Cybersecurity spaziale: perché i satelliti sono le nuove infrastrutture critiche



La cybersecurity spaziale è emersa come priorità strategica per l'Unione Europea. L'inclusione delle infrastrutture orbitali nella Direttiva NIS2 e la proposta dell'*EU Space Act* del giugno 2025 segnano un cambio di paradigma: i satelliti non sono più asset periferici, ma nodi critici dell'ecosistema digitale europeo. Questo articolo analizza le implicazioni tecniche, operative e regolatorie per i professionisti della sicurezza informatica, con particolare attenzione alle opportunità e agli obblighi per le aziende italiane della *space economy*.

L'orbita come nuovo perimetro di attacco

La cybersecurity spaziale non è più una disciplina di nicchia riservata agli addetti ai lavori delle agenzie governative. Con circa 13.000 satelliti attivi in orbita terrestre – di cui oltre l'80% in orbite LEO (*Low Earth Orbit*) – e la dipendenza crescente delle economie moderne da servizi *space-based*, il dominio orbitale rappresenta un'estensione naturale della superficie d'attacco cyber. Il numero di satelliti operativi cresce rapidamente: secondo i dati di Jonathan McDowell (Harvard-Smithsonian Center for Astrophysics), solo nella *Lower* LEO si contano oltre 12.200 *payload* attivi a inizio 2026.

Il rapporto *ENISA Space Threat Landscape 2025*, pubblicato il 26 marzo 2025, fotografa una situazione preoccupante: pratiche crittografiche deboli, *misconfiguration* software, *supply chain*

insicure e carenze nella resilienza operativa caratterizzano ancora gran parte del settore. La novità non è l'esistenza di vulnerabilità: è la scala del rischio e l'interdipendenza sistemica con le infrastrutture terrestri.

Per comprendere la portata del problema, consideriamo un dato: secondo l'*ESA Space Environment Report 2025*, si stimano oltre 1,2 milioni di frammenti di detriti spaziali superiori a 1 cm in orbita, oltre 50.000 dei quali superiori a 10 cm. Ogni collisione genera nuovi detriti, alimentando il rischio della sindrome di Kessler – una cascata autoalimentata che potrebbe rendere alcune orbite inutilizzabili per generazioni. La sicurezza fisica e quella cyber convergono: un attacco informatico che comprometta i sistemi di *collision avoidance* avrebbe conseguenze fisiche devastanti.

Viasat KA-SAT: anatomia del primo attacco cyber-cinetico sincronizzato

Il 24 febbraio 2022, un'ora prima dell'invasione russa dell'Ucraina, decine di migliaia di modem satellitari Viasat in Europa hanno cessato di funzionare. L'attacco, attribuito alla Russia da quasi venti Paesi tra cui l'UE e i *Five Eyes*, rappresenta il primo caso documentato di operazione cyber sincronizzata con un'offensiva militare convenzionale.

L'analisi tecnica rivela una sequenza sofisticata ma non particolarmente complessa. Gli attaccanti hanno sfruttato una *misconfiguration* in un'appliance VPN presso il centro di gestione Skylogic a Torino (sussidiaria di Eutelsat), ottenendo accesso alla rete di *management* della costellazione KA-SAT. Da lì, hanno utilizzato comandi di gestione legittimi per sovrascrivere la memoria flash di migliaia di modem residenziali, rendendoli inutilizzabili.

Il *malware* AcidRain, identificato da SentinelLabs, presentava similarità con VPNFilter – una campagna del 2018 attribuita da FBI e *Department of Justice* al governo russo. L'attacco non ha compromesso il satellite in sé, ma ha dimostrato che l'infrastruttura di terra rappresenta il punto debole dell'ecosistema spaziale.

Le conseguenze hanno superato i confini ucraini: 5.800 turbine eoliche Enercon in Germania hanno perso il monitoraggio remoto, e decine di migliaia di abbonati in tutta Europa sono rimasti *offline*. Il caso Viasat ha reso evidente ai *policy maker* europei che lo spazio è infrastruttura critica – e come tale va protetto.

Starlink e la guerra elettronica permanente

Se Viasat ha subito un attacco informatico, Starlink affronta dal marzo 2022 una campagna di *jamming* sistematica. Con oltre 9.300 satelliti attivi a gennaio 2026, la costellazione di SpaceX rappresenta la maggioranza dei satelliti operativi in orbita LEO.

Elon Musk ha dichiarato pubblicamente che SpaceX ha dovuto riprioritizzare risorse verso la *cyber defense* per contrastare il *jamming* russo. Gli aggiornamenti software hanno permesso di "bypassare" i tentativi di interferenza, trasformando la situazione in un gioco del gatto e del topo tra contromisure e contro-contromisure.

Gli eventi recenti in Iran (gennaio 2026) dimostrano che anche le costellazioni LEO non sono invulnerabili. Secondo quanto riportato da France 24 e Rest of World, le autorità iraniane hanno impiegato *jammer* GPS di grado militare per degradare le *performance* di Starlink, con perdite di pacchetti dati dal 30% fino all'80% in alcune aree urbane. A differenza dell'Ucraina, dove SpaceX ha risposto rapidamente con *patch* software, in

Iran la situazione rimane critica – suggerendo che l'efficacia delle contromisure dipende fortemente dal contesto operativo e dalla cooperazione del *vendor*.

Per i CISO (*Chief Information Security Officer*) delle organizzazioni che dipendono da comunicazioni satellitari, il messaggio è chiaro: il satellite non è una garanzia di resilienza assoluta, ma un ulteriore vettore da includere nei piani di *business continuity*.

VisionSpace e le vulnerabilità nei software di controllo missione

Al Black Hat USA 2025, i ricercatori di VisionSpace Technologies – Andrzej Olchawa e Milenko Starcik – hanno presentato risultati che avrebbero dovuto far riflettere l'intero settore spaziale. In totale, hanno identificato 37 vulnerabilità separate in software *open source* utilizzati da NASA, Airbus e altre organizzazioni per il controllo di missioni spaziali.

Il sistema Yamcs, impiegato per comunicare con satelliti in orbita, conteneva cinque CVE che avrebbero permesso a un attaccante di ottenere il controllo completo dell'applicazione. Durante la dimostrazione, i ricercatori hanno mostrato come fosse possibile inviare un comando ai propulsori di un satellite simulato per modificarne l'orbita – senza che il cambiamento apparisse immediatamente sull'interfaccia dell'operatore.

Ancora più grave la situazione di OpenC3 Cosmos, un altro sistema *open source* per stazioni di terra, dove sono state identificate sette vulnerabilità, incluse falle di *remote code execution*. Ma il dato più allarmante riguarda NASA Core Flight System (cFS) Aquila, utilizzato dal telescopio spaziale James Webb e dal *lander* lunare Odysseus: quattro vulnerabilità critiche, tra cui *denial-of-service* e *remote code execution*.

I ricercatori hanno anche analizzato CryptoLib, la libreria di crittografia *open source* utilizzata a bordo di molti satelliti, identificando vulnerabilità critiche sia nella versione NASA sia nella versione standard. “Abbiamo trovato vulnerabilità reali che permettono di crashare l’intero software di bordo con un singolo pacchetto non autenticato”, ha spiegato Starcik. “Se il satellite non è configurato correttamente, questo causa il *reset* di tutte le chiavi crittografiche”.

Tutte le vulnerabilità sono state responsabilmente segnalate e corrette. Ma il problema strutturale rimane: sistemi fondamentali del settore spaziale si basano su codice che può nascondere falle critiche senza un’adeguata revisione.

L’*EU Space Act*: *lex specialis* per la cybersecurity orbitale

Il 25 giugno 2025, la Commissione Europea ha pubblicato la proposta di regolamento sulla sicurezza, resilienza e sostenibilità delle attività spaziali nell’Unione – comunemente noto come *EU Space Act*. Si tratta dell’iniziativa legislativa più ambiziosa mai proposta per il settore spaziale europeo.

L’*EU Space Act* si articola su tre pilastri: *safety* (tracciamento oggetti spaziali e mitigazione detriti), *resilience* (requisiti di cybersecurity e *incident reporting*) e *sustainability* (valutazione del ciclo di vita ambientale). Per i professionisti della sicurezza informatica, è il secondo pilastro a meritare attenzione particolare.

La proposta configura l’*EU Space Act* come *lex specialis* rispetto alla NIS2: gli operatori spaziali che qualificano come entità essenziali o importanti applicheranno i requisiti di resilienza del regolamento spaziale, evitando duplicazioni. Questo non significa requisiti meno stringenti – al contrario.

Tra gli obblighi previsti:

- **Risk assessment lungo l'intero ciclo di vita** della missione spaziale
- **Penetration testing pre-lancio** obbligatorio (regime TLPT simile a DORA)
- **Incident reporting entro 12 ore** per asset *EU-owned*, 24 ore per altri – più stringente delle 24-72 ore della NIS2
- **Requisiti di propulsione** per costellazioni (10+ satelliti) per garantire manovrabilità di *collision avoidance*
- **Cybersecurity *by design*** integrata nei processi di autorizzazione

L'*EU Space Act* istituisce inoltre la *Union Space Resilience Network* (EUSRN) per facilitare la cooperazione tra Commissione, EUSPA e autorità nazionali competenti nella gestione degli incidenti cyber significativi e nell'allineamento con altri *framework* di cybersecurity UE.

Le sanzioni previste sono significative: multe fino al 2% del fatturato annuo globale totale, con poteri ispettivi *on-site* per la Commissione e l'Agenzia. Per gli operatori extra-UE che forniscono servizi spaziali in Europa, i requisiti si applicano comunque – un segnale chiaro della volontà di Bruxelles di stabilire standard globali.

Implicazioni per la *space economy* italiana

L'Italia è il terzo contributore dell'ESA e ospita infrastrutture strategiche: il centro ESRIN di Frascati, le sedi di Thales Alenia Space Italia e Telespazio, l'Agenzia Spaziale Italiana (ASI) e un tessuto di PMI innovative nel settore. Secondo i dati degli Stati Generali della Space Economy e il report Eurispes 2025, la *space economy* nazionale

comprende oltre 400 aziende, con un fatturato complessivo superiore ai 4 miliardi di euro e circa 13.500 addetti diretti. L'Italia è il sesto Paese al mondo per rapporto fra investimenti nello spazio e PIL.

Per le aziende italiane del settore, l'*EU Space Act* rappresenta sia un obbligo di *compliance* sia un'opportunità competitiva. Le organizzazioni che anticiperanno i requisiti di cybersecurity spaziale potranno posizionarsi come *partner* affidabili per progetti ESA, EUSPA e programmi *flagship* come IRIS² (la costellazione europea di comunicazioni sicure).

Alcune considerazioni operative per i CISO e i *security architect* delle aziende della *space economy*:

Supply chain security. L'attacco Viasat è partito da una VPN mal configurata presso un *partner*. La catena di fornitura del settore spaziale è globale e frammentata: componenti hardware da Taiwan, software *open source* da *repository* pubblici, integrazione in Europa, lancio da Guyana o Florida. Ogni anello è un potenziale vettore d'attacco. I requisiti dell'*EU Space Act* impongono *due diligence* rigorosa sui fornitori – inclusa la valutazione di rischi geopolitici.

***Security by design*.** A differenza di un data center, un satellite in orbita non può ricevere *patch* hardware. Le vulnerabilità identificate da VisionSpace dimostrano che il software di controllo missione deve essere sottoposto a *security review* rigorosa prima del lancio. L'approccio *shift-left* – integrare la sicurezza nelle fasi iniziali dello sviluppo – non è più opzionale.

Resilienza ibrida. La dipendenza da Galileo e GPS per il posizionamento, da Copernicus per l'osservazione terrestre, da costellazioni commerciali per le comunicazioni, crea interdipendenze complesse. I piani di *business continuity* devono prevedere scenari di degradazione o indisponibilità dei servizi *space-based*.

Coordinamento istituzionale. L'ecosistema europeo coinvolge ESA, EUSPA, ENISA, Commissione Europea e agenzie nazionali. Per le aziende italiane, l'ASI rappresenta il punto di riferimento primario, ma la complessità del quadro richiede competenze specifiche di *regulatory intelligence*.

Il coordinamento ESA-EUSPA-ENISA

La *governance* della cybersecurity spaziale europea si articola su tre pilastri istituzionali con competenze complementari.

ESA (Agenzia Spaziale Europea) gestisce gli aspetti tecnico-scientifici, inclusa la cybersecurity delle missioni che sviluppa e opera. Il centro ESEC di Redu (Belgio) ospita la *Cybersecurity Facility* per test e validazione, mentre ESRIN a Frascati analizza e investiga gli incidenti. L'ESA sta adottando certificazioni di cybersecurity che includono *best practice* di *secure software engineering* e architetture *zero-trust*.

EUSPA (Agenzia dell'Unione Europea per il Programma Spaziale) gestisce l'infrastruttura operativa di Galileo, EGNOS e Copernicus, e coordinerà l'implementazione del GovSatCom Hub per IRIS². L'*EU Space Act* ne amplia significativamente le responsabilità, includendo *assessment* tecnici per l'autorizzazione degli operatori e la gestione del Registro degli Oggetti Spaziali dell'Unione (URSO).

ENISA (Agenzia dell'Unione Europea per la Cybersecurity) fornisce l'expertise trasversale di cybersecurity, come dimostrato dal report *Space Threat Landscape 2025* che ha mappato 281 controlli di sicurezza da 13 *framework* di cybersecurity. ENISA detiene anche un ruolo di osservatore nell'EU Space ISAC (*Information Sharing and Analysis Centre*), istituito nel 2024 come hub per lo scambio di *threat intelligence* nel settore.

Per i professionisti della sicurezza italiani, questo

significa che la *compliance* alla cybersecurity spaziale richiederà familiarità con standard e *guideline* provenienti da fonti multiple – non solo la NIS2, ma anche gli standard ECSS (*European Cooperation for Space Standardization*), le *best practice* NASA e i *framework* specifici che emergeranno dall'implementazione dell'*EU Space Act*.

Oltre la *compliance*: prospettive strategiche

La cybersecurity spaziale non è solo un obbligo regolatorio: è un fattore competitivo in un mercato globale in forte espansione. Secondo le proiezioni di McKinsey e World Economic Forum, la *space economy* globale potrebbe raggiungere 1,8 trilioni di dollari entro il 2035, partendo dai 630 miliardi del 2023. Alcune tendenze meritano attenzione strategica.

***Active debris removal*.** Con l'accumulo di detriti che alimenta il rischio Kessler, emergeranno servizi di rimozione attiva (come la missione ClearSpace-1 dell'ESA). Questi sistemi introdurranno nuove superfici d'attacco: un veicolo spaziale progettato per "catturare" oggetti in orbita potrebbe teoricamente essere *weaponizzato* se compromesso.

***Software-defined satellites*.** La tendenza verso satelliti riconfigurabili via software aumenta la flessibilità operativa ma espande la superficie d'attacco. La capacità di modificare le funzionalità di un satellite in orbita è un vantaggio per l'operatore legittimo – e per un attaccante che ottenga accesso ai sistemi di comando.

Crittografia *quantum-resistant*. L'ESA sta sviluppando una piattaforma di verifica quantistica per contrastare la minaccia del *quantum computing* alla crittografia tradizionale. I satelliti lanciati oggi dovranno rimanere operativi per 5-15 anni: la crittografia post-quantum non è un problema futuro, è una decisione progettuale immediata.

Autonomia strategica. La dipendenza da costellazioni extra-europee (Starlink, GPS) per servizi critici crea vulnerabilità geopolitiche che il programma IRIS² mira a mitigare. Per le aziende della difesa e delle infrastrutture critiche, la provenienza dei servizi *space-based* diventerà un criterio di selezione.

Conclusioni

La cybersecurity spaziale è uscita dai laboratori delle agenzie governative per entrare nell'agenda strategica di ogni organizzazione che dipenda – direttamente o indirettamente – da servizi satellitari. E nella società digitale contemporanea, questo significa praticamente tutte.

L'*EU Space Act*, insieme al *framework* NIS2 e al report ENISA, definisce un nuovo *baseline* di sicurezza per il settore. Gli operatori italiani della *space economy* hanno l'opportunità di trasformare un obbligo di *compliance* in un vantaggio competitivo, posizionandosi come *partner* affidabili in un ecosistema europeo che valorizza sempre più la resilienza cyber.

Per i CISO e i *security architect*, il messaggio è chiaro: l'orbita non è più il confine ultimo del perimetro di sicurezza, è un'estensione che richiede competenze specifiche, collaborazione istituzionale e visione strategica. La cybersecurity spaziale non è il futuro: è il presente.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/cybersecurity-spaziale-satelliti/