

Il mercato dei droni vale cento milioni di euro in Italia e 2,6 miliardi di dollari nel mondo. È prevista una crescita del 30 per cento l'anno da qui al 2030.

UN MILIONE DI DRONI FUORI CONTROLLO

La più grande azienda di «aeromobili a pilotaggio remoto» è cinese e ha un grosso problema di sicurezza nella gestione dei dati dei suoi utenti. Ecco perché è attualmente nel mirino degli Stati Uniti. Intanto anche in Italia, dove la vendita di questi prodotti ha una crescita esponenziale, emergono nuovi rischi.

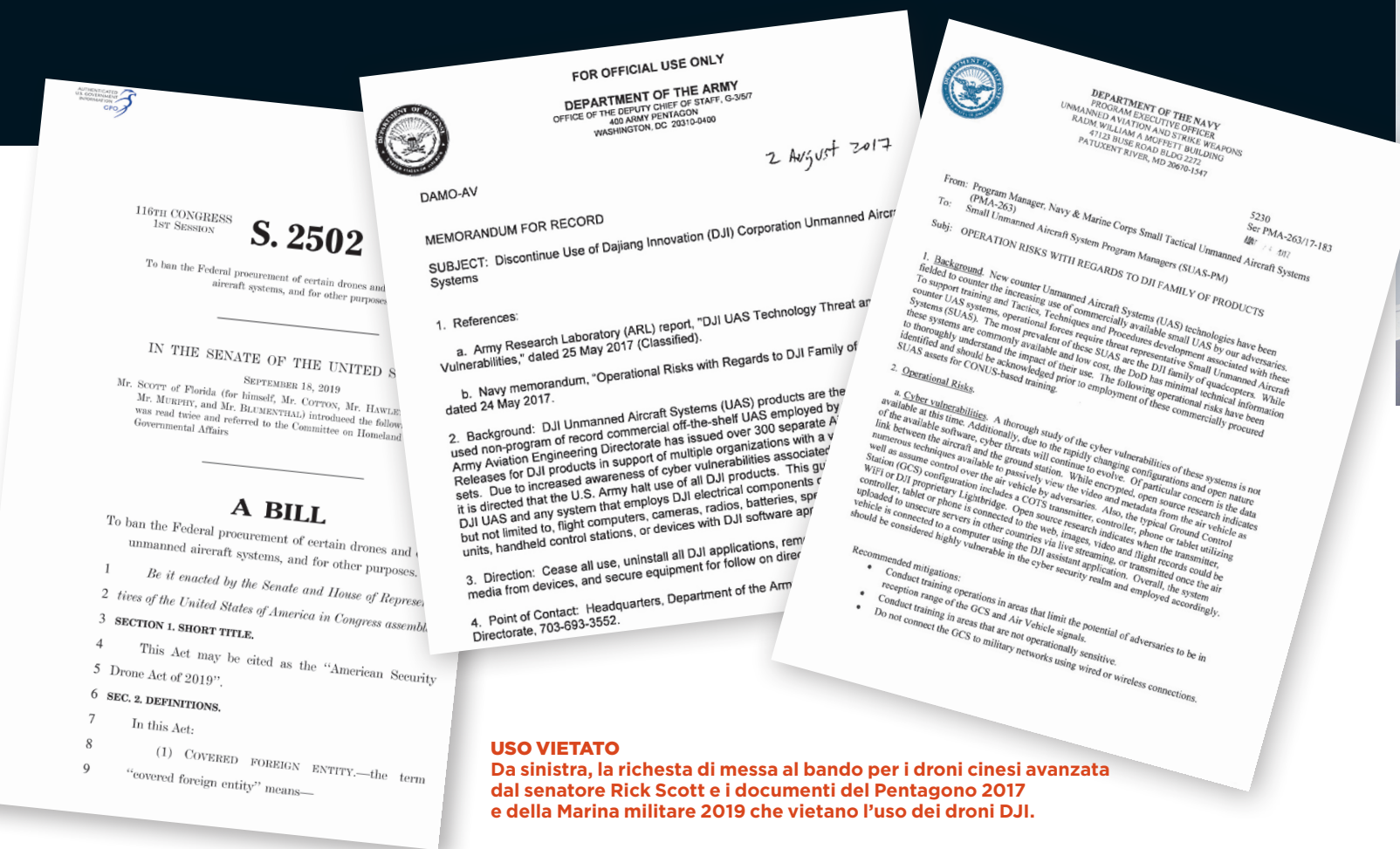
di Stefano Piazza e Luciano Tirinnanzi

Dopo la telefonia mobile e il 5G, si apre un nuovo fronte per le ambizioni espansionistiche cinesi. Ovvero i droni commerciali e il loro più grande produttore al mondo: la cinese Dji. Fondata a Shenzhen nel 2006 dall'ingegnere Wang Tao, la società rappresenta circa il 77 per cento delle vendite globali di droni. Il che spa-

venta soprattutto Washington, certa che questi nuovi strumenti tecnologici siano il nuovo «cavallo di Troia» che Pechino ha inviato in America e in Europa per carpire i segreti industriali euro-atlantici.

In effetti, il mercato e il fatturato di Dji sono cresciuti in maniera esponenziale: se nel 2012 il conto economico era 26 milioni di dollari, nel 2015 aveva già superato il

Gettyimages



USO VIETATO

Da sinistra, la richiesta di messa al bando per i droni cinesi avanzata dal senatore Rick Scott e i documenti del Pentagono 2017 e della Marina militare 2019 che vietano l'uso dei droni DJI.

miliardo (oggi raddoppiato) con un valore societario che sfiora i 10 miliardi di dollari.

Dopo le strabilianti performance di fatturato, però, nel 2019 DJI ha dovuto prima affrontare una serie di cause contro dipendenti infedeli, e poi in ambito giudiziario gestire la causa intentata da Autel, produttore di droni statunitense, nonché diretto concorrente nel mercato mondiale. Autel si è rivolto a uno degli studi legali più importanti degli States, lo studio Step-toe, denunciando illeciti in materia di tasse doganali da parte dei cinesi. Il team di avvocati dell'una e dell'altra parte si sono così scontrati in aula lo scorso 13 maggio 2020 presso la US International Trade Commission.

Il primo verdetto ha constatato che «la Sz DJI Technology Co. Ltd. e sette

entità correlate (insieme note come DJI) hanno violato la Sezione 337 del Tariff Act del 1930, e successive modifiche, importando e vendendo droni che violano il brevetto USA n. 9.260.184 appartenenti ad Autel».

Di conseguenza, il giudice amministrativo ha raccomandato di escludere dall'importazione negli Stati Uniti i prodotti in violazione, tra cui praticamente tutta la serie di modelli del colosso della robotica cinese: Mavic Pro, Mavic Pro Platinum, Mavic 2 Pro, Mavic 2 Zoom, Mavic Air e Spark.

Tutto questo, però, è niente rispetto al caos scoppiato dopo la pubblicazione sul *New York Times* dei risultati di due rapporti speciali - uno americano della società di cyber sicurezza Grimm e uno della francese

Synacktiv - che *Panorama* ha ottenuto in esclusiva. Quei rapporti affermano che l'app utilizzata sul sistema operativo Android di Google, indispensabile a manovrare il drone nel raccogliere grandi quantità di immagini e informazioni personali, le può anche inviare ai server del governo di Pechino senza alcuna autorizzazione dell'utente (è accaduto persino al figlio dei duchi del Sussex, Harry e Megan, fotografato a Los Angeles da un drone DJI).

L'azienda cinese, con una nota stampa, ha tentato di ridimensionare l'accaduto. Tuttavia, la polemica attorno ai suoi prodotti è stata sufficiente a mettere in allarme l'intero apparato di sicurezza degli Stati Uniti. Washington è ormai convinta che Pechino abbia avuto accesso alle informazioni di



circa un milione di cittadini americani. E la cosa non è piaciuta.

A nulla sono valsi i gesti di «appeasement» della compagnia: come quello tentato lo scorso aprile quando, in piena pandemia, DJI ha regalato a 43 polizie locali di 22 Stati americani decine di droni per permettere loro di monitorare e sorvegliare le sterminate aree scarsamente abitate degli Usa. È però bastato un tweet di un senatore repubblicano della Florida, Rick Scott, per rispedire l'omaggio al mittente: «Pensateci un secondo. Questo virus ha avuto origine nella Cina comunista e le bugie del Partito Comunista hanno contribuito a diffonderlo in tutto il



PRODUZIONE GLOBALE
La sede di DJI a Shenzhen. Nel 2021 si trasferirà in un nuovo, faraonico complesso.

IN AMERICA DJI HA DONATO DRONI A 43 POLIZIE DI 22 STATI

mondo. Ora stiamo usando droni prodotti da una società cinese e sostenuti dal PCC per imporre il distanziamento sociale. Questo è pazzesco!».

Rick Scott non è un politico qualsiasi, ma colui il quale aveva presentato al Senato una proposta per inibire a tutte le agenzie statunitensi la possibilità di utilizzare droni stranieri, «se il Paese è ufficialmente considerato una minaccia alla sicurezza nazionale». E la Cina, inutile dirlo, è la prima della lista.

DJI ha spiegato di non aver mai permesso l'invio di dati o file da utenti governativi verso alcun server della Cina, visto che i droni a scopo di sorveglianza non disporrebbero neanche di funzionalità internet. Ma perché allora DJI ha posto l'accento sulla parola «governativo»?

Semplicemente perché lo scorso settembre, dopo che il Pentagono ave-

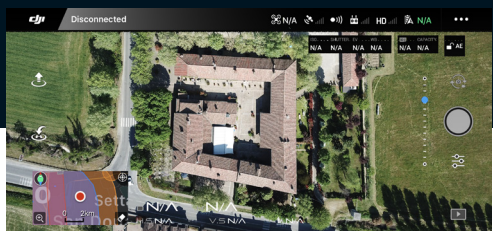
4,8 MILIARDI DI DOLLARI

Wang Tao, fondatore di DJI, vanta un patrimonio 4,8 miliardi di dollari e il 40 per cento delle azioni dell'azienda.

va acconsentito alle richieste di Scott e proibito l'acquisto di droni cinesi - causa problemi di sicurezza informatica - è emersa una serie di acquisti proprio di quegli stessi droni-spia prodotti da DJI: effettuati rispettivamente dalla Marina (190 mila dollari) e dell'Aeronautica (50 mila).

C'è di peggio. Gli Uav, gli «aeromobili a pilotaggio remoto» cinesi, sono andati alle squadre di tattiche speciali dell'Aeronautica e dei Seals, quindi agli operatori più importanti e segreti di cui Washington disponga. Cosa che ha allarmato il Congresso, nonostante il maldestro tentativo di Michael Oldenburg, portavoce dell'innovazione di DJI negli Stati Uniti, di ridimensionare la vicenda: «Le notizie sulle vulnerabilità della cyber sicurezza di DJI e il memorandum dell'Ufficio immigrazione e controllo doganale del Dipartimento della sicurezza interna erano completamente false».

Vero o falso che sia, il direttore della National counter-intelligence and security center, William R. Evanina, nel ricordare quello che ormai tutti sanno - ovvero che, per la legge cinese, ogni società tecnologica è tenuta a fornire alle autorità di Pechino, quando richiesto, le informazioni che ottiene o che sono depositate nelle proprie reti - ha precisato: «Tutti gli americani dovrebbero essere preoccupati che le loro immagini, dati biometrici, localizzazione e altre informazioni memorizzate su app cinesi possano essere trasferiti all'apparato di sicurezza di Stato cinese».



1 MILIONE DI DOWNLOAD

L'applicazione della Dji è progettata per pilotare il drone dal telefono. È stata scaricata da un milione di utenti. Secondo lo studio francese Synacktiv può essere «spiata» e controllata da remoto.

«QUESTI DRONI SONO PILOTABILI IN MODO OSTILE»

Lo rivelano i test di una società di sicurezza francese che ha analizzato gli aeromobili e le app di controllo Dji.

Tiphaine Romand-Latapie è un'ingegnere di Synacktiv, società francese che si occupa di test di sicurezza, ricerche sull'affidabilità e vulnerabilità delle difese tecnologiche di enti internazionali pubblici e privati. Esperta di crittografia applicata, ha lavorato anche per il colosso Airbus. Dalla sua posizione di ricercatrice, è molto preoccupata della vulnerabilità dei droni.

Secondo un vostro recente studio, i droni della compagnia cinese Dji non sono sicuri, visto che l'app che li controlla in volo può trasmettere informazioni sensibili a Pechino. È così?

Sì. E il motivo è semplice. Quando si acquista quella tipologia di droni, è necessario installare anche un'applicazione sul telefono, sia per pilotarlo sia per recuperare le immagini fotografiche scattate dal velivolo. Noi ci siamo concentrati sulla versione per Android. Le info e le immagini scattate dal drone via telefono vengono automaticamente dirette verso dei server in Cina: e così pure gli identificatori specifici del telefono o della carta Sim, gli identificatori della rete telefonica, gli identificatori dei telefoni vicini nella stessa rete, il modello di telefono, persino la luminosità dello schermo. Tecnicamente, il software è stato progettato per raccogliere molti dati, quindi ha un'enorme capacità. L'applicazione ha inoltre due diversi modi per aggiornare o installare nuovi software sul telefono. Nessuno dei due utilizza il sistema standard di download e aggiornamento dell'applicazione Google Play Store; il che significa che Google non ha alcun controllo su ciò che viene installato sul telefono dell'utente. Chiunque

abbia accesso ai server di aggiornamento con intenzioni ostili potrebbe quindi scegliere di far installare sul telefono un software ancora più invasivo, oppure potrebbe installare un software spia per prendere il controllo del telefono dell'utente, sfruttando i numerosi permessi già concessi all'applicazione (lettura contatti, microfono, fotocamera, accesso ai file, etc.) o ancora se rileva una vulnerabilità di Android. L'applicazione, inoltre, non si chiude quando l'utente effettua i gesti standard per chiudere le applicazioni, ma continua a funzionare e a inviare dati in rete. L'unico modo per l'utente di chiudere effettivamente l'applicazione è attraverso i menu di sistema di Android.

Ciò significa che sarebbe possibile far volare un drone direttamente dalla Cina?

L'app è progettata per pilotare il drone dal telefono. Quindi, tecnicamente parlando, un accesso ostile ai server dell'azienda potrebbe anche costringere l'utente a scaricare un'app che permetta il controllo da remoto del drone. Tuttavia, non riteniamo questo scenario molto probabile. Semmai, per un aggressore è più utile raccogliere dati dall'Uav o dal telefono in tempo reale, o prendere il controllo del telefono.

Quanto è vasto il fenomeno?

Il sito web del Dji e il «negozio» Google Play indicano che l'app è utilizzabile per pilotare tutti i modelli di drone del marchio Phantom 4. Tutti gli utenti di questa applicazione su Android sono quindi interessati. E parliamo di più di un milione di download. I conti sono presto fatti...

(S.P.-L.T.)

Insomma, «i droni-spia che spiano anche chi spia» sarebbero fuori controllo. E non è questione di scioglimento. Presto la vicenda potrebbe coinvolgere la stessa Italia. Secondo una ricerca dell'Osservatorio droni del Politecnico di Milano, infatti, tra il 2016 e il 2019 si sono registrati al portale dell'Ente nazionale per l'aviazione civile (Anac) complessivamente 13.479 droni, che corrisponde al quarto + 13 per cento annuo di fila.

Il 56 per cento appartiene a soli cinque costruttori: neanche a dirlo, la parte del leone spetta alla Dji (47 per cento), seguita a distanza siderale dall'americana Parrot (3 per cento), dalla cinese Yuneec (2,5 per cento), e dalle italiane DXdrone (2 per cento) e Italdron (1,5 per cento).

Un mercato che, solo nel nostro Paese, vale più di 100 milioni di euro. Secondo Cesare Caprarelli, progettista e costruttore del settore, «la politica delle maggiori aziende asiatiche produttrici di droni purtroppo non è basata sul concetto di "open-source", che permette di migliorare e implementare sistemi tecnologici con libertà scientifica e intellettuale, in una visione quindi di sviluppo globale. Al contrario, è una politica prettamente commerciale, che diffonde sistemi proprietari chiusi, i quali necessitano dei dati dell'utente per funzionare e/o per essere aggiornati».

Dopo il 5G, dunque, il prossimo passo sono i droni-spia. Un passo, appunto, in questa guerra sino-americana che è appena agli inizi. ■

© RIPRODUZIONE RISERVATA