CENTRO STUDI INTERNAZIONALI

DRONI CIVILI CONTRO OBIETTIVI SENSIBILI E INFRASTRUTTURE CRITICHE: UNA NUOVA TIPOLOGIA DI MINACCIA

Di Paolo Crippa

Marzo 2019

Lo scorso 19 dicembre il traffico aereo dell'aeroporto di Londra-Gatwick è stato interrotto per oltre 36 ore a causa dell'intrusione di un numero non precisato di velivoli a pilotaggio remoto (APR-UAV) di piccole dimensioni, penetrati all'interno del perimetro di competenza dell'autorità aeroportuale. Dopo essere stata informata dell'accaduto da una serie di testimoni oculari, Scotland Yard ha deciso di bloccare le attività dello scalo per ragioni di sicurezza. L'intrusione ha messo in luce la sostanziale impreparazione del dispositivo di sicurezza dell'aeroporto inglese ad affrontare questa nuova tipologia di minaccia. Dopo aver dispiegato 20 squadre di agenti, che non sono riusciti a individuare e a identificare i velivoli, le forze di polizia hanno richiesto l'intervento dell'Esercito. I militari, accanto al supporto logistico, hanno fornito alcuni sniper al fine di individuare e neutralizzare gli aeromobili ostili in maniera convenzionale. Dopo una breve valutazione, tuttavia, l'ipotesi di abbattere i velivoli è stata accantonata, a fronte dei rischi derivanti da una possibile caduta dei proiettili, nonché dell'eventuale drone colpito (che avrebbe potuto eventualmente trasportare esplosivo), all'interno del centro abitato circostante. Nonostante l'intervento delle forze di sicurezza si sia concluso con la riapertura del traffico aereo, gli UAV, quanto i loro piloti, non sono stati tutt'ora identificati. Gli inquirenti hanno escluso potesse trattarsi di uno sconfinamento dettato da un semplice errore umano, e parlano chiaramente di un atto deliberato di disturbo. Le intrusioni all'interno dello spazio aereo di Gatwick, avvenute a più riprese nell'arco della stessa giornata, hanno causato la cancellazione di oltre 800 voli, costringendo a terra più di 140.000 passeggeri, per un danno economico complessivo stimato intorno ai 25 milioni di dollari.

"Le intrusioni all'interno dello spazio aereo di Gatwick hanno causato la cancellazione di oltre 800 voli, costringendo a terra più di 140.000 passeggeri, per un danno economico stimato intorno ai 25 milioni di dollari."

A distanza di tre settimane, in data 8 gennaio 2019, la stessa dinamica si è ripetuta presso l'aeroporto di Heathrow, il primo scalo del Regno Unito, dove l'avvistamento di un UAV non identificato è bastato a bloccare il traffico per circa un'ora. In tale circostanza, la polizia inglese ha impiegato alcuni propri velivoli a pilotaggio remoto per operazioni di ricognizione e identificazione, che tuttavia hanno contribuito soltanto a creare ulteriore confusione, ostacolando la disamina della situazione. Anche in questo

caso rimane sconosciuta l'identità e gli obiettivi del (o degli) operatori del drone. La prossimità temporale dei due episodi ha avuto come immediata conseguenza l'innalzamento del livello d'allerta nei confronti di questa inedita tipologia di minaccia, nonché un complessivo peggioramento della percezione del rischio securitario all'interno del Paese, con specifico riferimento alle infrastrutture critiche. Come sottolineato dal Segretario britannico ai trasporti Chris Grayling in una dichiarazione pubblica, gli episodi di Gatwick e Heathrow rappresentano due *case-studies* estremamente preziosi, non solo per la Gran Bretagna, dal momento che contengono lezioni fondamentali per l'adeguamento dei sistemi di sicurezza pubblica al continuo evolversi delle minacce. Già nel novembre 2018, il Regno Unito, in linea con altri Paesi europei, aveva reso obbligatoria la registrazione di tutti i mini-droni ad uso civile di peso compreso tra i 250g e i 20kg, nonché un certificato di competenze di volo da ottenere online per tutti i futuri piloti. Nel luglio dello scorso anno, inoltre, un'ulteriore legge aveva istituito una *no-fly zone* per gli UAV sugli aeroporti inglesi, con pene fino a 5 anni per i trasgressori. Ciononostante, in luce dei recenti sviluppi, le autorità inglesi starebbero valutando di estendere ulteriormente tale area di interdizione, abbassando il tetto di volo a 400 piedi (122m) ed estendendo il perimetro *no-fly* fino a 3,1 miglia (5km) dalle piste. Nonostante la legislazione vigente, le misure sinora adottate non sono state sufficienti ad impedire le recenti intrusioni. L'azione scoordinata e inefficace delle forze di polizia nel gestire l'emergenza di Gatwick ha, infatti, evidenziato l'urgente necessità di sviluppare una specifica dottrina di contrasto, che coinvolga e coordini l'operato non soltanto delle forze dell'ordine, ma anche degli apparati di sicurezza privata di ciascun aeroporto.

"Gatwick e Heathrow rappresentano due case-studies preziosi, non solo per la Gran Bretagna, dal momento che contengono lezioni fondamentali per l'adeguamento dei sistemi di sicurezza pubblica al continuo evolversi delle minacce."

I profili di rischio associati ai mini-droni sono estremamente specifici e richiedono pertanto precise strategie di contrasto, che devono partire da un'attenta analisi delle loro peculiarità tecniche. Si tratta, innanzitutto, di dispositivi di facile reperibilità, spesso destinati ad uso ludico, che possono essere acquistati sul mercato per poche centinaia di euro. Oggigiorno, la difficile tracciabilità degli acquisti online, nonché la capillare

"I profili di rischio associati ai mini-droni sono estremamente specifici e richiedono pertanto precise strategie di contrasto."

presenza in rete di manuali d'istruzione per la fabbricazione rudimentale di droni a partire da componenti elettroniche di riciclo, (anche con l'ausilio della stampa 3D), rende tale tecnologia disponibile a gruppi o singoli di qualunque estrazione. Come dimostrato dall'esperienza di Gatwick e Heathrow, i droni di piccole dimensioni risultano difficilmente identificabili, dal momento che dispongono di una firma radar estremamente ridotta, che non può essere rilevata dai normali dispositivi di riconoscimento posti a monitoraggio del traffico aereo. Nonostante il sistema di pilotaggio remoto richieda generalmente che l'UAV rimanga all'interno del campo visivo del pilota, o per lo meno ad una distanza non superiore ad 1 km, oggi è possibile impostare preventivamente il percorso del drone mediante un tracciato GPS, consentendogli di operare in completa autonomia e garantendo all'operatore il massimo della copertura. Onde evitare lo sconfinamento all'interno di perimetri sensibili, la maggior parte degli UAV è dotata di 'geo-fences', ovvero barriere virtuali, operanti tramite segnale GPS, che impediscono ai droni di sorvolare luoghi sensibili quali aeroporti, ambasciate, basi militari o istituzioni pubbliche. Nonostante tali misure di sicurezza stiano progressivamente diventando obbligatorie per tutti i dispositivi commercializzati in Europa, le geo-fences possono essere facilmente disabilitate tramite software anche da individui sprovvisti di competenze informatiche specialistiche.

"I droni di piccole dimensioni risultano difficilmente identificabili, dal momento che dispongono di una firma radar estremamente ridotta."

La versatilità, la reperibilità, nonché la facilità d'impiego, rendono i droni una tecnologia particolarmente adatta ad azioni criminali o terroristiche. Una delle principali modalità attraverso cui un mini-UAV può effettuare un attacco prevede la dispersione sulla folla di materiale esplosivo, chimico o batteriologico. Nonostante, ad oggi, in Occidente non si siano ancora verificati episodi di tale natura, la capacità dello Stato Islamico di compiere attacchi tramite l'utilizzo di IED installati su UAV, comprovata dall'esperienza all'interno del teatro siriano, rende impossibile escludere ogni rischio. Occorre ricordare, ad esempio, che nel giugno dello scorso anno, in occasione dei mondiali di calcio, il gruppo jihadista aveva diffuso un video in cui si paventava un attacco sistematico nei confronti degli stadi di Mosca, compiuto tramite droni esplosivi.

"La versatilità, la reperibilità, nonché la facilità d'impiego, rendono i droni una tecnologia particolarmente adatta ad azioni criminali o terroristiche."

Chris Eaton, ex responsabile della sicurezza della FIFA, ha inoltre sottolineato lo scorso 22 gennaio in un articolo sul Daily Telegraph, come gli esperti di sicurezza da anni ormai paventano questo tipo di rischi negli stadi. Tale modalità d'azione risulta particolarmente insidiosa e pone seri problemi alle forze impegnate nelle attività contrasto, dal momento che la presenza di esplosivo a bordo dell'aeromobile rende impossibile neutralizzare la minaccia tramite mezzi convenzionali, come ad esempio un fucile di precisione o un'arma ad energia. Far precipitare un drone carico di materiale nocivo su un agglomerato urbano o su una folla significherebbe infatti portare a compimento l'azione criminale, contribuendo direttamente a massimizzarne i danni.

I mini-UAV sono inoltre in grado di arrecare ingenti danni con il semplice impatto cinetico, in particolar modo ad altri aeromobili in movimento. Secondo recenti studi condotti dall'Università di Daytona, un drone di soli 2kg può danneggiare irrimediabilmente le ali o il cockpit di un aereo di linea con il semplice contatto, qualora l'impatto avvenga ad una velocità superiore ai 200km/h.

Un ulteriore scenario, meritevole di seria considerazione al fine di valutare rischi e contromisure, è quello che vede un UAV piombare, o anche solo stazionare, su di un'area estremamente affollata. Il semplice sospetto che possa costituire una minaccia (trasportando ad esempio un IED), può generare panico tra gli astanti, innescando dinamiche di irrazionalità collettiva difficilmente controllabili ed estremamente pericolose per l'integrità fisica delle persone.

Oggi, dall'analisi dell'evoluzione delle diverse dottrine di guerra ibrida, condotta parimenti da attori statuali e non, emerge come il danno economico giochi un ruolo sempre più centrale all'interno delle strategie di offesa. Nonostante non sia assimilabile, in particolar modo sul piano morale, alla perdita di vite umane, paralizzare infrastrutture critiche, evidenziare vulnerabilità di sistema, indurre fughe di capitali o peggiorare sensibilmente l'attrattività di un mercato nazionale, può avere un impatto incredibilmente significativo sullo stato di salute e sulla resilienza dell'intero

"Anche il semplice sospetto che un mini-UAV possa costituire una minaccia (trasportando ad esempio un IED), può generare panico tra la folla, innescando dinamiche di irrazionalità collettiva difficilmente controllabili."

Sistema Paese. In quest'ottica, l'esperienza di Gatwick mostra come il semplice transito di un UAV all'interno di un perimetro interdetto, può infliggere perdite complessive nell'ordine dei milioni di dollari, senza contare esternalità negative nel medio periodo. È proprio la profonda disproporzione tra il capitale (umano, tecnologico, di rischio) investito nell'azione di disturbo e l'effetto sortito, tra le altre cose, a rendere i mini e micro-droni estremamente adatti a finalità terroristiche.

Per quanto riguarda l'attività di contrasto vero e proprio, l'azione delle forze di polizia inglesi ha evidenziato la mancanza di una chiara strategia operativa e di una razionale ripartizione dei compiti tra operatori civili e militari. In tale ambito, dove le Forze Armate hanno acquisito negli anni un capitale di conoscenze tecniche ed esperienza nettamente maggiore rispetto alla controparte civile, risulta fondamentale l'interscambio di informazioni e know-how, nonché attività congiunte di training, al fine di dotare anche le polizie nazionali delle capacità necessarie. Un ulteriore interrogativo, dunque, a cui saranno chiamati a rispondere i singoli Stati secondo le diverse sensibilità ed esigenze operative, riguarderà a quale componente dell'apparato di sicurezza nazionale affidare i compiti di contrasto ai velivoli a pilotaggio remoto (C-UAS). Un elemento dirimente, nella scelta se dotare di tale capacità una singola forza di intervento rapido a livello nazionale, un corpo di gendarmeria o ciascuno degli apparati di sicurezza dei principali scali aeroportuali, rimane certamente la disponibilità economica di ciascun Paese.

Sul fronte tecnologico, oggi le principali industrie della difesa, ma anche un nutrito network di piccole-medie aziende e start-up, stanno cercando di adeguare la propria offerta per rispondere ad una domanda in rapida ascesa. Attualmente, la maggior parte dei prodotti presenti sul mercato appartiene ad una fascia "alta", sia di sofisticazione tecnologica che di prezzo. Si tratta di dispositivi di difesa elettronica ideati in primo luogo per rispondere alle complesse esigenze delle Forze Armate. Tra le principali tecnologie C-UAS attualmente sul mercato, ricordiamo ad esempio il sistema DRONE DOME prodotto dall'israeliana Rafael Advanced Defence Systems di cui si sta dotando

"Sul fronte tecnologico, oggi le principali industrie della difesa, ma anche un nutrito network di piccole-medie aziende e start-up, stanno cercando di adeguare la propria offerta per rispondere ad una domanda in rapida ascesa."

l'aeroporto di Gatwick, o l'AUDS (Anti-UAV Defence System) schierato dal 22° reggimento SAS in occasione del matrimonio del Principe Harry, sviluppato da un consorzio di aziende inglesi. Sebbene gli Stati Uniti (Boeing, Battelle), e in particolar modo Israele (Rafael ADS, IAI), dominino attualmente il mercato tecnologico, l'Italia è presente con due prodotti estremamente all'avanguardia: il Falcon Shield sviluppato nel 2015 da Selex ES (oggi parte di Leonardo) e il sistema ADRIAN (Anti DRone Interception Acquisition and Neutralization) del gruppo Elettronica.

La soluzione integrata Falcon Shield è costituita da una serie di componenti elettro-ottici, tra cui il sistema modulare a lungo raggio NERIO-LR per sorveglianza e acquisizione, il sistema di ricognizione a lunghissimo raggio NERIO-ULR che integra la telecamera termica ad alte prestazioni Horizon, nonché da una suite di piattaforme e software di comando e controllo. Tale sistema consente il rilevamento della minaccia UAV in modalità multispettrale e, attraverso l'integrazione di una capacità di attacco elettronico, permette di acquisire il controllo di un drone e di condurlo a terra in modo sicuro, senza passare necessariamente ad un 'hard-kill' vero e proprio, condotto tramite disturbo elettromagnetico o dinamico, riducendo notevolmente eventuali danni collaterali.

L'ADRIAN, invece, testato dalla Polizia di Stato e frutto della stretta collaborazione tra lo stabilimento romano del gruppo e quello tedesco di Elettronica GmbH, con sede a Meckenheim, è un sistema appositamente ideato per l'impiego all'interno di aree particolarmente affollate, come possono essere piazze, stadi, aeroporti o altri obiettivi sensibili, con l'obiettivo specifico di ridurre sensibilmente i rischi relativi al precipitare del velivolo colpito a terra. ADRIAN, costituito da cinque sensori passivi Radio Control Interceptor collegati ad una stazione di controllo, ubicata all'interno di un van e gestita da un singolo operatore, è in grado di fondere i flussi di dati (acustici, elettro-ottici e radar) tramite un sofisticato algoritmo, al fine di individuare e localizzare il velivolo ostile e il suo operatore. Una volta concluse le operazioni di identificazione, è possibile procedere con la neutralizzazione tramite l'antenna di jamming presente sul van, interrompendo la

comunicazione tra il velivolo e il suo pilota, anche nel caso in cui il drone sia stato programmato per seguire una traiettoria preimpostata tramite GPS.

In generale, si tratta di sistemi di derivazione militare, dove la sensibilità dei dispositivi di rilevamento e l'estensione dell'area di copertura si traducono in costi estremamente elevati, generalmente nell'ordine dei milioni di dollari. Sino ad ora, infatti, i radar in grado di rilevare "piccoli oggetti volanti non cooperativi" erano appannaggio quasi esclusivo di società che avevano precedentemente sviluppato radar militari tradizionali per il rilevamento degli aeromobili, con un costo e una potenza (generalmente intorno ai 10W) poco adatti per il campo civile. Robin Radar Systems, l'azienda olandese rappresentata in Italia da Sigint, ha sviluppato invece due prodotti innovativi di grande efficacia: ELVIRA, concepito espressamente per gli UAV, di dimensioni contenute, trasportabile su pick-up e con una potenza di 4W, e MAX, originariamente progettato come radar ornitologico aeroportuale, che permetterà a breve anche di individuare ogni tipo di aeromobile a pilotaggio remoto.

"Robin Radar Systems, azienda olandese rappresentata in Italia da Sigint, ha sviluppato due prodotti innovativi di grande efficacia: ELVIRA, concepito espressamente per gli UAV, e MAX, originariamente progettato come radar ornitologico aeroportuale."

ELVIRA è un prodotto specificamente ideato per il rilevamento e il monitoraggio degli UAV, composto da un sistema radar integrato con un software intelligente che permette di ridurre al minimo i tempi di allarme in presenza di droni in avvicinamento da qualsiasi direzione, permettendo di reagire in tempi brevissimi. ELVIRA si distingue per la sua estrema versatilità. Può operare infatti agevolmente anche in condizioni di scarsa visibilità, all'interno di aree urbanizzate, in presenza di ostacoli fissi o in movimento, nonché in condizioni di inquinamento elettromagnetico. Il dispositivo inoltre, è efficace sia contro singoli aeromobili a pilotaggio remoto, sia contro sciami, siano essi teleguidati o programmati per il volo autonomo senza operatore. Il radar, con la sua capacità micro-Doppler, fornisce la necessaria conferma che il bersaglio ha una propulsione meccanica. In aggiunta, per una conferma visiva, il sistema è predisposto per una telecamera ad alta risoluzione brandeggiabile e zoomabile automaticamente sul bersaglio. A differenza dei sistemi di rilevamento di derivazione militare, ELVIRA dispone di un'interfaccia

utente estremamente intuitiva, che può essere gestita con facilità anche da operatori civili che non abbiano intrapreso un percorso di training specialistico. Tali caratteristiche, unite alla facilità di configurazione e alla possibilità di integrare le tracce e gli allarmi di ELVIRA come livello nei sistemi di sicurezza e comando e controllo (C2) di terze parti, rendono questo dispositivo estremamente adatto alle esigenze C-UAS di infrastrutture critiche di qualsiasi ordine di dimensione.

Sempre la Robin Radar System produce un altro dispositivo denominato MAX. Si tratta di un sistema di rilevamento estremamente sofisticato, caratterizzato dalla più alta velocità di rotazione disponibile oggi sul mercato, che permette l'aggiornamento della traccia ogni secondo, consentendo di visualizzare in modo univoco e dettagliato i percorsi di volo, tanto degli uccelli quanto degli UAV, direttamente su Google Earth. MAX è un sistema a sensore singolo che offre informazioni tridimensionali su tutti gli uccelli nell'ambiente circostante, con un raggio di copertura esteso fino ad un'altezza di circa 1.000 metri. Parallelamente a ELVIRA, anche il sistema MAX dispone di un ambiente software estremamente intuitivo, che lo rende particolarmente adatto a rispondere a esigenze operative in campo civile.

Nonostante, ad oggi, gli episodi di reale pericolo derivanti dall'intrusione di mini-UAV abbiano riguardato un numero estremamente esiguo di casi, è lecito pensare che, nel breve-medio periodo, contrastare tale tipologia di minaccia diventerà un'esigenza prioritaria. Al fine di fornire una risposta efficace a garantire la sicurezza non solo delle infrastrutture critiche, ma anche di obiettivi civili particolarmente sensibili (come avvenimenti pubblici, manifestazioni, concerti o summit internazionali) risulta indispensabile favorire la creazione di sinergie tra gli apparati di sicurezza pubblica e privata e il mondo delle aziende, attraverso la regia delle istituzioni nazionali.

"Risulta indispensabile favorire la creazione di sinergie tra gli apparati di sicurezza pubblica e privata e il mondo delle aziende, attraverso la regia delle istituzioni nazionali."