Terrorismo: una risposta alla sfida dei droni

Comunemente chiamati "droni", gli aeromobili a pilotaggio remoto (APR, ai quali ci si riferisce anche con gli acronimi UAV, RPA o UAS) hanno visto un incremento esponenziale delle vendite negli ultimi anni[1]. La tecnologia degli APR per fotografia e videografia di piccole dimensioni[2] si è evoluta a tal punto da offrire prodotti accessibili al consumatore medio, con prezzi simili a fotocamere digitali con caratteristiche qualitative praticamente identiche[3]. Rappresentano dunque un interessante caso di studio, includendo già nella loro forma originale un sistema di cattura immagine relativamente avanzato e avendo una capacità di volo tale da sopportare un carico utile (*payload*) maggiore rispetto a quello indicato dalle impostazioni di fabbrica, il che permette migliori stabilità e manovrabilità.

Già senza subire alcuna manomissione, possono essere utilizzati per violare la privacy e/o infrangere la normativa sulle zone non sorvolabili. Negli USA è sorto il problema dell'individuazione dei colpevoli anche di semplici infrazioni della legislazione sul volo[4]; mentre in Europa, i casi dei droni sugli aeroporti inglesi di Gatwick e Heathrow hanno evidenziato il potenziale di queste tecnologie nel creare disordine e disagi[5].

I sistemi di geo-fencing[6] di cui questi apparecchi sono dotati risultano fallibili. Il processo per rimuovere il GPS è abbastanza semplice – il drone viene poi manovrato basandosi solo su ciò che il sistema di raccolta immagini integrato trasmette. Anche il software appare disattivabile scaricando programmi dal web[7] o, in alcuni casi, risulta virtualmente inesistente[8].

---

1 European Commission (2014), "Remotely Piloted Aviation Systems (RPAs) – Frequently Asked Questions", p. 2 Link: https://bit.ly/2J2gmX9
European Aviation Safety Agency (2016). "Explanatory Note", *Prototype Commission Regulation on Unmanned Aircraft Regulation,* p. 13. Link: https://bit.ly/2IZFpKq

2 CLASSIFICAZIONE AEROMOBILI A PILOTAGGIO REMOTO

Categoria	*Raggio operativo (km)*	*Quota di volo (m)*	*Durata del volo (h)*	*MTOW (kg)*
Nano	< 1	100	< 1	< 0,0250
Micro	< 10	250	1	< 5
Mini	< 10	150 – 300	< 2	< 30

3 Una Canon Reflex entry-level, quale la EOS 1300D, è venduta sul sito ufficiale della Canon per € 470,99. Nella stessa fascia di ricadono anche le Nikon, per esempio la Nikon D3400.I droni delle serie Phantom e Mavic, le più famose dell'azienda cinese DJi, leader nel settore, hanno un prezzo compreso tra i 500 e i 1.200 dollari e sono tra i più venduti al mondo. Nel 2017, la DJi deteneva oltre il 36% del mercato nordamericano per questa tipologia di prodotti.
Chandler, C. (2017). "For China's high-flying drone maker, the sky's the limit", *Fortune*. Link: https://bit.ly/2vt9BWr
Glaser, A. (2017). "DJi is running away with the drone market", *Recode*. Link: https://bit.ly/2nNIhkd

4 Un esempio è il Caso Neistat a Manhattan.
P.A. Aitken (2017) "Copy of FAA message sent. Casey Neistat investigation lacks conclusive evidence", *Taitkenflight*. Link: https://bit.ly/2W2f5SY;
Andy (2017) "EXCLUSIVE: Details of Casey Neistat's FAA investigations", *Andy's Travel Blog*. Link: https://bit.ly/2TfKoli.

5 BBC (2018), "Gatwick airport: Drones ground flights", *BBC*. Link: https://bbc.in/2EvX5uW
BBC (2019), "Heathrow airport drone investigated by police and military", *BBC*. Link: https://bbc.in/2Hs4768
BBC (2019), "Heathrow airport: Drone sighting halts departures", *BBC*. Link: https://bbc.in/2RokRAL

6 "Geo-fencing is the concept of restricting drone access by designating specific areas where the drone's soft- ware and/or hardware is designed not to enter, even if the pilot, without intent, instructs the drone to go" European Aviation Safety Agency (2015), "Concept of Operations for Drones…", *ibidem*.

7 Ryan Whitman (2017) "Russian Company Is Selling Mods to Bypass DJI Drone Safety Features", *Extreme Tech*. Link: https://bit.ly/2YCHFj6

8 Dalle interviste condotte con appassionati del settore risulterebbe infatti che, nel momento in cui il drone DJi si avvicina ad aree non sorvolabili, l'operatore viene allertato con un avviso pop-up. Accettando l'avviso, il drone continua comunque a funzionare ed è ancora da accertare se e come il sistema di geo-fencing si comporterebbe in questo caso. Qui sotto si riporta il testo del pop-up che appare su un drone di marca DJi —

Nel teatro operativo siro-iracheno, i primi report sull'uso di 'droni' o 'droni armati' da parte di ISIS[9] risalgono al 2014 ed includono lo spionaggio dei movimenti delle linee nemiche curde e statunitensi nelle battaglie tra il 2014 e il 2017 in Iraq, il rilascio di esplosivi o l'uso di 'droni kamikaze'[10]. Molte sono le ragioni che hanno consentito ad ISIS di includerli nel proprio arsenale: l'acquisto anche per prodotti di seconda mano sul mercato online è semplice. Hanno dimensioni e volano ad altezze tali da non attirare l'attenzione dei radar né degli scudi protettivi, allo stesso tempo essendo difficili da vedere o *engage* dal personale a terra[11]. È facile manometterli e possono essere armati in diverse maniere. Da ultimo, servono il doppio scopo di offrire un'arma e al contempo le immagini delle loro attività: i video possono essere usati per propaganda, come già nel tardo 2017[12].

Questa tipologia di APR ha dunque il potenziale per divenire una seria problematica di sicurezza nazionale. Il ruolo della Difesa assurge a fondamentale, soprattutto nell'identificazione di possibili soluzioni e/o risposte a breve, medio e lungo termine, che garantiscano la sicurezza della popolazione civile in patria. Una risposta concertata tra Forze Armate e Forze dell'Ordine appare auspicabile[13].

In prima analisi, sorge il problema dell'individuazione dei potenziali obiettivi sensibili, più difficili da determinare rispetto alle infrastrutture critiche[14]. Il rischio sarebbe quello di dover 'coprire' con sistemi anti-drone l'intero territorio nazionale – un obiettivo, al momento, irraggiungibile per tempistiche, costi e livello della tecnologia attuale.

Sorge dunque la necessità di sviluppare un sistema integrato di *search, find and ID* totalmente automatizzato. Due le motivazioni: le tecnologie attualmente disponibili sul mercato non presentano un rapporto costi-benefici soddisfacente, considerato l'investimento necessario ad acquisirle; in secondo luogo, un sistema *fully automated*, avendo la capacità di resistere alla saturazione, esenterebbe dal mantenimento del *man in the loop*[15], in previsione di un futuro in cui gli attacchi possano essere condotti da *swarms*[16]*.* Attenzione particolare andrebbe dunque posta nei confronti della tempestività di reazione ed intervento, che si lega alla questione dell'*engagement*.

"**No-Fly Zones.** There are 1 Authorization Zone(s) nearby. Authorization zone type: Military Facility(Military Zones). Your aircraft may experience RTH interruption, hovering, or Intelligent Flight Mode cancellation. Please fly with caution. Do you wish to apply for Self-Unlocking to access these zones? No / Yes"

9 "[ISIS] è un progetto politico di lungo termine con confini mobili […] Frutto delle idee di Abu Musab al-Zarqawi, proclamato "Califfato" il 29 giugno 2014 da Abu Bakr al Baghdadi, ha ridisegnato la geografia del Medio Oriente cancellando i confini di Iraq e Siria prodotti dagli accordi di Sykes Picot del 1916. Si proietta contro gli stati postcoloniali che sorgono all'interno della mappa di "Bilad al Sham", la leggendaria nazione araba del Levante che corrisponde agli attuali territori di Iraq, Siria, Giordania, Libano, Israele e Autorità nazionale Palestinese", cit. M. Molinari (2015), "Il Califfato del terrore. Perché lo Stato Islamico minaccia l'Occidente", *Rizzoli*, pp. 10-11.

10 Peter Bergen e Emily Schneider (2014) "Now ISIS has drones?", *CNN.* Link: https://cnn.it/2SMwMWm
Ben Watson (2017) "The Drones of ISIS", *Defense One*. Link: https://bit.ly/2YmIus0
Mike Peshmerganor (2018), ***Blood Makes the Grass Grow: A Norwegian Volunteer's Fight Against the Islamic State,*** Independently Published.

11 L. E. Davis et al. (2014) "Armed and Dangerous? UAVs and U.S. Security", *RAND Corporation*. Link: https://bit.ly/2LMqWUu

12 In questo caso, si fa riferimento ad un video, circolato su internet dall'agenzia Amaq (affiliata ad ISIS) e rilanciato da ABC News (https://ab.co/2Ybr6en), in cui si vedeva un drone sganciare munizioni su un deposito di armamenti siriano. Nonostante lo scetticismo dell'autore di questo studio sull'autenticità delle immagini, rimane innegabile il potenziale propagandistico di queste tecnologie. Link al video: https://bit.ly/2Yxz9BH

13 Al momento, infatti, sono dotati di sistemi jammer i servizi centrali di Polizia, i quali sono coinvolti in casi di esigenza specifica, oppure gli uffici in cui vengono discussi argomenti riservati, al fine di effettuare le bonifiche periodiche.

14 Decreto Legislativo 11 aprile 2011, n. 61, in attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione.
Testo del Decreto Legislativo: https://bit.ly/2NRjMQj
Testo della Direttiva europea: https://bit.ly/2Y6pUZ8

15 "*Human-in-the-loop* (HITL). A model that requires human interaction." Cit. USA Department of Defense (1998), "DoD Modeling and Simulation (M&S) Glossary", DOD 5000.59-M, p. 124 (enfasi nel testo).

16 "UAV swarms, inspired mainly by the swarms of insects, are groups of small independent unmanned vehicles that coordinate their operations through autonomous communications to accomplish goals as an intelligent group, with or without human supervision. It may be a heterogeneous mix of machines with dissimilar tasks but contributing

L'obiettivo a lungo termine dovrebbe presupporre lo sviluppo di sistemi che possano agire sugli algoritmi di controllo al fine di "rubare" il drone – il che permetterebbe di farlo atterrare in una zona sicura. Il pericolo infatti non deriva solo dal rischio di un drone armato balisticamente e/o con esplosivo, ma anche CBRN[17]. Si necessita dunque di un protocollo che preveda una zona di quarantena, nella prospettiva di salvaguardare non solo la popolazione civile, ma anche il personale specializzato addetto.

Essendo comunque questo un obiettivo non raggiungibile nel breve periodo, va effettuata un'analisi dei costi/benefici relativi alle attuali possibilità di *engagement*. Nella conduzione di tale analisi, rimangono sempre da ricordare i problemi relativi alla TIPOLOGIA DI COMANDO del drone (pilotato a distanza o con route preimpostata) e alla TIPOLOGIA DI ARMAMENTO (il rilascio della carica esplosiva/CBRN avviene con comando manuale del pilota, o quando il drone si trova su determinate coordinate, o con timer).

I possibili *outcome* sono sostanzialmente quattro. Perso il segnale con il telecomando, il drone può rimanere in fase di stallo (*frozen*) a mezz'aria, fare ritorno al punto in cui si trova il telecomando, o atterrare. In assenza di un sistema *fail-safe*[18], potrebbe schiantarsi al suolo[19]: in questo caso, se dotato di carica esplosiva, potrebbe detonare; se armato con cariche CBRN, queste nell'impatto potrebbero contaminare l'area.

Una prima opzione di tecnologia anti-drone riguarderebbe l'impiego di *jammer*, traslando il loro utilizzo dal teatro operativo come *counter-IED system*[20]. Il loro impatto su tecnologie e infrastrutture civili se utilizzate in territorio urbano rimane da valutare caso per caso[21]. Considerando le relativamente brevi distanza e durata di volo di droni con potenziale malevolo, l'assenza di un sistema *jammer* in loco, mobile[22] o fisso, comporterebbe un mancato *engagement*.

---

synergistically to the overall mission objectives", cit. Puneet Bhalla (2015), "Emerging Trends in Unmanned Aerial Systems", *Scholar Warrior*, Autumn 2015, p. 89.

17 Chemical, Biological, Radiological and Nuclear.

18 Definitions of "fail-safe" —
(American English): *adj*. "[D]esignating, of, or involving a procedure designed to prevent malfunctioning or unintentional operation […]".
(British English): *adj*. "Something that is fail-safe is designed or made in such a way that nothing dangerous can happen if a part of it goes wrong".
Collins Dictionary, link: https://bit.ly/2Y98T1i

19 Durante una gara di droni svoltasi a Torino nell'estate 2019, un attacco hacker al Wi-Fi dell'organizzazione ha reso i droni incontrollabili da parte degli operatori. Questo è dovuto al fatto che tutti gli APR erano telecomandati a distanza sulla stessa rete Wi-Fi, offerta dagli organizzatori – dunque, attaccare questa infrastruttura equivaleva ad un attacco cyber che non aveva nessun effetto diretto sui droni (non si interveniva infatti sulle macchine), bensì sulla comunicazione wireless in senso lato. Le cause dell'"impazzimento" sono da ritrovarsi nel fatto che questi APR fossero droni da corsa di fattura artigianale, presumibilmente senza alcun sistema di *fail-safe*, già lanciati a forte velocità nel momento in cui l'attacco li ha scollegati dai loro telecomandi.
Alessandro Contaldo (2019), "Attacco hacker alla drone race: i quadricotteri fuori costretti ad atterraggi di emergenza", *La Repubblica*. Link: https://bit.ly/2NPVGv

20 Qui di seguito si forniscono alcune definizioni —
"An improvised explosive device (IED) is a type on unconventional explosive weapon that can take any form and be activated in a variety of ways. They target soldiers and civilians alike. In today's conflicts, IEDs play an increasingly important role and will continue to be part of the operating environment for future NATO military operations. NATO must remain prepared to counter IEDs in any land or maritime operation involving asymmetrical threats, in which force protection will remain a paramount priority." in NATO (2018), *Improvised explosive devices*, www.bit.ly/2Ykd4qb.
"**Electronic Warfare:** The use of electromagnetic (EM) or directed energy to exploit the electromagnetic spectrum. It may include interception or identification of EM emissions (es.: SIGINT), employment of EM energy, prevention of hostile use of the EM spectrum by an adversary, and actions to ensure efficient employment of that spectrum by the user-State. An example of electronic warfare is radio frequency jamming" in Michael N. Schmitt, editor (2016), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, p. 565 (enfasi nel testo).

21 L'utilizzo di jammer di uso comune (civili) è legale, ancorché vengano rispettati i limiti di emissione ed esposizione previsti per legge e non causino interruzione di pubblico servizio (art. 340 del Codice Penale). Le Forze Armate e dell'Ordine possono farne uso in casi particolari, quando cioè operano *in deroga*, per es. per questioni di pubblica sicurezza, protezione di personalità, ordine pubblico *et simili*.

22 Come può essere, per esempio, la pistola jammer Wilson.

I sistemi fissi in ambienti urbani possono però presentare problematiche riguardanti il rumore di sottofondo.

Una seconda ipotesi sarebbe l'utilizzo di armi convenzionali balistiche allo scopo di abbattere il drone, o eventualmente armate con proiettili a rete[23]. Questa opzione andrebbe in realtà considerata solo come una *last resort*, per le motivazioni riguardanti la tipologia di armamento riportate sopra. Indubbio è comunque il rischio per la popolazione civile, nel caso la minaccia si materializzasse in luoghi affollati.

Una terza opzione sarebbe l'uso di rapaci. La reattività di questi animali e il loro impatto economico li rendono una competitiva soluzione a breve termine. Un nucleo di falconeria è stimato ad un costo massimo di 50.000€ – ciò significa che, con un budget di tre milioni[24], si potrebbero installare circa sessanta nuclei di falconeria. Il costo per il mantenimento di un singolo nucleo non supererebbe le poche decine di migliaia di euro all'anno[25].

Una quarta opzione riguarderebbe le armi ad emissione di onde radio, tra le quali un sistema di manifattura americana: nonostante le specifiche siano interessanti, ricade nella categoria necessitante l'autorizzazione della Federal Communications Commission per essere venduto o affittato ad utilizzatori non-federali[26].

Infine, interesse crescente stanno acquisendo le armi ad energia diretta – come il dispositivo Counter Unmanned Aerial System (C-UAS) messo a disposizione dei fucilieri del 16° Stormo dell'Aeronautica Militare durante la visita del Presidente russo Vladimir Putin a Roma nel luglio 2019: si tratta di un "sistema radar di rilevamento munito di dispositivi e ottiche diurne e notturne per l'interdizione elettronica del volo"[27].

Sul breve termine, appare come una soluzione percorribile la costituzione di un progetto pilota che utilizzi un nucleo di falconeria al fine di monitorare situazioni eccezionali che presentano un'alta concentrazione di persone, ed eventualmente intervenire in caso di necessità, quali per esempio la S. Messa domenicale in Vaticano o le future Olimpiadi invernali di Milano-Cortina 2026.

Andrebbe inoltre accentuato il lavoro di scambio di informazioni tra Forze Armate, intelligence e Forze dell'Ordine, con l'obiettivo di prevedere possibili trend basandosi sulle manomissioni definite come "apportabili" in rete da hobbisti, appassionati e/o attori malintenzionati. Sarebbe infatti da evitare il ragionamento per il quale una possibile manomissione, non risultando funzionante, possa essere scartata dall'elenco delle possibili minacce: nel momento in cui l'idea per l'utilizzo di un APR viene messa in circolo, essa andrebbe considerata come attuabile, nell'immediato o in un più distante futuro.

23 COMFOTER SPT (2018), "Sperimentazione antidrone del COMACA", *Esercito*. Link: https://bit.ly/2HeeZnR
Stato Maggiore Esercito (2018), "Sperimentazione antidrone del COMACA", *Difesa Online*. Link: https://bit.ly/32Xf9b5
Maurizio Tortorella (2019), "Abbattete quel drone", *Panorama*. Link: https://bit.ly/2GwHUBF.
Secondo indiscrezioni, queste esercitazioni sarebbero state condotte utilizzando fucile Beretta calibro 12.

24 La scelta di questo dato non è casuale. Apparentemente, il sistema 'Drone Dome', di manifattura israeliana, usato presso l'aeroporto di Gatwick contro il drone che aveva causato lo stop del traffico aereo sarebbe costato al Regno Unito circa 2.6 milioni di sterline – al cambio attuale, quasi 2.9 milioni di euro.
Joe Pinkstone (2018), "The £2.6m Israeli 'Drone Dome' system that the Army used to defeat the Gatwick UAV after the technology was developed to fight ISIS in Syria", *Daily Mail Online*. Link: https://dailym.ai/2T4PKXb

25 Come risulta da alcune stime fatte da esperti del settore in sede d'intervista.

26 Si tratta del DronekillerTM, prodotto dalla IXI Technology. Sito aziendale: https://bit.ly/30ZSOaU
IXI Technology, documento recante le specifiche del Dronekiller: https://bit.ly/2Ykc5ax

27 Cit. da Ministero della Difesa / Stato Maggiore della Difesa (2019), "Le Forze Armate concorrono alla cornice di sicurezza per la visita del Presidente Putin", *Difesa. Link:* https://bit.ly/2YzxkF4

Tutti gli indirizzi web indicati nel presente studio sono stati consultati in ultima istanza il 27 settembre 2019.