



Center for Cyber Security and  
International Relations Studies

# *Droni civili per terrorismo, quali soluzioni al problema*

Ginevra Fontana



UNIVERSITÀ  
DEGLI STUDI  
FIRENZE

**Research Analysis**

*Novembre 2018*



## **Center for Cyber Security and International Relations Studies (CCSIRS)**

Centro Interdipartimentale di Studi Strategici,  
Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

**<https://www.cssii.unifi.it/ls-6-cyber-security.html>**

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.



Center for Cyber Security and  
International Relations Studies

# ***Droni civili per terrorismo, quali soluzioni al problema***

**Ginevra Fontana**



UNIVERSITÀ  
DEGLI STUDI  
FIRENZE

**Research Analysis**

*Novembre 2018*

## Riguardo all'autore

**Ginevra Fontana** Si è laureata in Studi Internazionali presso l'Università di Trento, con una tesi sul diritto delle minoranze come strumento della sicurezza internazionale, analizzando il caso dei parlanti lingua russa in Lettonia. Frequenta il corso di Laurea magistrale in Studi sulla Sicurezza Internazionale presso la Scuola Superiore Sant'Anna e l'Università di Trento. Dal 2014 è Allieva del Collegio Bernardo Clesio. Si interessa principalmente di terrorismo, cyber sicurezza, conflitti armati, diritto delle minoranze, traffico d'armi e cooperazione tra forze armate. È co-autrice dell'articolo "Drone warfare in Niger", pubblicato su SecurityPraxis.eu nel Novembre 2017.

## **Droni civili per terrorismo, quali soluzioni al problema<sup>1</sup>**

Prezzi accessibili, misure ridotte che li rendono una perfetta arma-in-potenza e facilità di modifica. Sono molte le ragioni per cui i droni civili sono sempre più usati dai gruppi terroristici. I possibili argini alla loro proliferazione incontrollata anche fuori da zone di guerra, dal geofencing a norme specifiche. Dalla proliferazione di droni ad uso civile per videografia e fotografia derivano una serie di problematiche particolarmente difficili da risolvere, che non si limitano al semplice rischio di schianto al suolo — che non va sottostimato. Altri rischi riguardano la privacy: droni dotati di fotocamere che operano in aree ad alta densità abitativa espongono a violazioni di privacy, permettendo la raccolta dati in luoghi altrimenti difficilmente accessibili, quali finestre poste ai piani superiori degli edifici, balconi, tetti. Va tenuto presente che queste attività, di per sé illegali se considerate alla luce del regolamento ENAC, possano accadere indipendentemente dalle intenzioni dell'operatore. È importante sottolineare che queste tecnologie stanno diventando una problematica di sicurezza anche per un altro motivo: sono molto difficili da identificare. Come evidenziato da Davis et al<sup>2</sup>, i droni per videografia e fotografia venduti correntemente hanno dimensioni e volano ad altezze tali da renderli difficilmente identificabili dai radar e particolarmente difficili da abbattere utilizzando armi convenzionali da parte delle forze di terra. Un drone della serie Phantom della DJi può volare fino ad un massimo di 7 chilometri di distanza dall'operatore prima di perdere il segnale. Ciò rende questi apparecchi dei possibili

---

<sup>1</sup> La seguente analisi è apparsa su [Agenda Digitale](https://www.agendadigitale.eu/sicurezza/droni-civili-a-scopo-offensivo-problemi-e-soluzioni/) il giorno 08 novembre 2018 ed è reperibile al seguente link <https://www.agendadigitale.eu/sicurezza/droni-civili-a-scopo-offensivo-problemi-e-soluzioni/>.

<sup>2</sup> Davis, L.E. et al. (2014) Armed and Dangerous? UAVs and U.S. Security, *RAND Corporation*. Link: <https://www.jstor.org/stable/10.7249/j.ctt6wq880.1>

mezzi per compiere attività illegali a breve raggio, quali attacchi terroristici o spionaggio.

## **Droni a scopo offensivo: il caso Hezbollah**

L'utilizzo di comuni droni ad uso civile da parte di Hezbollah come arma contro l'esercito israeliano era già avvenuto tra il 2013 e il 2014. All'epoca, i tentativi si erano rivelati per lo più degli insuccessi, in quanto le forze israeliane erano spesso riuscite ad identificare ed abbattere i droni prima che questi potessero raggiungere i propri obiettivi. Ciononostante, i successi nel contrattacco potrebbero essere considerati più come dovuti allo stato di allerta – generalmente alto – mantenuto dallo Stato d'Israele, piuttosto che a una specifica capacità di neutralizzare la minaccia costituita dall'uso non-convenzionale di droni civili. Nell'agosto 2017, sono affiorate notizie su come Hezbollah stesse usando i droni contro lo Stato Islamico in Siria; un mese dopo, le forze israeliane hanno abbattuto un drone, anch'esso operato da Hezbollah, di manifattura iraniana. Hezbollah non usa solo droni a scopo offensivo: utilizza anche APR per videografia e fotografia a scopi di ISR (intelligence, sorveglianza, ricognizione), gli stessi per i quali altri Stati – tra cui gli USA – utilizzano droni di dimensioni nettamente maggiori (quali gli MQ-1 e gli MQ-9). Il caso più eclatante rimane quello del drone operato da Hezbollah che è riuscito a raccogliere immagini di un centro di ricerca nucleare israeliano a Negev, vicino Simona – immagini delle quali l'Iran è successivamente entrato in possesso.

È da sottolineare come Hezbollah sia da considerare come un caso precursore di tipo *'borderline'*, cioè più un caso limite, che un attuale esempio di organizzazione terroristica operante droni. Come meglio spiegato da David et al., “[...] Hezbollah [...] è più un mini-esercito che un classico gruppo terroristico [...]” Da almeno cinque anni,

Hezbollah sembra essere in possesso di quella che si potrebbe definire una flotta di droni, migliorando significativamente il proprio arsenale dopo i fallimenti avuti con i droni civili: si suppone che l'organizzazione sia ora in possesso – ed operi – droni di manifattura iraniana, teoricamente in grado di rivaleggiare con gli MQ-1 e MQ-9 americani. Probabilmente seguendo questo esempio, e sfruttando le nuove tecnologie a disposizione sul mercato a prezzi molto più bassi, almeno un'organizzazione terroristica ha incominciato ad usare droni civili per i propri obiettivi: lo Stato Islamico (IS).

## **Il caso di studio: lo Stato Islamico**

Già nel 2014 erano apparsi i primi report di come IS stesse utilizzando 'droni' o 'droni trasformati in armi'. Articoli pubblicati su giornali statunitensi e testate online affermavano che, durante la battaglia di Mosul nel 2017, IS usasse droni per spiare gli spostamenti delle truppe americane e sganciare bombe, o come 'droni suicidi' (solitamente piccoli droni dotati di esplosivi che vengono fatti schiantare contro obiettivi prefissati, per es. edifici o folle). Le ragioni per cui i gruppi terroristici stanno ricorrendo ai droni civili per videografia e fotografia sono molteplici.

- Prima di tutto, essi sono particolarmente accessibili, sia in termini di prezzo, sia perché la loro vendita non è particolarmente regolata. Sebbene il produttore DJi non venda i propri prodotti in Iraq e Siria, ad esempio, i gruppi terroristici possono facilmente acquistarli online. Vecchie versioni dei droni DJi, quali il Phantom 2, vengono vendute su Amazon tra i 250 ed i 400 dollari, con la possibilità di spedizione in tutto il mondo a seconda del venditore.
- In secondo luogo, il fatto che siano droni relativamente piccoli li rende la perfetta arma-in-potenza. Come menzionato

precedentemente, questa categoria di droni è difficilmente identificabile: sono piccoli a sufficienza per essere invisibili ai radar, possono essere fatti volare ad altezze che non attirano l'attenzione dei sistemi di controllo aereo e degli scudi protettivi, ed allo stesso tempo sono difficilmente visibili dalle persone al suolo.

- In terzo luogo, questa tipologia di droni è facilmente modificabile, rendendone quindi possibile la trasformazione in armi in molteplici modi. Una delle cose più semplici da fare è sostituire la fotocamera con dell'esplosivo, in tal modo trasformando l'apparecchio in un drone suicida. Un'operazione leggermente più complicata, ma molto valida in termini di pay-off, è l'installazione di un meccanismo di rilascio: molti video e guide fai-da-te sono disponibili online, specialmente su piattaforme quali YouTube, e spiegano passo per passo come modificare l'apparecchio. Sistemi di rilascio-e-consegna sono venduti su internet da varie aziende con prezzi a partire da meno di 150 dollari americani.
- Infine, ma di non minore importanza, questi droni possono servire un doppio scopo: arma e testimonianza delle loro azioni contemporaneamente. Le immagini registrate possono essere usate per scopi di propaganda, come è già successo nel tardo 2017. A partire dal 2017, si è presentato un problema inedito: IS non stava semplicemente usando un *qualsiasi* tipo di drone presente sul mercato. Vari articoli, immagini e video provano che stesse usando particolarmente spesso droni dalla linea *Phantom* della DJi. Per la compagnia, la faccenda si è di colpo trasformata in un problema più 'serio': dal momento che questa preferenza era stata resa di pubblico dominio, il rischio di cattiva pubblicità derivante dall'accostamento dell'organizzazione terroristica con i prodotti dell'azienda andava risolto. Nella

primavera del 2017, DJi ha silenziosamente avviato un update al proprio sistema di *geo-fencing*, che doveva rendere i suoi droni non più operabili nella “maggior parte di Iraq e Siria” — ciononostante, nel tardo 2017, alcuni articoli già affermavano che il sistema potesse essere bypassato o forzato utilizzando dei ‘pacchetti’ apparentemente sviluppati da hacker russi ed acquistabili online.

## **Il fallito attentato a Maduro**

Nonostante le informazioni sui droni civili utilizzati da Hezbollah ed IS fossero già note da anni, l’opinione pubblica mondiale si è resa conto di quanto questa problematica toccasse da vicino anche chi non abitava in zone di guerra solo il 4 agosto 2018, quando due droni sono esplosi nelle vicinanze di una parata militare presenziata da Nicolás Maduro, il Presidente del Venezuela. L’analisi delle immagini dell’attentato non lasciano dubbi sulla provenienza dei droni: due DJi Industrial Matrice 600, droni civili per fotografia e videografia di qualità professionale. Le specifiche dichiarate dall’azienda garantiscono un raggio di volo fino a cinque chilometri di distanza dall’operatore, capacità di carico fino a sei chilogrammi, ed una autonomia fino a sei ore. Secondo quanto riportato dal New York Times, questi droni – venduti a più di 5.000 dollari l’uno – sarebbero stati dotati di cariche esplosive composte di C4, con la precisa intenzione di assassinare il presidente venezuelano.

## **Possibili soluzioni**

### ***Geo-fencing***

Sebbene imperfetti, i sistemi di *geo-fencing* potrebbero essere la migliore risposta all’uso dei droni in aree di guerra da parte di gruppi

terroristici. Il maggiore incentivo all'implementazione di tali sistemi per le aziende risiede nella cattiva pubblicità che l'uso dei loro prodotti in zone di guerra comporta: i droni per fotografia e videografia, mentre da un lato stanno avendo un boom di vendite a causa della loro affidabilità, potrebbero vedere la loro popolarità diminuire nel caso in cui venissero sempre più associati a gruppi terroristici. Nello scenario peggiore, queste tecnologie potrebbero diventare iper-regolamentate se diventassero sempre più correlate ai gruppi terroristici nella narrativa dei media.

## **Legislazione**

Allo stesso tempo, il *geo-fencing* non dissuaderà i gruppi terroristici dall'usare i droni in aree non-ristrette, quali zone non di guerra. È qui che gli approcci legislativi verranno in aiuto. Come spiegato precedentemente, ci sono norme specifiche per regolare l'uso dei droni in Europa e negli USA, ma necessitano di modifiche e sono scarsamente implementate. Sia l'Europa che gli USA sono sulla strada giusta per garantire un efficace monitoraggio di queste tecnologie sul proprio territorio; allo stesso tempo, l'industria si sta evolvendo velocemente, e la legislazione fatica a tenere il passo. Il migliore approccio sarebbe probabilmente quello di regolare a monte la vendita di droni, collaborando con le compagnie che li producono e con i venditori. I droni per videografia e fotografia sono attualmente trattati dal pubblico più come un'estensione di una telecamera che come un oggetto volante, con tutte le problematiche che questa capacità comporta.

## **Tecnologie anti-droni**

Come sottolineato da Karpowicz<sup>3</sup>, le tecnologie anti-drone diventeranno una parte sostanziale del mercato relativo ai droni nel prossimo futuro. Le start-up attive in quest'ambito rappresentano infatti una nicchia di mercato con un enorme potenziale. Attualmente, le tecnologie anti-drone esistenti necessitano ancora di implementazioni ulteriori, ma si prospetta comunque un aumento nel loro utilizzo – limitatamente all'ambito militare o governativo – nei prossimi anni.

## **Conclusioni**

Nel caso degli APR per videografia e fotografia, risulta evidente come lo sviluppo tecnologico stia viaggiando ad una velocità esponenzialmente maggiore rispetto a quello normativo. Il mercato civile si sta espandendo, portando sempre più ricavi e posti di lavoro – ma anche più utenti, inclusi gruppi terroristici quali IS. I rischi che una proliferazione incontrollata comportano anche all'infuori delle zone di guerra iniziano a vedersi, come il caso dell'attentato al presidente venezuelano Maduro ha sottolineato. Un'azione concertata tra organi preposti al controllo e aziende produttrici sembra ad oggi la soluzione migliore, più immediata e meno dispendiosa, per evitare che gli APR civili diventino una problematica di sicurezza tale da renderli fuori legge.

---

<sup>3</sup> Karpowicz, J. (2018). "8 Commercial Drone Predictions for 2018", *Commercial UAV Expo*. Link: <https://www.expouav.com/wp-content/uploads/2017/12/8-Commercial-Drone-Predictions-for-2018.pdf>.



**Center for Cyber Security and International Relations Studies (CCSIRS)**

Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

<https://www.cssii.unifi.it/ls-6-cyber-security.html>