GOVTECH

L'approccio italiano al dominio spaziale interconnesso con il cyberspazio e le tecnologie emergenti

A cura di *Valentina Chabert*

21 MAGGIO 2026

Questo studio analizza l'approccio italiano al dominio spaziale come dimensione strategica sempre più interconnessa con il cyberspazio e le tecnologie emergenti. Il paper esamina le interdipendenze tra infrastrutture spaziali e sicurezza cibernetica, evidenziando i rischi derivanti dalla digitalizzazione dei sistemi satellitari. Particolare attenzione è dedicata alle implicazioni per la sicurezza nazionale e alla resilienza delle infrastrutture critiche, nonché al ruolo dell'Italia nella filiera spaziale e alle iniziative di rafforzamento industriale e tecnologico.

GovTech – Geopolitical Brief n. 62/maggio 2026

Centro Studi Geopolitica.info | www.geopolitica.info | centrostudi@geopolitica.info

Il volume costituisce un prodotto di ricerca del progetto "GovTech – Governare l'era tecnologica: l'Italia tra cybersecurity, intelligenza artificiale e nuove sfide internazionali" realizzato dal Centro Studi Geopolitica.info in collaborazione con il Centro di Ricerca Cooperazione con l'Eurasia, il Mediterraneo e l'Africa Sub-Sahariana (CEMAS) e finanziato dall'Unità di Analisi, Programmazione, Statistica e Documentazione Storica del Ministero degli Affari Esteri e della Cooperazione Internazionale. Le opinioni contenute nella presente pubblicazione sono espressione degli autori, e non rappresentano necessariamente le posizioni del Ministero degli Affari Esteri e della Cooperazione Internazionale, né quelle delle altre Istituzioni partner.

ISSN : 3103-3407

INDICE

L'approccio italiano al dominio spaziale interconnesso con il cyberspazio e le tecnologie emergenti

Valentina Chabert

Spazio: da dominio di interesse scientifico a terreno di competizione

Dagli anni Cinquanta ed in particolare a partire dai primi esperimenti di messa in orbita di satelliti durante l'era del bipolarismo nelle relazioni internazionali, il settore spaziale ha subìto profonde modifiche in termini di innovazione tecnologica e assetti cooperativi tra potenze spaziali. In particolare, gli ultimi decenni sono stati testimoni di una progressiva erosione del monopolio statale nel settore spaziale, in favore dell'ingresso di società private dotate di notevoli capacità tecniche, ingenti disponibilità di capitali e di una spinta innovativa tale per cui sembra prendere forma un modello di *governance* "dal basso verso l'alto",[1] guidato da società commerciali che promettono sviluppi tecnologici continui, rapidi e più economici rispetto al passato.[2] Su questa linea, l'entrata in una nuova fase della corsa allo spazio ha portato all'alternanza di una significativa cooperazione internazionale (la costruzione della Stazione Spaziale Internazionale ne è un esempio) con periodi di più intensa competizione tra potenze, mosse da differenti imperativi di natura securitaria, economica e geopolitica.[3] In un simile contesto, il progressivo sviluppo tecnologico ha svolto un ruolo chiave nell'identificazione dell'ambiente spaziale come infrastruttura critica. All'aumento del numero di satelliti in orbita è infatti corrisposta una crescente dipendenza umana da tali sistemi, tale per cui attualmente le infrastrutture spaziali risultano fondamentali per le comunicazioni, la

[1] P. Samson, Is the Earth's Orbit Becoming a Lawless Frontier?, *CICI Cybersecurity and Outer Space Essay Series*, 2023.
[2] L. Dawson, *The politics and perils of space exploration. Who will compete, who will dominate?* Springer, 2nd edition, 2021, p. 44.
[3] Società Italiana per l'Organizzazione Internazionale (SIOI), *Alla conquista dell'ottavo continente: lo Spazio, La Comunità Internazionale,* Quaderno 21, Editoriale Scientifica Napoli, 2021, p. 46.

navigazione e l'osservazione della Terra, così come per la sincronizzazione delle transazioni finanziarie, i trasporti e le previsioni meteorologiche, tra gli altri aspetti. [4] I sistemi basati sullo spazio risultano altresì critici nel corso di operazioni militari, consentendo un comando e controllo sicuri, la navigazione, la raccolta di informazioni e l'allerta precoce delle minacce. Inoltre, le infrastrutture spaziali forniscono comunicazioni essenziali per il coordinamento delle forze, la guida di sistemi d'arma e il monitoraggio dei movimenti sul terreno dell'avversario. Pertanto, anche in prospettiva militare si riconferma il ruolo centrale dei sistemi spaziali, il cui eventuale danneggiamento potrebbe destabilizzare la prontezza militare, la risposta alle crisi e la coesione delle Forze Armate di uno Stato.[5]

Come emergerà nel corso del presente lavoro, affermandosi quale spina dorsale di alcune delle principali attività economiche moderne, l'infrastruttura spaziale è ugualmente oggetto di potenziali effetti dannosi derivanti da eventuali perdite di capacità, aprendo parallelamente a rischi e vulnerabilità non trascurabili da parte degli Stati. [6] La dimensione cibernetica diviene, a questo proposito, imprescindibile: nonostante un generale consenso sulla necessità di un'attenzione mirata alla connessione tra spazio extra-atmosferico e spazio cibernetico alla luce delle potenziali minacce alla sicurezza provenienti dalla vulnerabilità delle infrastrutture critiche spaziali e da attacchi mirati contro di esse, attualmente non si riscontrano linee guida dettagliate e specifiche per il settore della sicurezza informatica destinate agli operatori di satelliti

[4] Cfr. M. Spagnulo, *Capitalismo stellare. Come la nuova corsa allo spazio cambia la Terra*, Rubettino, 2023.

[5] J. Cournoyer, Securing the space-based assets of NATO members from cyberattacks. A framework to strenghten cybersecurity in outer space, *Royal Institute of International Affairs International Security Programme Research Paper,* 2025, pp. 6-8.

[6] B. Gallant, J. Miller, The Growth of the Space Economy and New Cyber Vulnerabilities, *CIGI Cybersecurity and Outer Space Essay Series*, 2023.

commerciali e in generale all'intera catena delle infrastrutture spaziali - dalle orbite ai segmenti di terra.[7] Tuttavia, la crescente dipendenza del settore spaziale dai sistemi informatici e il conseguente nesso "spazio-*cyber*" derivante dall'impiego di componenti *hardware* e *software*, dalla riconfigurazione dei satelliti in orbita, dall'utilizzo dell'intelligenza artificiale e di tecnologie quantistiche rendono le risorse e i dati spaziali sempre più suscettibili a nuove forme di vulnerabilità informatica, in un contesto spaziale sempre più congestionato, contestato e competitivo.[8] Le vulnerabilità descritte e le tendenze evolutive del settore spaziale interessano anche l'Italia, la cui infrastruttura spaziale si regge su una rete di aziende pionieristiche attive nel settore della difesa, piccole e medie imprese, *startup* d'avanguardia e un sistema di alleanze che si realizza tramite una stretta cooperazione con le principali potenze spaziali internazionali - gli Stati Uniti *in primis* - e una collaborazione strategica con l'Agenzia Spaziale Europea (ESA).[9]

In questo contesto, il lavoro porrà al centro l'approccio italiano al dominio spaziale come ambito strategico sempre più interconnesso con il cyberspazio e le tecnologie emergenti, volgendo lo sguardo alle crescenti interdipendenze tra le infrastrutture spaziali, la cybersicurezza e l'intelligenza artificiale. Si evidenzieranno in modo particolare i rischi e le vulnerabilità legate alla digitalizzazione dei sistemi spaziali – dalle orbite in cui stazionano i satelliti, ai dati e al cosiddetto *ground segment*, al fine di valutare le potenziali implicazioni in termini di sicurezza nazionale. Da ultimo, un'enfasi sull'interconnessione del

[7] European Union Agency for Cybersecurity (ENISA), *Space Threat Landscape*, 2025, pp. 7-8.
[8] A. Shul, W. Wark, J. West, Securing the new Space Domain: An Introduction, *CIGI Cybersecurity and Outer Space Essay Series*, 2023.
[9] K. Muti, O. Credi, G. La Rocca, Il sistema-Paese Italia di fronte alle sfide dello spazio: tra space economy, cooperazioni internazionali e cybersecurity, *Istituto Affari Internazionali*, 2023, p. 5. Si veda anche A. Aresu, R. Mauro, *I cancelli del cielo. Economia e politica della grande corsa allo spazio 1950-2050*, Luiss University Press, 2022.

settore spaziale con il dominio cibernetico intende mettere in risalto una concezione sempre più radicata dello spazio come estensione della dimensione *cyber*, idonea a configurarsi come nesso imprescindibile nei moderni scenari di competizione tecnologica.

Spazio extra-atmosferico e spazio cibernetico: convergenza securitaria e tecnologie emergenti

Nonostante sussistano differenze strutturali tra i due domini, il cyberspazio e lo spazio extra-atmosferico condividono una serie di analogie derivanti dalla loro natura aperta, condivisa e transfrontaliera. [10] Pertanto, una maggiore interdipendenza tra le due dimensioni dovuta all'incremento del numero di satelliti e la conseguente digitalizzazione dei sistemi spaziali hanno significativamente acuito i rischi di attacchi informatici contro le infrastrutture spaziali. In effetti, i satelliti sono spesso dotati di componenti *software* e di connessione ad internet. Inoltre, la maggior parte dei processi di progettazione, produzione, collaudo, lancio e gestione dei satelliti avviene tramite tecnologie digitali. A ciò è dunque seguita un'estensione della superficie di attacco, ossia dei punti di accesso potenzialmente sfruttabili da un aggressore per interrompere, danneggiare, disabilitare o assumere il controllo di un satellite. A titolo di esempio, alcuni studi hanno calcolato che un'eventuale indisponibilità del sistema di navigazione statunitense GPS potrebbe generare un impatto economico di circa 1 miliardo di dollari al giorno. Similmente, un attacco informatico ad un satellite potrebbe causare un'interruzione dei mercati finanziari, dei trasporti su strada, delle previsioni metereologiche, delle reti

[10] P. Meyer, Outer Space and Cyber Space: a Tale of Two Security Realms, in: A. M. Osula, H. Roigas (eds), *International Cyber Norms: Legal, Policy and Industry Perspectives*, NATO CCD COE Publications, 2016.

elettriche e addirittura del controllo del traffico aereo o di operazioni militari in corso.[11]

Tuttavia, la sicurezza informatica dei sistemi spaziali non si limita al satellite in orbita, bensì comprende l'intera catena di approvvigionamento, l'utente, i segmenti di terra e quelli spaziali durante l'intero ciclo di vita dell'infrastruttura, creando ulteriori livelli di complessità. I sistemi spaziali infatti consistono di tre componenti, tutte ugualmente necessarie al corretto funzionamento dell'infrastruttura: i satelliti in orbita, le comunicazioni e i dati inviati da e verso i satelliti e le stazioni di terra che controllano i satelliti o ricevono i dati e i segnali da essi. Dunque, le capacità informatiche risultano fondamentali per l'ambiente spaziale nel suo complesso e per la stabilità e la prevedibilità delle sue risorse.[12]

Sebbene gli attacchi informatici richiedano un alto grado di comprensione degli *asset* spaziali presi di mira, essi non esigono necessariamente risorse significative per essere portati a termine. I cyberattacchi contro i satelliti implicano di fatto una serie complessa di vulnerabilità che compromettono la stabilità e la funzionalità dei sistemi spaziali. Tra esse si distinguono il *jamming*, lo *spoofing* e il *Man-in-the-Middle* (MiTM). Il *jamming* prevede l'interruzione deliberata della connettività del server attraverso un'interferenza con i segnali di comunicazione, ottenuta trasmettendo energia elettromagnetica sulle stesse frequenze dei segnali bersaglio e sovraccaricando il ricevitore. In questo modo, viene impedito il recupero dei segnali attaccando il *downlink* tra il satellite e il ricevitore a terra o l'*uplink* tra la stazione di terra e il satellite. Il fine ultimo di un simile attacco consiste nell'intralciare trasmissioni, reti o servizi internet per

[11] C. Poirier, Understanding Cybersecurity in Outer Space, *CSS Analyses in Security Policy*, n. 343, 2024, p.2.
[12] V. Samson, The Cyber Counterspace Threat: Coming Out of the Shadows, *CICI Cybersecurity and Outer Space Essay Series,* 2023.

interferire con le comunicazioni satellitari globali, con impatti estesi sino al diniego del servizio e all'interruzione di sistemi critici dipendenti dai satelliti sulla Terra o nello spazio. Sulla stessa linea, lo *spoofing* sfrutta una tecnica illusoria tale per cui l'attore altera i segnali di comunicazione per ingannare il destinatario, dando l'impressione di autenticità dei dati. La tecnica di attacco sfrutta i ricevitori *online,* facendo credere che i segnali decimati siano autentici e dunque mettendo in pericolo veicoli spaziali o satelliti alterandone la traiettoria per il tramite di dati ingannevoli. Per quanto riguarda le reti e i sistemi informatici spaziali, gli aggressori possono altresì manipolare i sensori o i dati da cui dipendono i sistemi o le reti: questi si basano su dati precisi per eseguire operazioni computerizzate automatizzate, raccogliere informazioni e comunicare dettagli significativi ai controllori di terra. Manipolando questi dati, gli aggressori possono causare operazioni automatizzate indesiderate, innescando un comportamento imprevedibile del veicolo spaziale o del satellite. Inoltre, i dati manipolati potrebbero inviare ai controllori di terra informazioni ingannevoli, minando l'affidabilità e l'integrità del veicolo spaziale. Da ultimo, un attacco *MitM* si verifica quando l'autore falsifica e intercetta i dati posizionandosi tra l'utente e il sistema.

I moderni attacchi informatici contro i sistemi spaziali risultano solitamente più difficili da rilevare, con conseguenze che vanno dalla negazione del servizio su vasta area o guasti mirati all'integrità dell'infrastruttura.[13] Non sono inoltre da escludere ulteriori modalità attraverso cui le capacità informatiche potrebbero essere impiegate deliberatamente al fine di danneggiare tanto i satelliti militari quanto quelli commerciali. Intrusioni informatiche potrebbero infatti consentire il controllo dei satelliti e la loro trasformazione in strumenti capaci di schiantarsi

[13] K. Yang, M. Hassan, A review of the legal nature of cyberattacks in outer space, *Acta Astronautica*, vol. 244, 2026, pp. 335-343.

contro altri *hardware* presenti in orbita, causando danni tali da renderli inutilizzabili.[14] È quanto è avvenuto nel 1998 a seguito del controllo, da parte di un gruppo di hacker, del satellite astronomico tedesco ROSAT, i cui pannelli solari sono stati puntati verso il sole e dunque distrutti, causando detriti che ancora oggi rappresentano un rischio per la sicurezza di altri oggetti e operatori in orbita. Più di recente, nel mese di novembre 2021, la Federazione Russa ha distrutto un satellite di epoca sovietica – il *Kosmos 1408* – per il tramite di un missile antisatellite che ha generato oltre 1500 frammenti e costretto gli astronauti presenti sulla Stazione Spaziale Internazionale a rifugiarsi nelle capsule di emergenza in via precauzionale. Infine, sul fronte cinese un simile episodio risale al 2007, con la deliberata distruzione da parte delle autorità di Pechino del satellite meteorologico *Fengyun-1C* attraverso un missile ASAT. Oltre a produrre più di 3500 frammenti di detriti ancora oggi in orbita, l'attacco contro il satellite ha messo in luce il rischio concreto di compromissione di ulteriori sistemi spaziali potenzialmente coinvolti.

Limitatamente alle conseguenze, oltre ai danni di natura non fisica gli attacchi informatici alle infrastrutture spaziali possono risultare in altrettanti danni significativi all'*hardware*. Offensive mirate contro sistemi satellitari sono suscettibili di danneggiare fisicamente i satelliti, deorbitandoli, provocando detriti in orbita, danni sulla Terra e interruzioni di servizi critici, con conseguenti danni a infrastrutture e talvolta vite umane. A questo proposito, l'Agenzia dell'Unione Europea per la Cybersicurezza (ENISA) ha stimato che le conseguenze derivanti da attacchi cibernetici contro infrastrutture critiche spaziali risulterebbero ulteriormente aggravate dal duplice uso degli *asset* satellitari, per cui tecnologie commerciali destinate all'uso civile potrebbero

[14] J. West, Where Outer Space Meets Cyberspace: A Human-Centric Look at Space Security, *CICI Cybersecurity and Outer Space Essay Series,* 2023.

comunque essere impiegate come armi a sostegno di obiettivi geopolitici.[15] È quanto emerso, ad esempio, dall'attacco cibernetico al satellite Viasat nel 2022 a poche ore dall'invasione russa dell'Ucraina, responsabile dello spegnimento di decine di migliaia di modem in tutta Europa e dell'interruzione tanto di attività economiche, quanto di diverse funzioni vitali tra cui servizi di emergenza.[16]

Simili effetti a catena sono destinati a diventare più comuni con l'avvento dell'intelligenza artificiale e dell'*Internet of Things* (IoT), che crea complesse reti interconnesse di dispositivi informatici, macchine, dati, oggetti e persone fortemente dipendenti dai sistemi spaziali.[17]

Pertanto, la sicurezza informatica dei sistemi spaziali assume un ruolo fondamentale per garantire il corretto funzionamento dei servizi spaziali e delle infrastrutture di supporto.[18] Tuttavia, permangono numerose criticità al fine del raggiungimento di tale obiettivo. *In primis*, secondo quanto emerge dallo *Space Attacks Open Database Project*, una base dati che raccoglie informazioni relative ad attacchi pubblicamente noti contro satelliti tra il 1977 e il 2019, la divulgazione di episodi di offese cibernetiche non risulta essere una pratica consolidata.[19] In aggiunta, è solo con l'integrazione di studi specifici[20] e rapporti pubblicamente disponibili su singoli incidenti di sicurezza informatica nel dominio spaziale che si evince una più ampia targetizzazione di obiettivi commerciali, governativi e -

[15] ENISA, *cit.,* p. 8.
[16] *Ivi,* pp. 17-18.
[17] R. Mazzolin, Responding to the Cybersecurity Challenges of the New Space Environment, *CICI Cybersecurity and Outer Space Essay Series*, 2023.
[18] C. Poirier, Establishing a governance for cyber operations in outer space: Exploring challenges faced by space and cyber commands, *Acta Astronautica*, vol. 237, 2025, p. 236.
[19]Space Attacks Open Database Project. Disponibile al link: https://www.spacesecurity.info/space-attacks-open-database/.
[20] W. Wark, The Five Eyes and Space: A New Frontier for an Old Intelligence Alliance, *CICI Cybersecurity and Outer Space Essay Series*, 2023.

soprattutto dagli anni 2000 - del *ground segment* dell'infrastruttura spaziale.[21] In secondo luogo, permangono incertezze relative al nesso tra gli ambiti giuridici dello spazio extra-atmosferico e del cyberspazio, con la potenziale sussistenza di una zona grigia in cui l'applicazione del diritto internazionale risulta poco chiara o carente. In effetti, il diritto fornisce un contributo essenziale alla *governance* senza tuttavia essere sufficiente a garantire una condivisione piena ed efficiente delle responsabilità tra gli attori che operano nel settore spaziale, complice la natura multiforme delle vulnerabilità e delle minacce informatiche, la multifunzionalità dei sistemi spaziali e l'interconnessione delle capacità spaziali con i servizi terrestri. Dunque, la cooperazione e il coordinamento tra operatori geograficamente dispersi e tra settori commerciali e governativi diventa essenziale e al contempo una sfida, anche all'interno di un singolo Stato o di un gruppo di alleati. A livello globale, inoltre, una simile sfida è ulteriormente complicata dalla competizione tra potenze e da una diversa percezione delle minacce, lasciando scoperto un fronte essenziale per il futuro del settore spaziale.[22]

In terzo luogo, come anticipato, le interferenze informatiche appaiono difficili da rilevare, da distinguere da fonti involontarie o naturali e complesse da attribuire a specifici attori. Il fatto che le capacità informatiche siano utilizzate non solo dagli Stati ma anche da attori non statuali inclusi *hacktivisti*, gruppi terroristici, *proxy* e criminali informatici, rende ancora più intricata l'individuazione e la persecuzione dei responsabili. Nel complesso, risulta dunque difficile prevenire simili attacchi a fronte della continua evoluzione delle minacce, degli attori coinvolti e dei punti di vulnerabilità, non limitati al software bensì inclusivi della

[21] ENISA, *cit.,* p. 29; C. Poirer, Understanding Cybersecurity in Outer Space, *cit.,* p.2.
[22] A. Shul, W. Wark, J. West, *cit.*

rete di componenti, servizi e fornitori delle catene di approvvigionamento dei sistemi satellitari.[23]

Alla luce di ciò, un aggiornamento delle strategie di tutela delle infrastrutture critiche che includa anche i sistemi spaziali nella loro interezza potrebbe avere un impatto significativo in termini di resilienza e preparazione alle minacce provenienti dal dominio cyberspaziale. A questo proposito, standard tecnici, di servizio e requisiti di condivisione delle informazioni, così come una migliore allocazione delle risorse per la mitigazione delle conseguenze derivanti da attacchi cibernetici, appaiono urgenti per il rafforzamento delle capacità di cybersicurezza dei sistemi spaziali. Non meno importante, infine, l'elemento umano, che rimane la chiave di volta per l'incremento di strategie efficaci di difesa cibernetica: un ecosistema solido capace di valorizzare al meglio esperti e professionisti del settore è quantomai essenziale per la formazione di una futura generazione di specialisti in grado di combinare un'elevata conoscenza informatica con la comprensione dei rischi e delle vulnerabilità derivanti dal settore spaziale, da realizzarsi in combinazione con il settore privato , il cui ruolo nella filiera spaziale è teso ad un progressivo incremento.[24]

Il ruolo dell'Italia nella filiera spaziale internazionale: verso la definizione di una profondità strategica

Con il lancio del San Marco 1 il 15 dicembre del 1964 grazie all'ingegno di un gruppo di ricercatori dell'Università "La Sapienza", l'Italia si è affermata come potenza nel teatro spaziale mantenendo una posizione di successo per tutti i decenni successivi, tanto a livello europeo con il contributo alla fondazione

[23] J. West, *cit.*
[24] B. Gallant, J. Miller, *cit.*

dell'Agenzia Spaziale Europea, quanto a livello internazionale.[25] L'ambizione di portare l'Italia al centro dell'attenzione mondiale in ambito spaziale si è recentemente concretizzata con l'approvazione del Senato, lo scorso 20 dicembre 2023, del disegno di legge sul *Made in Italy*, che prevede interventi di valorizzazione, promozione e tutela delle eccellenze nazionali italiane anche nel campo della politica industriale del Paese, con iniziative volte a stimolare e proteggere la crescita delle filiere strategiche nazionali in vista delle sfide globali del presente. Al settore spaziale quale pilastro decisivo per il comparto industriale italiano è stata riservata un'attenzione particolare anche nell'ottica del raggiungimento dell'obiettivo più ampio di garantire un accesso autonomo europeo allo spazio. Un proposito che si intreccia nuovamente, nella storia dell'Italia, con il continente africano, da cui sono dipesi il protagonismo e l'iniziale avventura spaziale italiana e che ha visto un rinnovato interesse del paese in ambito spaziale soprattutto nei confronti del Kenya attraverso il Piano Mattei. A titolo di esempio, in conclusione dell'incontro a Roma con il presidente del Kenya William Ruto il 20 aprile scorso, il Premier Giorgia Meloni ha infatti affermato con decisione la volontà dell'Italia di potenziare il Centro Spaziale Luigi Broglio di Malindi, base operativa dell'Agenzia Spaziale Italiana (ASI), al fine di renderlo un *hub* continentale di formazione ed eccellenza tale da permettere all'Italia una proiezione nel continente africano, strategico per i lanci orbitali grazie alla sua vicinanza all'equatore.[26]

[25] S. Marchisio, Italy as the Launching State of the San Marco I, *Ordine Internazionale e Diritti Umani*, 2025.

[26] AGEEI, Spazio, Italia-Kenya, Meloni incontra il Presidente Ruto, 21 aprile 2026. Disponibile al link: https://ageei.eu/spazio-italia-kenya-meloni-incontra-il-presidente-ruto-potenziare-il-centro-spaziale-luigi-broglio-a-malindi/.

Al contempo, il protagonismo dell'Italia nel *dossier* spazio si espleta attraverso numerosi assetti collaborativi soprattutto in ambito europeo e occidentale, in modo particolare attraverso la cooperazione con la NASA. Di fatto, con un miliardo di euro di budget annuale, il supporto chiave è fornito dall'ASI, che svolge il compito di coordinare progetti relativi all'esplorazione spaziale, all'osservazione della Terra e all'abilitazione dell'industria spaziale. Al contempo, l'Italia risulta essere il terzo finanziatore dell'ESA, nonché tra i firmatari degli Accordi Artemis, grazie ai quali le imprese italiane hanno svolto un ruolo protagonista nella missione Artemis II lanciata il 1° aprile 2026 e ricopriranno altresì una posizione di prim'ordine per le successive missioni. Con la coordinazione dell'ASI, la Penisola ha infatti apportato un notevole contributo ad *Orion*, il modulo di servizio che insieme al *Space Launch System* della NASA ha costituito il fulcro di Artemis I; in Artemis II, Leonardo ha realizzato i pannelli fotovoltaici che compongono le ali del modulo e le unità di controllo e distribuzione della potenza, fondamentali per fornire alimentazione a tutta l'elettronica di bordo e alimentare *Orion* durante il viaggio di andata e ritorno dalla Luna; infine, nel sito di Thales Alenia Space a Torino sono in realizzazione per la NASA e l'ASI la prima casa sulla Luna per gli astronauti e il primo *lander* lunare europeo – *Argonaut* – progettato per l'ESA per il trasporto e l'atterraggio di carichi sulla superficie lunare.

Non meno importante, in termini legislativi la centralità del settore spaziale italiano si deve ad una riconfigurazione delle norme esistenti in materia a partire dal 2018, dapprima con la legge 7/2018 *Recante Misure per il Coordinamento della Politica Spaziale e Aerospaziale e Disposizioni concernenti l'Organizzazione e il Funzionamento dell'Agenzia Spaziale Italiana*, che ha previsto che la direzione e il coordinamento delle politiche spaziali e aerospaziali siano attribuiti al Presidente del Consiglio, mentre gli indirizzi di Governo ad un comitato

interministeriale *ad hoc*.[27] In particolare, le telecomunicazioni, la navigazione e l'osservazione della Terra saranno oggetto delle politiche sviluppate nei prossimi anni, in aggiunta alla *Strategia Nazionale di Sicurezza per lo Spazio* approvata dal COMINT nel luglio dello stesso anno.[28] Tra gli obiettivi strategici del documento, la garanzia della sicurezza delle infrastrutture spaziali e la tutela del comparto istituzionale, industriale e scientifico figurano tra le priorità del Paese. Più recentemente, con la legge 89 del 13 giugno 2025 recante *Disposizioni in materia di economia dello spazio*, anche l'Italia si è dotata di una disciplina delle attività spaziali condotte da operatori privati sul territorio nazionale e da operatori italiani al di fuori del territorio nazionale, sul modello già adottato da numerosi paesi europei ed extraeuropei.[29]

Con queste premesse, dall'interconnessione tra il settore spaziale e la cybersicurezza e le implicazioni securitarie descritte nel paragrafo precedente, emerge una chiara necessità per l'Italia di adattare il proprio approccio strategico integrando sicurezza spaziale e cibernetica. In modo particolare, un simile approccio risulta impellente alla luce dell'importanza che il settore spaziale ha rivestito e che occupa nel panorama economico attuale, frutto di una crescente attenzione all'operato di *startup*, piccole e medie imprese e società già attive nel campo dell'industria della difesa, che hanno assunto un ruolo via via più incisivo nel settore della *new space economy* e nelle partnership internazionali dell'Italia in ambito spaziale.

[27] Legge 11 gennaio 2018 n.7, pubblicata in G.U. n.34 del 10 febbraio 2018.
[28] Presidenza del Consiglio dei Ministri, Strategia nazionale di sicurezza per lo spazio, COMINT, 18 luglio 2019.
[29] Presidenza del Consiglio dei Ministri, Ufficio per le Politiche Spaziali e Aerospaziali, *Disposizioni in materia di economia dello spazio.* Disponibile al link: https://www.ufficiopolitichespaziali.gov.it/home/normativa/disposizioni-in-materia-di-economia-dello-spazio/.

A tale scopo, il Ministero degli Esteri e della Cooperazione Internazionale (MAECI) ha progressivamente riconosciuto la rilevanza strategica del settore spaziale e la necessità di garantire la protezione delle infrastrutture critiche da minacce cibernetiche, promuovendo specifiche linee di indirizzo politico e partecipando a programmi di cooperazione con partner internazionali volti al rafforzamento della sicurezza spaziale e *cyber*. Il MAECI ha infatti riconosciuto come lo spazio rappresenti per l'Italia un motore di innovazione tecnologica, competitività e crescita economica attraverso una solida partecipazione ai principali programmi europei ed internazionali, sostenuta da uno sforzo diplomatico che ha permesso all'Italia di presiedere il Comitato delle Nazioni Unite per gli usi pacifici dello spazio extra-atmosferico (COPUOS) nel biennio 2026-2027.[30] Al fine di promuovere una maggiore cooperazione internazionale nell'utilizzo pacifico dello spazio e allo stesso tempo la sicurezza, il MAECI ha altresì intrapreso una ferma strategia diplomatica in ambito cibernetico, fondata sul multilateralismo e la condivisione di informazioni finalizzata a prevenire attacchi cibernetici e contribuire alla definizione di una governance del cyberspazio aperta, accessibile e rispettosa del diritto internazionale. L'impegno del MAECI si concretizza, tra gli altri fronti, nell'attuazione della *Strategia Nazionale di Cybersicurezza* nei fora multilaterali e nell'ambito di coalizioni informali, a livello europeo, onusiano, nell'Alleanza Atlantica, nel contesto dell'Organizzazione per la Sicurezza e la Cooperazione in Europa (OSCE) e in seno al G7. Considerate le principali minacce cibernetiche che potrebbero rappresentare una minaccia per la sicurezza del paese, la coordinazione del MAECI e dell'Agenzia per la Cybersicurezza Nazionale garantisce all'Italia la partecipazione alla *Counter Ransomware Initiative*, avviata informalmente nel

[30] MAECI, Spazio. Disponibile al link: https://www.esteri.it/it/diplomazia-economica-e-politica-commerciale/diplomaziaeconomica/spazio/.

2021 con l'obiettivo di contribuire al fenomeno del furto di dati a scopo di estorsione. Attraverso il MAECI l'Italia ha poi aderito, nel 2023, al *Meccanismo di Tallin*, al fine di sistematizzare e coordinare le attività di assistenza civile all'Ucraina nel campo della cybersicurezza a fronte delle conseguenze dell'aggressione russa. A tal proposito, l'Italia deterrà la presidenza del Meccanismo nei mesi di luglio-dicembre 2026, incentrando la propria attività sulla valorizzazione del partenariato pubblico-privato. Da ultimo, il MAECI ha promosso la presenza italiana a fianco di altri 26 paesi anche nel *Processo di Pall Mall*, un'iniziativa informale lanciata nel 2024 da Francia e Regno Unito per contrastare la proliferazione e l'utilizzo irresponsabile di prodotti commerciali di intrusione cibernetica.[31]

Altrettanto rilevante risulta il rafforzamento da parte dell'Italia della propria postura securitaria attraverso l'allineamento delle proprie strategie spaziali e di cybersicurezza con l'Alleanza Atlantica. La NATO ha infatti individuato lo spazio extra-atmosferico come quinto dominio operativo accanto allo spazio aereo, quello terrestre, quello marino e quello cibernetico, rendendo necessaria la protezione delle infrastrutture critiche posizionate in tale area o dipendenti dallo spazio stesso ai fini della sicurezza dell'Alleanza. A tal proposito, l'Italia ha integrato progressivamente i propri *asset* spaziali (come il sistema di comunicazione militare SICRAL) all'interno di architetture di rete orientate alla sicurezza e alla resilienza.[32] Al contempo, si registra un'intensa cooperazione

[31] MAECI, Diplomazia Cibernetica. Disponibile al link: https://www.esteri.it/it/politica-estera-e-cooperazione-allo-sviluppo/temi_globali/diplomazia_cyber_e_digitale/diplomazia-cibernetica/.

[32] Presidenza del Consiglio dei Ministri, *Government Guidelines on Space and Aerospace*, 14 gennaio 2025. Disponibile al link: https://presidenza.governo.it/AmministrazioneTrasparente/Organizzazione/ArticolazioneUffici/UfficiDirettaPresidente/UfficiDiretta_Meloni/Ufficio_ConsMilitare/GovernmentGuidelinesOnSpaceAndAerospace.pdf.

con la NATO in termini di condivisione delle informazioni relative ad attacchi cibernetici e nell'ambito dei dati di *Space Domain Awareness* (SDA), contribuendo al monitoraggio di detriti, vettori e attività ostili in orbita che potrebbero compromettere la sicurezza collettiva. Uno sforzo che a livello interno si è concretizzato nella firma di un accordo quadro nel mese di ottobre 2025 tra l'Agenzia Spaziale Italiana e l'Agenzia per la Cybersicurezza Nazionale (ACN) inteso a rafforzare contemporaneamente la resilienza cibernetica e la sicurezza del settore spaziale e aerospaziale italiano per il tramite di soluzioni di sicurezza avanzate, crittografia *quantum-resistant*, metodologie *zero trust* e attività per prevenire e contrastare minacce cibernetiche che potrebbero riguardare le infrastrutture spaziali e il relativo *downstream* applicativo.[33] Dal punto di vista industriale, in linea con la *Commercial Space Strategy* dell'Alleanza Atlantica, l'Italia ha recentemente consolidato i propri legami di sicurezza con alcuni alleati chiave, come dimostrato dai recenti dialoghi strategici sullo spazio con gli Stati Uniti conclusosi nel mese di aprile 2026.[34] Obiettivo finale dell'Italia risulta dunque quello di garantire la resilienza di servizi civili e militari essenziali per la sicurezza del paese, posizionandosi come partner tecnologico e strategico fondamentale per la difesa collettiva della NATO. In questo senso, la rilevanza strategica a cui è assurto lo spazio richiede infatti una presenza italiana di primo piano: a tale fine, ad un costante sviluppo delle proprie capacità tecnologiche e spaziali dovrà affiancarsi la protezione dei propri *asset* strategici e delle infrastrutture critiche spaziali, che potrebbero divenire *target* di specifiche e

[33] Agenzia Spaziale Italiana (ASI), Accordo tra ASI e ACN per rafforzare la cybersicurezza del settore spaziale e aerospaziale, 6 ottobre 2025. Disponibile al link: https://www.asi.it/2025/10/accordo-tra-asi-e-acn-per-rafforzare-la-cybersicurezza-del-settore-spaziale-e-aerospaziale/.

[34] US Department of State, Joint Statement on the Second US – Italy Space Dialogue, 17 aprile 2026. Disponibile al link: https://www.state.gov/releases/bureau-of-oceans-and-international-environmental-and-scientific-affairs/2026/04/joint-statement-on-the-second-u-s-italy-space-dialogue.

deliberate attività malevole di natura cibernetica volte a destabilizzare il paese e a minarne la sicurezza per il tramite degli strumenti della guerra cosiddetta "ibrida", a dimostrazione di quanto lo spazio sia divenuto un dominio operativo sul quale si proiettano tanto alleanze quanto fronti di competizione in essere sulla superficie terrestre.[35]

Conclusioni

Alla luce delle dinamiche analizzate, il dominio spaziale si configura non solo come un'infrastruttura critica autonoma, bensì come una vera e propria estensione del cyberspazio, con cui condivide vulnerabilità, logiche operative e crescente interdipendenza tecnologica. In questo senso, lo spazio extra-atmosferico assume il ruolo di *enabling domain*, ossia di moltiplicatore di capacità civili e militari che abilita funzioni essenziali per le economie contemporanee e, al contempo, rappresenta uno dei principali teatri della competizione tecnologica tra attori statali e non statali. La convergenza tra sistemi spaziali, cybersicurezza e tecnologie emergenti – *in primis* l'intelligenza artificiale – rafforza ulteriormente questa centralità, amplificandone tuttavia anche la superficie di attacco e la complessità della gestione del rischio.

Appare dunque necessario superare approcci settoriali e frammentati, al fine di promuovere una maggiore integrazione tra politiche spaziali e cibernetiche tramite strategie coordinate che tengano conto dell'intero ciclo di vita delle infrastrutture spaziali, includendo tanto i segmenti orbitali quanto quelli terrestri e digitali. Parallelamente, risultano imprescindibili investimenti mirati nel rafforzamento della sicurezza informatica dei sistemi spaziali e nell'adozione

[35] V. Chabert, *Guerre Spaziali. Conflitti e competizione per le risorse nell'era delle società private*, Ledizioni, 2025.

responsabile dell'intelligenza artificiale, al fine di garantire resilienza e capacità di risposta in un ambiente sempre più competitivo.

Infine, la natura intrinsecamente globale e interconnessa dello spazio impone un rafforzamento della cooperazione internazionale. La definizione di standard condivisi, meccanismi di fiducia reciproca e iniziative multilaterali nel campo della sicurezza *space-cyber* rappresentano elementi chiave per mitigare i rischi sistemici e prevenire escalation indesiderate. In questa prospettiva, l'Italia – forte del suo posizionamento industriale e delle sue alleanze strategiche – ha l'opportunità di contribuire attivamente alla costruzione di un quadro normativo e operativo più integrato, capace di rispondere alle sfide emergenti e di valorizzare appieno il potenziale dello spazio come dominio abilitante del futuro tecnologico.

Riferimenti bibliografici

AGEEI, Spazio, Italia-Kenya, Meloni incontra il Presidente Ruto, 21 aprile 2026. https://ageei.eu/spazio-italia-kenya-meloni-incontra-il-presidente-ruto-potenziare-il-centro-spaziale-luigi-broglio-a-malindi/.

Agenzia Spaziale Italiana (ASI), Accordo tra ASI e ACN per rafforzare la cybersicurezza del settore spaziale e aerospaziale, 6 ottobre 2025. https://www.asi.it/2025/10/accordo-tra-asi-e-acn-per-rafforzare-la-cybersicurezza-del-settore-spaziale-e-aerospaziale/.

A.Aresu, R. Mauro, *I cancelli del cielo. Economia e politica della grande corsa allo spazio 1950-2050*, Luiss University Press, 2022.

V. Chabert, *Guerre Spaziali. Conflitti e competizione per le risorse nell'era delle società private*, Ledizioni, 2025.

J. Cournoyer, Securing the space-based assets of NATO members from cyberattacks. A framework to strenghten cybersecurity in outer space, *Royal Institute of International Affairs International Security Programme Research Paper,* 2025.

L. Dawson, *The politics and perils of space exploration. Who will compete, who will dominate?* Springer, 2nd edition, 2021.

European Union Agency for Cybersecurity (ENISA), *Space Threat Landscape*, 2025.

B. Gallant, J. Miller, The Growth of the Space Economy and New Cyber Vulnerabilities, *CIGI Cybersecurity and Outer Space Essay Series*, 2023.

Legge 11 gennaio 2018 n.7, Gazzetta Ufficiale n.34, 10 febbraio 2018.

MAECI, Spazio. https://www.esteri.it/it/diplomazia-economica-e-politica-commerciale/diplomaziaeconomica/spazio/.

MAECI, Diplomazia Cibernetica. Disponibile al link: https://www.esteri.it/it/politica-estera-e-cooperazione-allo-sviluppo/temi_globali/diplomazia_cyber_e_digitale/diplomazia-cibernetica/.

S. Marchisio, Italy as the Launching State of the San Marco I, *Ordine Internazionale e Diritti Umani*, 2025.

R. Mazzolin, Responding to the Cybersecurity Challenges of the New Space Environment, *CICI Cybersecurity and Outer Space Essay Series*, 2023.

P. Meyer, Outer Space and Cyber Space: a Tale of Two Security Realms. In: A. M. Osula, H. Roigas (eds), *International Cyber Norms: Legal, Policy and Industry Perspectives*, NATO CCD COE Publications, 2016.

K. Muti, O. Credi, G. La Rocca, Il sistema-Paese Italia di fronte alle sfide dello spazio: tra space economy, cooperazioni internazionali e cybersecurity, *Istituto Affari Internazionali*, 2023.

C. Poirier, Establishing a governance for cyber operations in outer space: Exploring challenges faced by space and cyber commands, *Acta Astronautica*, vol. 237, 2025.

C. Poirier, Understanding Cybersecurity in Outer Space, *CSS Analyses in Security Policy*, n. 343, 2024.

Presidenza del Consiglio dei Ministri, Government Guidelines on Space and Aerospace, 14 gennaio 2025. https://presidenza.governo.it/AmministrazioneTrasparente/Organizzazione/ArticolazioneUffici/UfficiDirettaPresidente/UfficiDiretta_Meloni/Ufficio_ConsMilitare/GovernmentGuidelinesOnSpaceAndAerospace.pdf.

Presidenza del Consiglio dei Ministri, Strategia nazionale di sicurezza per lo spazio, COMINT, 18 luglio 2019.

Presidenza del Consiglio dei Ministri, Ufficio per le Politiche Spaziali e Aerospaziali, *Disposizioni in materia di economia dello spazio.* https://www.ufficiopolitichespaziali.gov.it/home/normativa/disposizioni-in-materia-di-economia-dello-spazio/.

P. Samson, Is the Earth's Orbit Becoming a Lawless Frontier?, *CICI Cybersecurity and Outer Space Essay Series*, 2023.

V. Samson, The Cyber Counterspace Threat: Coming Out of the Shadows, *CICI Cybersecurity and Outer Space Essay Series,* 2023.

A.Shul, W. Wark, J. West, Securing the new Space Domain: An Introduction, *CIGI Cybersecurity and Outer Space Essay Series*, 2023.

Società Italiana per l'Organizzazione Internazionale (SIOI), *Alla conquista dell'ottavo continente: lo Spazio, La Comunità Internazionale,* Quaderno 21, Editoriale Scientifica Napoli, 2021.

Space Attacks Open Database Project. https://www.spacesecurity.info/space-attacks-open-database/.

M. Spagnulo, *Capitalismo stellare. Come la nuova corsa allo spazio cambia la Terra*, Rubettino, 2023.

US Department of State, Joint Statement on the Second US – Italy Space Dialogue, 17 aprile 2026. https://www.state.gov/releases/bureau-of-oceans-and-international-environmental-and-scientific-affairs/2026/04/joint-statement-on-the-second-u-s-italy-space-dialogue.

W. Wark, The Five Eyes and Space: A New Frontier for an Old Intelligence Alliance, *CICI Cybersecurity and Outer Space Essay Series*, 2023.

J. West, Where Outer Space Meets Cyberspace: A Human-Centric Look at Space Security, *CICI Cybersecurity and Outer Space Essay Series,* 2023.

K. Yang, M. Hassan, A review of the legal nature of cyberattacks in outer space, *Acta Astronautica*, vol. 244, 2026.

BIOGRAFIA DELL'AUTORE

Valentina Chabert è dottoressa di ricerca in Diritto Internazionale presso Sapienza Università di Roma e analista di politica internazionale per numerose riviste, think tank e centri di ricerca nazionali ed internazionali. È cultrice della materia in Sicurezza e Studi Strategici presso l'Università LUMSA e in Relazioni Internazionali e Global Governance presso l'Università degli Studi Internazionali di Roma (UNINT). Ha svolto reportage in Ucraina, Caucaso Meridionale e Balcani e condotto attività di ricerca presso l'International Institute for the Unification of Private Law (UNIDROIT), il Consiglio d'Europa, il Center of Analysis of International Relations di Baku e presso le università di Ginevra e Aix-en-Provence. È membro dell'Advisory Board del The Hague Research Institute for Eastern Europe, the South Caucasus and Central Asia.

Geopolitica.info

CENTRO STUDI

Il Centro Studi

Il Centro Studi Il Centro Studi Geopolitica.info nasce nel 2004 con l'obiettivo di offrire un contributo al dibattito sulla politica estera, la geopolitica e le relazioni internazionali dalla prospettiva dell'Italia. Le attività del Centro Studi si articolano in tre filoni principali: la pubblicazione della Rivista online Geopolitica.info e la ricerca in materia di politica internazionale e geopolitica; la formazione attraverso i corsi in presenza e i corsi online sulla piattaforma www.onlineducation.it; l'organizzazione di momenti di dibattito pubblico sui temi dell'agenda politica italiana relativi alle relazioni internazionali. Tutte le attività sono consultabili sul sito web www.geopolitica.info.

I Report del Centro Studi

I report del Centro Studi Geopolitica.info sono collezioni di saggi, realizzati dai ricercatori afferenti alle varie aree del Centro, dedicati ai grandi temi dell'attualità della politica internazionale. Pubblicati a cadenza trimestrale, i report si contraddistinguono per il rigore metodologico e la profondità analitica. Combinando insieme accessibilità e solidità scientifica, essi offrono analisi rigorose e tempestive sui principali dossier della scena globale.

Centro Studi Geopolitica.info

www.geopolitica.info | centrostudi@geopolitica.info