IL SOLE 24 ORE – 10 OTTOBRE 2025

La nuova frontiera della sicurezza nazionale contro i cyber attacchi

di Emilio Cozzi

Settembre 2017. Notte. Da qualche parte oltre le nuvole, due punti luminosi viaggiano uno accanto all'altro. Chi, con un telescopio, li guardasse da terra, noterebbe che il puntino più piccolo si avvicina al più grosso, come lo inseguisse. Ciò che anche all'osservatore più accorto potrebbe sfuggire, è di stare testimoniando un attacco satellitare. Lo conferma la Direction Générale de l'Armement francese, che da giorni monitora il cielo con tracciatori radar e telescopi ottici. La luce più grossa è Athena-Fidus, un sistema satellitare per comunicazioni a banda larga sviluppato dall'Agenzia spaziale italiana e da quella francese (il Cnes) e dedicato al supporto delle Forze armate dei due Paesi. L'altra luce, la più piccola, è Launch-Olymp – i russi lo chiamano "Olymp K" – un satellite spedito in orbita il 28 settembre del 2014 dal cosmodromo di Baikonur, in Kazakistan. Non si sa molto di lui, a parte il fatto che quella notte di settembre sia stato a pochi chilometri da Athena-Fidus. Che nello spazio significa accanto. «Era vicino», avrebbe commentato un anno dopo Florence Parly, all'epoca ministra delle Forze armate francesi, «talmente vicino che avremmo potuto credere stesse captando le nostre comunicazioni. Domani chi ci dice non ritornerà accanto a uno dei nostri satelliti?». Lungi da ipotesi, dal 2017 le offensive ai satelliti e ai sistemi spaziali tout-court, cioè anche al loro segmento terrestre, sono una realtà via via più frequente e pronta a testimoniare quanto la sicurezza nazionale non possa più prescindere dallo spazio, non a caso entrato nel novero dei "domini operativi" Nato nel 2019. «Le comunicazioni satellitari nei conflitti armati sono essenziali quando i sistemi terrestri sono distrutti o indisponibili - dice Clémence Poirier, ricercatrice

senior del Center for Security Studies all'Eth di Zurigo - consentono di trasmettere ordini tra i livelli strategico, operativo e tattico, e permettono di pilotare droni e ricevere immagini dalle telecamere».

Lo ribadiscono i numeri: «Nel 2024 – continua Poirier - ho monitorato 254 attacchi con droni contro i modem Starlink in Ucraina. I picchi si sono registrati durante le offensive russe a Charkiv e Donetsk, e nell'incursione ucraina a Kursk». Le parole di Poirier palesano un fatto: oggi, in caso di guerra o crisi geopolitiche, gli attacchi all'ecosistema spaziale sono sistematici. Il motivo è semplice: i satelliti sono diventati fondamentali per qualsiasi operazione militare, e gli autori delle minacce lo hanno capito fra i primi.

«Attraverso l'intelligence *open source* – continua Poirier – abbiamo monitorato 165 operazioni informatiche contro il settore spaziale nel contesto della guerra in Ucraina e altre 117 nel conflitto israelo-palestinese. A giugno, nelle sole due settimane di guerra fra Israele e l'Iran, sono state condotte circa 70 operazioni informatiche contro sistemi o entità spaziali». Se si escludono quelle naturali, causate da tempeste geomagnetiche o eruzioni solari in grado di compromettere gli apparati orbitanti, le minacce si manifestano con tecnologie e modalità diverse: possono essere cinetiche, cioè attuate attraverso missili anti-satellite, come quelli già testati da Stati Uniti, Russia, Cina e India; non cinetiche, con armi laser capaci di "accecare" un apparato; elettroniche, con l'interferenza (il cosiddetto "jamming") o la falsificazione di un segnale (lo "spoofing"), per esempio Gps oppure informatiche, attraverso *malware* distribuiti su una rete terrestre, o software capaci di interrompere un collegamento o un servizio spaziale. Non sono da escludere anche sabotaggi interni, da parte di un dipendente che lavori in segreto per interessi o Paesi terzi.

Secondo Poirier, le ragioni per cui le offensive stanno aumentando afferiscono a tre fattori principali: l'evoluzione dei sistemi, che nel passaggio al digitale "hanno ampliato la superficie di attacco"; la ricomparsa di conflitti armati, «accompagnati da una significativa attività informatica da parte di attori

statali, attivisti e criminali, schierati con una delle parti belligeranti»; e la consapevolezza che la società intera oggi dipende dai sistemi spaziali, spesso alla base di infrastrutture critiche. «Anche senza saperlo, ognuno di noi utilizza i satelliti mediamente 40 volte al giorno».

Basterebbe pensare ai sistemi di navigazione e posizionamento su cui si basa la gestione globale del traffico marittimo e aereo, al monitoraggio del territorio, al meteo e a buona parte delle transazioni bancarie e delle telecomunicazioni. «L'attacco informatico contro un satellite commerciale può essere più pericoloso di un'offensiva ad apparati militari. In uno scenario di conflitto o di guerra ibrida, prendere di mira i sistemi satellitari può avere effetti a cascata sui servizi essenziali. Se per esempio qualcuno rendesse inutilizzabile il Gps, causerebbe una perdita media di un miliardo di dollari al giorno solo al Pil degli Stati Uniti». Almeno quest'ultimo scenario, però, è per ora fantascientifico: queste capacità sono soprattutto nelle mani dei principali Stati nazionali. Sebbene le organizzazioni terroristiche, in particolare in Africa, ricorrano sempre più spesso all'utilizzo illegale di satelliti per comunicare, oggi nessuno dispone di capacità di attacco informatico in grado di mettere in ginocchio un Paese. Per di più la consapevolezza cresce: «La sicurezza informatica spaziale – nota Poirier - oggi è riconosciuta nelle politiche e nelle leggi. La prima bozza della legge spaziale dell'Unione europea, presentata a giugno dalla Commissione, prevede numerose misure di sicurezza, come il monitoraggio di anomalie e incidenti, il riconoscimento dei diritti di accesso tramite protocolli di gestione dell'identità, e i test di vulnerabilità. Agenzie spaziali come la Nasa, il Cnes o quella britannica (Uksa) hanno sviluppato guide sulla sicurezza informatica per i veicoli spaziali, riassumendo le migliori pratiche. Anche l'industria sta adottando una prassi per cui la sicurezza informatica è inclusa fin dalla progettazione il che rende i sistemi più sicuri. In molti, oggi, sviluppano prodotti per la sicurezza adattati ai vincoli e alle specificità dell'ambiente orbitale». Lo ha confermato, giusto il 6 ottobre, l'accordo quadro di collaborazione tra l'Agenzia per la cybersicurezza nazionale (Acn) e l'Agenzia spaziale italiana (Asi), teso a rafforzare la resistenza e la resilienza cibernetica del Paese: oggi la sicurezza è extraterrestre. O non è.