensione del pericolo; e
- Radar, per il rilevamento a lungo raggio, l'accurata localizzazione ed il tracciamento (anche nel caso di sciami di droni e classificazione dei droni anche nel caso di droni autonomi che non inviano alcun segnale radio).

Quando viene usato un radar per il rilevamento di un drone, sia nel caso di un radar “stand alone” o parte di un sistema integrato, dovrebbe essere un radar micro-doppler. I radar micro-doppler sono appositamente progettati per distinguere i droni dagli uccelli. Questo esclude la possibilità di falsi allarmi causati dai volatili, fenomeno frequente con i radar tradizionali.

Le più comuni tecnologie comprendono: Disturbatori di radio frequenza (RF Jammer), GPS Spoofers, Dispositivi Microonde ad Alta Potenza (HPM), Reti e Fucili per lanciare Reti, Laser ad Alta Energia, Uccelli Predatori. Nessuna di queste è consentita dai regolamenti, tuttavia possono essere concesse delle deroghe. In un aeroporto, i fucili per lanciare reti hanno un basso rischio di danni collaterali

Disturbatori RF, GPS Spoofing ed Impulsi Elettromagnetici (EMPs) generati da dispositivi HPM hanno un maggior rischio di danni collaterali in un aeroporto, ma possono essere usati con successo se coordinati e gestiti correttamente.

T-Shield Defense S.r.l.

Via Luigi Mainoni d'Intignano, 17/A – 20125 Milano

tel. 02 45482197 – fax 02 84891855 – e-mail info@t-shielddefense.com P.I. 11766490962



Grazie per la Vostra attenzione

Per maggiori informazioni su come utilizzare un sistema anti-drone integrato con l'utilizzo di radar micro-doppler, per progettare e pianificare un sistema di difesa potete contattare:

Sigint Srl

Giuseppe Ferrara
g.ferrara@sigintsr.it
Mob. +39 320 9525353

T-Shield Defense Srl

Giuseppe Ferrara
g.ferrara@tshielddefense.com
Mob. +39 320 9525353