Tutti i rischi (anche cyber) dei droni commerciali Made in China

Ginevra Fontana

To cite this article: Fontana, G. (2018), Tutti i rischi (anche cyber) dei droni commerciali Made in China, Formiche. This article was first published on Formiche on 24 November 2019 and is therefore also available here: https://formiche.net/2018/11/cyber-droni-china/

L'analisi di Ginevra Fontana del Center for Cyber Security and International Relations Studies dell'UniFi.

Gli aeromobili a pilotaggio remoto (APR), comunemente chiamati "droni", hanno visto la loro diffusione crescere esponenzialmente nell'ultimo decennio. La tecnologia si è evoluta velocemente, offrendo prodotti sempre più accessibili al consumatore medio. I droni per videografia e fotografia hanno ora prezzi simili a comuni fotocamere digitali e hanno performance, a livello qualitativo, praticamente identiche. Nei prossimi anni si prevede a livello europeo una crescita del mercato di riferimento, con la conseguente creazione di migliaia di posti di lavoro e ritorni economici nell'ordine dei miliardi di euro. A livello legislativo, l'Europa ha cercato di rimanere al passo con l'evoluzione tecnologica senza ostacolare lo sviluppo dell'industria.

UNA CRESCITA ESPONENZIALE

I droni commerciali venduti per scopi di fotografia e videografia hanno fatto segnare una crescita esponenziale nelle vendite negli ultimi quattro anni, ed il trend sembra confermarsi nelle proiezioni future. La cinese DJi, azienda leader nel settore degli APR ad uso civile, ne è il più lampante esempio: i suoi droni per fotografia e videografia sono tra i più venduti al mondo, con un prezzo che oscilla tra i 100 ed i 5mila dollari. Tra questi, gli apparecchi delle due serie più famose, i droni Phantom e Mavic, sono venduti ad un prezzo compreso tra i 500 ed i 1.200 dollari. Sebbene il cartellino non li renda esattamente i più convenienti sul mercato, la qualità dell'immagine delle serie Phantom e Mavic – del tutto simile ad una fotocamera nella stessa fascia di prezzo – fa sì che la domanda si mantenga alta. A riprova di ciò, è sufficiente far notare come la DJi detenga al momento oltre il 36% del mercato Nord Americano per questa

tipologia di prodotti. Anche se i droni della DJi, nonostante il prezzo elevato, hanno registrato un così alto successo, va sottolineato che a livello mondiale queste tecnologie stanno diventando sempre meno costose e più accessibili. Un comune "drone per selfie" può essere acquistato in un qualsiasi negozio di elettronica per meno di 50 euro – una fascia di prezzo più che accessibile al consumatore medio. APR per fotografia e videografia più sofisticati possono invece superare le migliaia, a seconda della qualità dell'immagine, il tempo di volo, la resistenza alle condizioni atmosferiche, il raggio di volo ed altre variabili. Inoltre, la tecnologia in questo settore è sempre più user- friendly. Al posto di software particolarmente complicati che necessitano di una certa competenza professionale, le aziende (la stessa DJi in primis) hanno difatti sviluppato app sempre più intuitive, con le quali gli utenti possono facilmente pilotare i propri droni da cellulare e tablet, sfruttando il segnale Wi-Fi emesso da tali dispositivi, il Bluetooth (per i droni meno costosi e con un raggio di volo inferiore), o anche i segnali radio. Con l'esclusione dei droni più economici, la maggior parte degli apparecchi è anche connessa con tecnologia GPS. Tale tipologia di controllo remoto espone, comunque, gli APR a problematiche quali, prima di tutto, la perdita di segnale con l'apparecchio – eventualità che ha reso necessario lo sviluppo di sistemi del cosiddetto tipo 'fail-safe'.

I PROBLEMI CORRELATI

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 (o il loro furto attraverso operazioni di hackeraggio) 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, i droni per videografia e fotografia venduti correntemente hanno dimensioni e volano ad altezze tali da renderli (1) difficilmente identificabili dai radar; (2) 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 mezzi per compiere attività illegali a breve raggio, quali attacchi terroristici o spionaggio.

LE POSSIBILI SOLUZIONI

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. 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 sia 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. Come sottolineato da Karpowicz, 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.

INSEGUENDO LA TECNOLOGIA

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 alcuni casi dimostrano. 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.