Istituto Affari Internazionali

ISSN 2280-6164

DOCUMENTI IAI 23 | 06 - MARZO 2023

Il dominio spaziale e la minaccia cyber

di Ottavia Credi, Giancarlo La Rocca e Alessandro Marrone

ABSTRACT

Le attività spaziali sono cruciali per il funzionamento delle società moderne, dalle attività economiche a quelle nel campo della sicurezza e difesa. Data la natura critica dell'infrastruttura spaziale, essa rischia di essere obiettivo di una vasta gamma di attacchi, inclusi quelli di natura cyber. La minaccia cyber ai sistemi spaziali è in continua evoluzione, caratterizzata anche da una potenziale convergenza con strumenti di guerra elettronica. Il conflitto in Ucraina ha dimostrato il legame di interdipendenza tra il dominio spaziale e quello cyber, nonché la loro importanza per le operazioni nei domini fisici, e ha reso ancora più evidente le vulnerabilità dei sistemi spaziali a questa tipologia di attacchi. La posizione dell'Unione europea al riguardo è in fase di definizione, anche attraverso politiche e investimenti mirati al raggiungimento di un più alto livello di autonomia nel settore. La Nato sta sviluppando una propria postura spaziale, a seguito del riconoscimento ufficiale di spazio e cyberspazio come domini operativi. Ciononostante, l'attuale livello di cybersicurezza di gran parte delle infrastrutture satellitari europee non è soddisfacente e dovrebbe essere considerato un tema prioritario da affrontare con urgenza.

keywords

Spazio | Cyber | Difesa | Sicurezza | Infrastrutture | Satelliti | Ucraina | Ue | Nato | Italia

ISSN 2280-6164

Il dominio spaziale e la minaccia cyber

di Ottavia Credi, Giancarlo La Rocca e Alessandro Marrone*

1. Due domini co-dipendenti

Le attività spaziali hanno effetti concreti sul funzionamento della società *in toto*[1]. Il caso dei servizi globali di navigazione satellitare (*Global Navigation Satellite System*, Gnss) come Galileo è particolarmente pregnante, in quanto da essi dipendono numerose attività – dalla finanza, alla mobilità, all'energia ma anche risposta e gestione della risposta a calamità ed emergenze, come nel caso del recente terremoto in Siria e Turchia[2]. Anche il settore militare è fortemente connesso e dipendente dagli assetti spaziali, sia nel caso di servizi di posizionamento, navigazione e sincronizzazione (*Position Navigation and Timing*, Pnt) che di Osservazione della Terra e comunicazione satellitare.

A dimostrazione della rilevanza del dominio spaziale in campo economico e finanziario, secondo le stime della Commissione europea il 10 per cento del prodotto interno lordo (Pil) dell'Unione europea (Ue) dipende dalla costellazione Galileo, mentre il programma Copernicus e le Sentinelle in orbita che lo compongono sono il maggiore fornitore di dati al mondo[3]. La sola missione Aeolus dell'Agenzia spaziale europea (*European Space Agency*, Esa) di servizi meteorologici e studio

[1] Intervista, 2 dicembre 2022 b.

[2] Si veda: Esa, *Satellites Support Impact Assessment after Türkiye–Syria Earthquakes*, 13 febbraio 2023, https://www.esa.int/Applications/Observing_the_Earth/Satellites_support_impact_assessment_after_Tuerkiye_Syria_earthquakes.

[3] Sito della Commissione europea: *EU Space Programme*, https://defence-industry-space.ec.europa.eu/node/142_en.

* Ottavia Credi è ricercatrice nei Programmi Sicurezza e Difesa dell'Istituto Affari Internazionali (IAI). Giancarlo La Rocca è ricercatore junior nei Programmi Sicurezza e Difesa dello IAI. Alessandro Marrone è responsabile del Programma Difesa dello IAI. Per l'utile e costruttivo scambio di vedute, lo IAI desidera ringraziare i rappresentanti delle istituzioni intervistati: Servizio europeo per l'azione esterna; Agenzia dell'Unione europea per il programma spaziale; Eutelsat; United Nations Institute for Disarmament Research; Centre for Security, Diplomacy and Strategy della Brussels School of Governance della Vrije Universiteit Brussel; il Ministero della Difesa e in particolare l'Ufficio Generale Spazio dello Stato Maggiore della Difesa e il Comando Operazioni in Rete; Agenzia spaziale europea.

· Questo studio è stato preparato per il seminario "La minaccia cyber allo spazio" organizzato dallo IAI presso la sede dell'Istituto il 14 marzo 2023 con il supporto di Elettronica, ed è stato rivisto alla luce del dibattito ivi svoltosi.

dei venti crea benefici recentemente stimati nell'ordine dei 10 miliardi di euro[4]. Il settore a valle della catena del valore spaziale (*downstream*) si popola sempre più di nuovi utilizzatori ed è traino della crescita globale della *space economy*, con al centro l'utilizzo del dato spaziale.

Le attività spaziali sono altrettanto cruciali per il successo di operazioni militari. Il servizio pubblico regolamentato (*Public Regulated Service*, Prs) di Galileo, di prossima attivazione, renderà possibili ulteriori attività in campo militare. A dimostrazione di ciò, l'Ue sta esaminando l'impatto del Prs per operazioni di difesa europea tramite il progetto *Galileo for EU Defence* (Geode) e in generale della navigazione satellitare, con il progetto *EU Radio Navigation Solution* (Euras) in corso nell'ambito della Cooperazione strutturata permanente (*Permanent Structured Cooperation*, Pesco) e il progetto del Fondo europeo per la difesa (*European Defence Fund*, Edf) *Space and ground-based Navwar surveillance* (dall'acronimo di *Navigation Warfare*)[5]. Risulta dunque chiara e tangibile la natura critica dell'infrastruttura spaziale, in orbita e a terra, e di conseguenza la possibilità di essere un target di esplicito valore per una vasta gamma di attacchi, inclusi di natura cyber.

Il dominio spaziale e quello cyber sono strettamente interdipendenti: da un lato, il secondo è abilitato dagli assetti in orbita; dall'altro, i sistemi spaziali dipendono dallo scambio di dati che avviene nello spettro del cyberspazio[6]. Lo stesso decreto del Presidente del Consiglio dei ministri n. 131 del 30 luglio 2020 che definisce il "perimetro di sicurezza nazionale cibernetica", identifica spazio e cyberspazio tra i settori di attività ritenuti critici per il Paese ai fini della sicurezza nazionale[7]. Si tratta di due domini nati sotto l'egida militare, che hanno subìto derive particolari che ne hanno determinato una crescita non lineare[8].

Oltre a essere interdipendenti tra loro, il dominio spaziale e quello cyber sono interdipendenti con i tradizionali domini terrestre, aereo e navale, nell'ottica delle operazioni militari multi-dominio e dello sviluppo tecnologico verso nuove generazioni di sistemi d'arma necessariamente integrate con le dimensioni spaziali

[4] Esa, *Valuing the Benefits of ESA Aeolus Missions to European Decision Makers*, luglio 2022, https://space-economy.esa.int/article/136/valuing-the-benefits-of-esa-aeolus-missions-to-european-decision-makers.

[5] Si veda: Commissione europea, *GEODE (Factsheet)*, 15 giugno 2020, https://ec.europa.eu/commission/presscorner/detail/it/fs_20_1084; Sito Pesco: *EU Radio Navigation Solution (EURAS)*, https://www.pesco.europa.eu/project/eu-radio-navigation-solution-euras; Portale Funding & Tender Opportunities della Commissione europea: *Space and Ground-based NAVWAR Surveillance*, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2021-space-d-sgns.

[6] Intervista, 6 dicembre 2022.

[7] Decreto del Presidente del Consiglio dei Ministri 30 luglio 2020 n. 131, https://www.normattiva.it/uri-res/N2Ls?urn:nir:presidente.consiglio:decreto:2020;131; intervento di Gianluca Galasso al seminario IAI "La minaccia cyber allo spazio", 14 marzo 2023, https://www.iai.it/it/node/16684.

[8] Intervento di Carmine Masiello al seminario IAI "La minaccia cyber allo spazio", cit.

ISSN 2280-6164

e cyber[9]. Tale corrispondenza tra quarto e quinto dominio trova riscontro anche nella recente Strategia spaziale dell'Unione europea per la sicurezza e la difesa (*EU Space Strategy for Security and Defence*, Eusssd), che nella definizione del dominio spaziale fa rientrare ciascuna componente rilevante per il funzionamento di sistemi e servizi tra cui anche il cyber e i link di radio frequenza su cui viaggiano le informazioni[10].

La dimensione digitale che caratterizza il cyberspazio tanto quanto l'*outer space* li ha portati a formare una relazione ancora più stretta, di co-dipendenza, pur restando intrinsecamente diversi[11]. La pervasività del dominio cyber è infatti proprietà condivisa dai sistemi spaziali, in particolare i servizi forniti dai satelliti. Secondo la Strategia spaziale pubblicata dal Pentagono nel 2020, le capacità spaziali sono parte integrante della vita moderna, più o meno inconsapevolmente per gli utilizzatori finali, ma anche componente fondamentale del potere militare, al punto da essere alla base del "modo di vivere e del modo di fare la guerra"[12]. Inoltre, la *National Defense Strategy* del 2022 dichiara di prioritaria importanza gli investimenti volti ad aumentare la resilienza nei domini cyber e spazio, perché a supporto dell'intero strumento militare[13]. Considerata la tendenza verso la progressiva digitalizzazione dei sistemi spaziali e la rilevanza dei satelliti, anche per la conservazione dei dati, la pervasività dei due nuovi domini è destinata ad aumentare nel tempo[14].

Cyberspazio e *outer space* condividono alcune caratteristiche chiave[15]. Si tratta di domini in costante aggiornamento e rapido sviluppo, dove poter cercare un primo vantaggio competitivo in caso di conflitto, e in cui proliferano nuovi attori non statali. Gli attacchi condotti in questi domini sono di difficile attribuzione, e rischiano di portare alla escalation. Ciò è particolarmente vero nel campo cyber, dove la deterrenza *by denial* è strutturalmente molto difficile, e si tende piuttosto a un approccio di deterrenza *by punishment* o alla difesa attiva[16]. Rispetto ai domini

[9] Intervista, 13 dicembre 2022.

[10] Commissione europea, *Strategia spaziale dell'Unione europea per la sicurezza e la difesa* (JOIN/2023/9), 10 marzo 2023, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52023JC0009. Si veda anche il sito della Commissione europea: *EU Space Strategy for Security and Defence*, https://defence-industry-space.ec.europa.eu/node/437_en.

[11] Intervista, 6 dicembre 2022.

[12] Dipartimento della Difesa Usa, *Defense Space Strategy. Summary*, giugno 2020, p.3, https://www.defense.gov/News/Releases/Release/Article/2223539.

[13] Dipartimento della Difesa Usa, *2022 National Defense Strategy*, ottobre 2022, https://www.defense.gov/National-Defense-Strategy.

[14] Intervista, 13 dicembre 2022.

[15] Alessandro Marrone e Michele Nones, "Spazio e difesa: un legame crescente. Executive summary", in *Documenti IAI*, n. 22|02 (febbraio 2022), https://www.iai.it/it/node/14670; Alessandro Marrone e Michele Nones (a cura di), "The Expanding Nexus between Space and Defence", in *Documenti IAI*, n. 22|01 (febbraio 2022), https://www.iai.it/it/node/14669.

[16] Si veda al riguardo: Alessandro Marrone, Ester Sabatino e Ottavia Credi, "L'Italia e la difesa cibernetica", in *Documenti IAI*, n. 21|12 (settembre 2021), https://www.iai.it/it/node/14125. Mentre la deterrenza *by denial* mira a prevenire un'azione lasciando intendere al nemico che i costi di tale azione sarebbero superiori ai benefici che ne trarrebbe dato l'alto livello di difesa in campo, la deterrenza *by punishment* si attua tramite la minaccia di ritorsione con l'uso della forza nell'eventualità in cui

© 2023 IAI
ISSN 2280-6164
DOCUMENTI IAI 23 | 06 - MARZO 2023

tradizionali, sia nel cyberspazio che nell'*outer space* trovare un terreno comune a livello internazionale su norme di comportamento risulta quindi più complesso. Infine, si tratta dei domini meno conosciuti dagli stessi attori che vi operano, sia perché più nuovi degli altri sia per le loro caratteristiche strutturali di spazi non finiti[17].

Risulta quindi necessario approcciare *outer space* e cyberspazio con la consapevolezza della stretta relazione che vi intercorre, come asserito dal documento di postura strategica dello US Space Command, dove si ricerca con priorità l'integrazione e la sincronizzazione della dimensione cyber negli assetti spaziali[18]. Anche la Cina ha dimostrato di aver acquisito tale consapevolezza, con la creazione nel 2015 della Strategic Support Force (Ssf), che raccoglie e integra nelle operazioni militari le capacità in ambito cyber, spazio, *information operations*, *psychological warfare* e guerra elettronica (*electronic warfare*, Ew). L'approccio olistico di Pechino sembra in parziale controtendenza con quello occidentale di attuare il riconoscimento dello spazio in dominio operativo attraverso la creazione di strutture e comandi *ad hoc*, prettamente dedicati alle attività e operazioni orbitali, piuttosto che integrare lo spazio all'interno di comandi pre-esistenti e che comprendono più domini[19].

2. La natura della minaccia cyber al dominio spaziale

Con l'avvento delle capacità spaziali, non è trascorso molto tempo prima dello sviluppo speculare di capacità di *counterspace* più o meno sofisticate. In generale, si distingue tra minacce cinetiche e non, e la seconda tipologia comprende minacce cyber, elettroniche ed elettromagnetiche. A differenza della minaccia cinetica, manifestabile attraverso attacchi fisici all'infrastruttura di terra, diretti alla distruzione di un satellite colpito da armi terrestri oppure co-orbitali, la minaccia cyber è virtuale, volta primariamente alla sottrazione di dati, all'interruzione (reversibile o meno) dei servizi erogati, e alla manipolazione dei sistemi informatici e di controllo del sistema spaziale. In quanto digitale, la minaccia cyber si distingue dunque da quella cinetica per l'assenza di un attacco fisico, non necessitando ad esempio della distruzione – facilmente attribuibile – di un satellite con conseguente creazione di detriti in orbita. Questo porta gli esperti a considerare il cyberspazio

l'avversario intraprenda un'azione ostile.

[17] House of Commons Defence Committee, *Defence Space: Through Adversity to the Stars?*, 11 ottobre 2022, https://publications.parliament.uk/pa/cm5803/cmselect/cmdfence/182/report.html.

[18] James H. Dickinson, *Fiscal Year 2023 Priorities and Posture of United States Space Command. Presentation to the Senate Armed Services Committee*, 1 marzo 2022, p. 13-16, https://www.armed-services.senate.gov/imo/media/doc/USSPACECOM%20FY23%20Posture%20Statement%20SASC%20FINAL.pdf. Si veda anche James H. Dickinson, *Fiscal Year 2024 Priorities and Posture of United States Space Command. Presentation to the Senate Armed Services Committee*, 9 marzo 2023, https://www.armed-services.senate.gov/imo/media/doc/USSPACECOM%20Posture%20Statement%20-%20SASC%209%20Mar%202023.pdf.

[19] Alessandro Marrone e Michele Nones, "Spazio e difesa: un legame crescente", cit.

ISSN 2280-6164

come un ambiente in cui è più facile attaccare piuttosto che difendersi[20].

La diffusione di capacità di *counterspace* rende necessario incrementare la sicurezza del dominio spaziale, intesa nella doppia accezione anglosassone. È infatti importante distinguere tra *space safety*, che riguarda i rischi che possono derivare da circostanze ed eventi accidentali come detriti spaziali, tempeste solari e meteoriti, e *space security*, che concerne minacce intenzionali condotte da attori con fini malevoli. L'essere *secure* è quindi una condizione necessaria del dominio spaziale ai fini delle attività in orbita, istituzionali o commerciali che siano. Se si considera la componente cyber, appare evidente che le due accezioni di sicurezza si influenzano a vicenda, a detrimento finale di ciascuna componente: se i sistemi spaziali non sono *safe*, essi saranno più inclini a non essere *secure* – e viceversa[21]. Per di più, la stessa negligenza diffusa a livello istituzionale o aziendale, insieme a un'insufficiente cultura della sicurezza, contribuisce sostanzialmente al rischio di attacco cyber a sistemi spaziali[22].

Diversi esperti, inclusi quelli della Space Development Agency (Sda) della US Space Force, identificano gli attacchi cyber come la principale minaccia al dominio spaziale[23]. Per certi versi, questi attacchi potrebbero infatti rappresentare una forma silenziosa e virtuale di trasformazione dello spazio in un campo di battaglia[24]. Secondo l'Agenzia dell'Unione europea per la cibersicurezza (*European Union Agency for Cybersecurity*, Enisa), assetti e infrastrutture spaziali saranno tra i dieci target che, da oggi al 2030, si dimostreranno più sensibili a livello di cybersicurezza[25].

L'attacco cyber contro sistemi spaziali non è una nuova fattispecie, in particolare contro l'infrastruttura di terra, essendo in tutto simile ad attacchi classici contro altri tipi di sistemi e infrastrutture terrestri. Ad esempio, nel 2021 la National Aeronautics and Space Administration (Nasa) ha reso pubblico che il numero di attacchi subiti nel corso di quattro anni ammonta a 6,000[26]. Ciononostante, a livello globale è stato sinora reso pubblico un numero piuttosto contenuto di attacchi cyber condotti contro sistemi spaziali. Il valore relativamente basso di questo dato è riconducibile a diverse spiegazioni. In primo luogo, è importante puntualizzare

[20] Intervista, 9 febbraio 2023. Sui vantaggi strutturali dell'offesa sulla difesa nel cyberspazio si veda, tra gli altri: Alessandro Marrone, "I princìpi della cyber-defence", in *Airpress*, n. 127 (novembre 2021), p. 18-21.

[21] Intervista, 6 dicembre 2022.

[22] Ibid.

[23] Brian Weeden e Victoria Samson (a cura di), *Global Counterspace Capabilities. An Open Source Assessment*, Secure World Foundation, aprile 2022, p. 13-02, https://swfound.org/counterspace.

[24] Giancarlo La Rocca, "The Technology Dimension and Duality", in Alessandro Marrone e Michele Nones, "The Expanding Nexus between Space and Defence", cit., p. 83.

[25] Enisa, *Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride*, 11 novembre 2022, https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030.

[26] Nasa, "NASA's Cybersecurity Readiness", in *NASA OIG Reports*, n. IG-21-019 (18 maggio 2021), https://oig.nasa.gov/docs/IG-21-019.pdf; Brian Weeden e Victoria Samson (a cura di), *Global Counterspace Capabilities*, cit., p. 13-01.

ISSN 2280-6164

come lo sviluppo dei sistemi impiegabili in attività di *cyber war* rientra tra le materie protette da un alto livello di segretezza a livello nazionale[27]. In secondo luogo, per quanto concerne le realtà aziendali, spesso si pone un problema di possibile danno di immagine nel rendere noto un attacco cyber subìto[28]. Infine, è frequente che i Paesi stessi si astengano dal condividere informazioni con organizzazioni internazionali riguardo tentativi di attacchi cyber ai propri sistemi spaziali[29]. Ciò è dovuto anzitutto al timore di dimostrarsi vulnerabili a tale tipologia di minaccia, ma anche alla preoccupazione che tali informazioni trapelino ad attori terzi concorrenti o ostili[30]. Non disporre di dati completi riguardo la minaccia cyber ad assetti e infrastrutture spaziali, tuttavia, non fa che contribuire a una generale sottovalutazione della minaccia[31]. Si registra infatti una tendenza a trascurare la minaccia cyber a sistemi spaziali, concentrando gli sforzi principalmente sulle infrastrutture terrestri[32].

3. Attacchi cyber a sistemi spaziali

3.1 Vulnerabilità dei sistemi spaziali

L'interdipendenza tra dominio spaziale e cyber si traduce spesso in vulnerabilità poiché, in caso di anomalia o di incidente, rischia di innescarsi un effetto domino tale per cui un eventuale attacco cyber a un sistema spaziale si propaga fino a impattare il servizio stesso per cui il sistema spaziale viene impiegato[33].

Un sistema spaziale può essere attaccato su tre fronti: la catena di approvvigionamento (*supply chain*), l'infrastruttura di terra a supporto dei dispositivi in orbita (segmento di terra), e i satelliti stessi (segmento spaziale)[34]. È importante sottolineare come, generalmente, il segmento che viene colpito da un attacco cyber è quello che l'autore dell'attacco stesso ritiene più vulnerabile[35].

La *supply chain* dei sistemi spaziali è vulnerabile sul fronte dei software tanto quanto quello degli hardware, in particolare per quanto riguarda l'equipaggiamento e i prodotti provenienti da un mercato di massa non specializzato e *commercial-off-the-shelf* (Cots)[36]. Le cosiddette *corporate application*, vale a dire i diversi elementi

[27] Brian Weeden e Victoria Samson (a cura di), *Global Counterspace Capabilities*, cit., p. 13-02.
[28] Intervista, 1 dicembre 2022.
[29] Intervista, 2 dicembre 2022 a.
[30] Ibid.
[31] Ibid.; intervista, 9 febbraio 2023; intervento di Sergio Antonio Scalese al seminario IAI "La minaccia cyber allo spazio", cit.
[32] Brandon Bailey et al., *Defending Spacecraft in the Cyber Domain*, Center for Space Policy and Strategy, novembre 2019, p. 1 e 5, https://csps.aerospace.org/node/85; intervista, 1 dicembre 2022.
[33] Intervista, 1 dicembre 2022.
[34] Brian Weeden e Victoria Samson (a cura di), *Global Counterspace Capabilities*, cit., p. 13-01.
[35] Intervista, 9 febbraio 2023.
[36] Brandon Bailey et al., *Defending Spacecraft in the Cyber Domain*, cit., p. 7.

ISSN 2280-6164

che costituiscono la catena di approvvigionamento di un sistema spaziale, sono tra i target più a rischio di attacchi cyber[37]. Un attacco cyber ai danni della catena di approvvigionamento di un sistema spaziale può avvenire, ad esempio, tramite componenti elettroniche, materiali danneggiati o contraffatti, o l'installazione di codici informatici che permettono all'aggressore di prendere il controllo del sistema (le cosiddette *backdoor*)[38].

Il segmento di terra è forse la componente più vulnerabile ad attacchi cyber, alla portata anche di attori non statali. Ciò è dovuto a molteplici fattori, tra i quali l'ampiezza di servizi erogati a terra che coinvolgono stazioni di controllo, di *data relay* e anche dei terminali in possesso degli utenti, e dalla frequente completa assenza di misure di *cyber securisation*[39]. Il segmento di terra trasmette segnali *uplink* verso l'assetto in orbita e riceve segnali *downlink* che gestisce ed eventualmente distribuisce agli utenti, moltiplicando teoricamente i punti di accesso ed esponendo il sistema a più rischi e minacce[40]. Esso può essere minacciato sia a livello di network che di equipaggiamento[41]. Tipologie di attacchi cyber ai danni del segmento di terra comprendono, ad esempio, l'impiego di sistemi *unmanned*, l'interruzione o il malfunzionamento della connessione, o il sabotaggio fisico dell'infrastruttura stessa[42]. I terminali che si trovano in alcune infrastrutture di terra a supporto di sistemi spaziali sono spesso target di attacchi cyber. Infatti, pur rappresentando il punto di accesso degli assetti satellitari, spesso questi terminali non sono protetti da processi di autenticazione[43]. Altro target particolarmente vulnerabile del segmento di terra sono i trasponditori che emettono e ricevono segnali radio, così come i terminali che si trovano nelle infrastrutture di terra[44].

Il segmento spaziale, composto da prodotti e software progettati appositamente per questo dominio, comprende i sistemi in orbita e attiene al controllo stesso del satellite (*Telemetry, Tracking and Command*, Tt&c). Si tratta del segmento meno accessibile[45], anche perché nella maggior parte dei casi è completamente isolato dall'esterno. Esso ha limitati punti di accesso ed è basato su tecnologie più robuste con requisiti di sicurezza tendenzialmente più alti, a parziale deterrenza di un attacco. Quando è un satellite – o una sua componente – a essere attaccato, il target è spesso un elemento vulnerabile del software o dell'hardware[46]. Particolare

[37] Intervista, 7 dicembre 2022.
[38] Brian Weeden e Victoria Samson (a cura di), *Global Counterspace Capabilities*, cit., p. 13-03.
[39] Interviste, 2 dicembre 2022 a; 2 dicembre 2022 b; 6 dicembre 2022; 18 gennaio 2023.
[40] Intervista, 13 dicembre 2022.
[41] Intervista, 7 dicembre 2022.
[42] Brian Weeden e Victoria Samson (a cura di), *Global Counterspace Capabilities*, cit., p. 13-04.
[43] Beyza Unal, "Cybersecurity of NATO's Space-based Strategic Assets", in *Chatham House Research Papers*, luglio 2019, p. 8, https://www.chathamhouse.org/node/23173.
[44] Intervista, 6 dicembre 2022.
[45] Intervento di Danilo Figà al seminario IAI "La minaccia cyber allo spazio", cit.
[46] Brian Weeden e Victoria Samson (a cura di), *Global Counterspace Capabilities*, cit., p. 13-05.

© 2023 IAI
ISSN 2280-6164
DOCUMENTI IAI 23 | 06 - MARZO 2023

– ma non meno rilevante – è la minaccia co-orbitale, più legata tuttavia a sviluppi di tecnologie come le armi a energia diretta (*Directed Energy Weapons*, Dew), combinazioni di operazioni nello spettro elettromagnetico con attività cyber, o scenari di operazioni cinetiche e di spionaggio (*Electronic e Signal Intelligence*). Non è infatti trascurabile la possibilità di un attacco cyber indirizzato a un satellite con l'obiettivo di rendere il satellite stesso uno strumento impiegabile per un attacco cinetico nello spazio[47].

Secondo alcuni esperti, tra i target in orbita più a rischio vi sono le grandi costellazioni di satelliti: dal momento che sono prodotti in serie, un attacco a un satellite rischia di produrre un effetto domino e danneggiare tutti gli altri componenti della costellazione[48]. In altre parole, se tutti gli assetti orbitanti hanno lo stesso design, essi condivideranno la medesima vulnerabilità. Altri ritengono invece che se un singolo satellite di una grande costellazione viene colpito, l'effetto sia contenuto poiché l'attacco non comporta la perdita di segnale, vista l'alta ridondanza (*redundancy*) ottenuta grazie all'elevato numero di elementi in orbita[49]. Inoltre, prendendo ad esempio la piccola costellazione del programma Copernicus, si può evidenziare come i satelliti siano estremamente differenziati in base alle esigenze dei principali clienti (*customised*), con software a bordo diversi e i rispettivi codici e processori noti in teoria soltanto a coloro i quali li hanno progettati[50].

Più un sistema è connesso a un network aperto, più è vulnerabile ad attacchi cyber e, di conseguenza, necessitante di un'adeguata cybersicurezza[51] – fermo restando che la presenza o assenza di protezione cyber può fare la differenza. I sistemi più vulnerabili sono infatti quelli maggiormente supportati da Internet ed esposti a un network aperto, ed è per questo che la maggior parte dei satelliti è separata dalla rete[52]. In questo senso, tutti i sistemi collegati alla rete – inclusi quelli spaziali – sono vittime di una vulnerabilità intrinseca[53]. Particolarmente sensibile ad aggressioni cyber è la connessione tra stazioni di controllo terrestri e satelliti in orbita. Questo tipo di attacco avviene in genere tramite la tecnica cosiddetta *man-in-the-middle* (Mitm), per cui, l'aggressore intercetta e/o compromette i dati nel lasso di tempo in cui passano dal mittente al destinatario[54].

Talvolta si commette l'errore di pensare sia sufficiente applicare misure di cybersicurezza soltanto ai segmenti classificati dei programmi spaziali[55]. È invece

[47] Intervista, 9 febbraio 2023.
[48] Intervista, 6 dicembre 2022.
[49] Interviste, 7 dicembre 2022; 23 marzo 2023.
[50] Intervista, 2 dicembre 2022 b.
[51] Intervista, 6 dicembre 2022.
[52] Intervista, 2 dicembre 2022 b.
[53] Intervista, 9 febbraio 2023.
[54] Brian Weeden e Victoria Samson (a cura di), *Global Counterspace Capabilities*, cit., p. 13-04.
[55] Intervista, 23 marzo 2023.

© 2023 IAI
ISSN 2280-6164
DOCUMENTI IAI 23 | 06 - MARZO 2023

necessario proteggerli nella loro interezza, soprattutto perché è più probabile che subiscano attacchi cyber mirati ai loro segmenti non classificati i quali, se colpiti, possono dare origine a conseguenze molto serie.

Come noto, il settore militare è sempre più dipendente dai servizi garantiti dai sistemi in orbita[56]. Le Forze Armate di qualsiasi Paese militarmente avanzato richiedono costante comunicazione, connessione, e accesso a grandi quantità di informazioni per la pianificazione e condotta delle operazioni, ma anche per la postura di deterrenza e difesa nazionale e Nato nonché per le regolari attività di addestramento o di esercitazione, e in generale per il funzionamento dello strumento militare – specie se interforze e interoperabile nel quadro Nato o Ue[57]. Poiché i segnali dei satelliti militari sono più protetti e resilienti, così come i satelliti stessi sono più robusti e difficili da penetrare, le maggiori vulnerabilità di tipo cyber dei sistemi spaziali utilizzati dalla Difesa andrebbero rintracciate nelle catene di approvvigionamento e, in particolare, nella presenza di *backdoor* nel sistema di criptaggio, che permettono a un possibile aggressore di aggirare il sistema prendendone il controllo[58]. Ciò è particolarmente rilevante in caso di assetti obsoleti, vale a dire in orbita da più di dieci anni, che hanno oltrepassato il loro limite di vita operativa previsto in fase di design.

3.2 Tipologie e conseguenze di attacchi cyber

L'azione cyber si traduce in attività molto diverse, che variano dallo spionaggio alla manipolazione di dati e sistemi[59]. Tra le tipologie principali di attacco vi sono l'intercettazione e la corruzione di dati e il sequestro illegittimo del controllo di un sistema[60]. Indipendentemente dalla tecnica utilizzata per condurlo, un attacco cyber necessita di quattro elementi per poter essere mosso: accesso, vulnerabilità, una struttura di comando e controllo (C2), e l'introduzione forzata di dati (cosiddetti "bug") in un software[61]. Gli attacchi cyber, siano essi mirati a colpire un sistema spaziale o terrestre, prevedono infatti generalmente l'introduzione forzata di dati in un software, danneggiandolo[62]. In questo modo, i sistemi possono essere sfruttati, ad esempio, per eseguire azioni e codici o ottenere accessi non autorizzati, o addirittura mandare in crash i sistemi stessi[63]. L'immissione di dati incorretti può inoltre generare azioni letali sul sistema, quale lo spostamento o la modifica dell'orbita satellitare. Il modo in cui un aggressore colpisce un sistema spaziale tramite un attacco cyber dipende ovviamente non solo dalle sue capacità, ma anche

[56] Beyza Unal, "Cybersecurity of NATO's Space-based Strategic Assets", cit., p. 9.
[57] Intervista, 6 dicembre 2022.
[58] Beyza Unal, "Cybersecurity of NATO's Space-based Strategic Assets", cit., p. 7.
[59] Brian Weeden e Victoria Samson (a cura di), *Global Counterspace Capabilities*, cit., p. 13-09.
[60] Todd Harrison et al., "Space Threat Assessment 2020", in *CSIS Reports*, marzo 2022, p. 7, https://www.csis.org/analysis/space-threat-assessment-2020.
[61] Brian Weeden e Victoria Samson (a cura di), *Global Counterspace Capabilities*, cit., p. 13-01.
[62] Ibid.
[63] Intervista, 13 dicembre 2022.

ISSN 2280-6164

dai suoi obiettivi[64]. La magnitudine della minaccia cyber è infatti proporzionata alle conseguenze che essa può avere sui sistemi spaziali. Tra quelle più severe vi sono la disattivazione dell'equipaggiamento di un satellite, l'interruzione delle comunicazioni che arrivano al e partono dal satellite, e la possibilità che un avversario prenda il controllo di un satellite carpendone il sistema C2[65]. Nei casi più estremi, un attacco può tradursi nella distruzione di satelliti o di loro componenti[66].

Se si considera il Programma spaziale europeo, ad esempio, un attacco contro Copernicus potrebbe risultare nell'invio di messaggi errati o mancanti dei dati di Osservazione della Terra. Un'aggressione cyber a Galileo potrebbe causare errori fino alla perdita di segnale e l'interruzione di servizi terrestri quali la distribuzione di energia, con danni gravissimi. Un attacco al sistema di comunicazione satellitare per scopi governativi (*Governmental Satellite Communication*, GovSatCom) potrebbe infine provocare la perdita di comunicazioni sicure – un fenomeno particolarmente grave per gli stati, soprattutto per le conseguenze sulle operazioni militari[67].

3.3 Una minaccia in evoluzione

Negli ultimi 20 anni si è assistito a una graduale evoluzione della minaccia, in termini di soggetti coinvolti, trend e capacità[68]. Tra gli sviluppi più rilevanti si segnala come attacchi cyber contro sistemi spaziali siano ormai alla portata anche di attori non statali quali individui e organizzazioni criminali e terroristiche, hacker, attivisti[69].

Il rischio è che la minaccia cyber ai danni di sistemi spaziali aumenti con l'utilizzo di satelliti commerciali o di ricerca, potenzialmente caratterizzati da un basso livello di cybersicurezza, evidenziando alcune questioni attinenti al fenomeno del *new space*[70]. Infatti, nonostante la necessità di una solida pianificazione dell'attacco, che rimane complesso e sofisticato soprattutto se scagliato contro sistemi altamente *customised*, la minaccia cyber ha una bassa barriera d'accesso e può essere portata avanti anche da attori non istituzionali.

Tra i motivi per cui alcuni esperti ritengono che la minaccia cyber al dominio spaziale è destinata ad aumentare vi è anche la difficoltà di attribuzione di un attacco cyber. Si tratta di un processo complicato e talvolta fallimentare anche

[64] Brandon Bailey et al., *Defending Spacecraft in the Cyber Domain*, cit., p. 4.
[65] Todd Harrison et al., "Space Threat Assessment 2020", cit., p. 5; intervista, 7 dicembre 2022.
[66] Brian Weeden e Victoria Samson (a cura di), *Global Counterspace Capabilities*, cit., p. 13-01.
[67] Intervista, 2 dicembre 2022 b.
[68] Ibid.
[69] Brian Weeden e Victoria Samson (a cura di), *Global Counterspace Capabilities*, cit., p. 13-01; Brandon Bailey et al., *Defending Spacecraft in the Cyber Domain*, cit., p. 1.
[70] Intervista, 2 dicembre 2022 a; Brandon Bailey et al., *Defending Spacecraft in the Cyber Domain*, cit., p. 8.

ISSN 2280-6164

nel dominio spaziale in quanto azione giuridicamente vincolata e che spesso non conduce a un reale riconoscimento di responsabilità[71]. Questo implica tra l'altro un elevato rischio di errata assegnazione della colpa di un'aggressione e, di conseguenza, il pericolo di *escalation*[72]. Allo stesso tempo, ciò comporta una notevole difficoltà nell'erogazione di sanzioni o altre soluzioni diplomatiche contro il vero aggressore[73]. Non da ultimo, la difficoltà di attribuzione rende più difficile la deterrenza *by punishment*, perché l'autore dell'attacco può sperare di passare inosservato ed evitare quindi la rappresaglia nel dominio cyber o in altri domini.

Ulteriore spiegazione del probabile aumento della minaccia cyber ad assetti spaziali è da trovarsi nella relativa convenienza di un tale attacco se confrontato con attacchi cinetici convenzionali, i quali risultano distruttivi con effetti negativi distribuiti su tutti gli attori – detriti (*debris*) *in primis* – e sono facilmente attribuibili. Tale caratteristica convenienza si applica a stati così come ad attori non statali, con il rischio crescente che individui o gruppi criminali o terroristici sviluppino conoscenze sufficientemente avanzate a condurre un attacco cyber ai danni di un sistema spaziale.

4. Minaccia elettronica e elettromagnetica

Mentre gli attacchi cyber colpiscono, tramite metodi digitali, il software di un sistema – ovvero il sistema informatico che trasmette dati, e il dato stesso – gli attacchi elettronici ed elettromagnetici mirano rispettivamente all'hardware di un sistema e ai segnali a radiofrequenza (Rf) dello stesso, facendo parte dal punto di vista dottrinale della dimensione spaziale e di *information warfare* piuttosto che di quella cyber[74].

La guerra elettronica consiste nella conduzione di attività nello spettro elettromagnetico in ambito di operazioni militari. Si tratta di attività pianificate, programmate e dirette verso un obiettivo specifico[75]. In un contesto civile o governativo, invece, simili attività sono più generalmente note come interferenze[76]. La minaccia elettromagnetica è considerata oggi tra le più probabili per i sistemi spaziali, indipendentemente dalla protezione e resilienza di un satellite e con bassissime barriere di accesso per arrecare un danno, anche attraverso strumentazione poco sofisticata ed economica[77].

[71] Intervista, 9 febbraio 2023.
[72] Brian Weeden e Victoria Samson (a cura di), *Global Counterspace Capabilities*, cit., p. 13-09.
[73] Intervista, 1 dicembre 2022.
[74] Beyza Unal, "Cybersecurity of NATO's Space-based Strategic Assets", cit., p. 5; interviste, 6 dicembre 2022; 13 dicembre 2022.
[75] Intervista, 1 dicembre 2022.
[76] Ibid.
[77] Ibid.; intervista, 13 dicembre 2022.

ISSN 2280-6164

Le tecniche di Ew comprendono, tra le altre, la *deception*, ovvero l'utilizzo di metodi ingannevoli per circuire e deviare l'attività dell'avversario. Ulteriore tipologia di attacco è il *jamming*, ovvero il disturbo delle comunicazioni che avvengono tramite segnale radio. Lo *spoofing* consiste invece nell'attacco a sensori e/o ricevitori che risulta nella falsificazione di informazioni – una tecnica che può avere gravi conseguenze per gli utenti e la società nel suo complesso in caso di attacco ai sistemi di Gnss ed è relativamente facile da attuare[78].

Come per gli attacchi cyber, aggressioni tramite interferenze elettromagnetiche presentano difficoltà *in primis* di identificazione e poi di attribuzione. In un primo momento, l'operatore di un satellite può avere difficoltà nel riconoscere la tipologia di attacco a un assetto spaziale, ed è possibile che sospetti di un malfunzionamento del satellite dovuto, ad esempio, a *jamming*, prima di ipotizzare che si tratti di un attacco cyber[79]. Vale tuttavia la pena sottolineare come un attacco elettronico o elettromagnetico non escluda uno di tipo cyber, dal momento che questi attacchi possono avvenire contemporaneamente[80].

Secondo alcuni esperti in uno scenario futuro la componente elettronica ed elettromagnetica andrà a convergere con quella cyber, con malware che agiranno in simbiosi e complementarietà con sistemi di Ew[81]. La combinazione di queste operazioni, abbinata allo sviluppo di nuove tecnologie quali ad esempio Dew con rilevanti applicazioni nell'ambiente orbitale (*space-on-space*), potrà risultare in effetti considerevoli nella competizione spaziale. Aumentando progressivamente, e dovutamente, il livello di cyber sicurezza dei sistemi, e/o in presenza di network chiusi meno vulnerabili, l'attaccante potrebbe ricercare una convergenza tecnologica tra attività nello spettro elettromagnetico e nel dominio cyber. In un certo senso, un canale di accesso wireless per operazioni cyber diventa lo spettro elettromagnetico e in particolare i segnali Rf, abilitanti della minaccia e della capacità cyber stessa[82].

L'adattamento della tecnologia di Ew verso questi scenari e l'integrazione di capacità convergenti e complementari è parte di un processo evolutivo in corso negli Stati Uniti[83]. Sia per l'Esercito che per la Marina statunitense, l'integrazione

[78] University of Texas at Austin, "UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea", in *UT News*, 29 luglio 2012, https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea.

[79] Intervista, 7 dicembre 2022.

[80] Ibid.; intervista, 9 febbraio 2023.

[81] Intervista, 18 gennaio 2023. Si veda, a questo proposito, la sezione 5.

[82] Mark Pomerleau, "Services Working to Convergence EW, Cyber Warfare Capabilities", in *DefenseScoop*, 30 settembre 2022, https://defensescoop.com/?p=60993.

[83] Mark Pomerleau, "US Military to Blend Electronic Warfare with Cyber Capabilities", in *C4ISRNET Daily Briefs*, 14 aprile 2021, https://www.c4isrnet.com/electronic-warfare/2021/04/14/us-military-to-blend-electronic-warfare-with-cyber-capabilities; Sydney J. Freedberg Jr., "Russian Robots: Fear Jammers, Not Terminators", in *Breaking Defense*, 5 ottobre 2017, https://breakingdefense.com/?p=39684; Catherine A. Theohary e John R. Hoehn, "Convergence of Cyberspace Operations and Electronic Warfare", in *CRS In Focus*, 13 agosto 2019, https://sgp.fas.org/crs/natsec/IF11292.pdf.

ISSN 2280-6164

delle capacità attraverso *jammer* di nuova generazione si accompagna a strategie di impiego operativo congiunto di azioni cyber e di Ew. Da parte sua, la Russia ha dimostrato capacità di questo tipo, anche in ottica di *information* e *psychological warfare*, applicate in particolare al sistema di Ew "Leer-3" basato sull'utilizzo di droni in grado di bloccare le comunicazioni in porzioni di territorio e di inviare false informazioni[84]. L'applicazione di tale convergenza tra cyber e Ew potenzialmente rappresenta una evoluzione della minaccia anche contro i sistemi spaziali[85].

5. Il caso ucraino

Il conflitto attualmente in corso in Ucraina dimostra il legame che unisce il dominio spaziale e quello cyber[86]. Negli anni, la Russia ha provato di essere in grado di condurre attacchi cyber di varia natura[87]. Le capacità tecnologiche di Mosca rappresentano infatti un pericolo non trascurabile per i Paesi membri dell'Alleanza atlantica[88]. La Russia sta dando prova delle proprie potenzialità cyber ed elettromagnetiche anche durante l'attuale conflitto in Ucraina: negli ultimi dieci mesi si sono registrati attacchi (riusciti, falliti o sventati) tramite *jamming* del segnale elaborato dal sistema di posizionamento globale (*Global Positioning System*, Gps) utilizzato da sistemi a pilotaggio remoto, *Distributed Denial of Service* (DDoS) ai danni di dispositivi radio e telefonici, e furto di dati militari criptati[89].

L'aggressione russa all'Ucraina ha reso ancora più evidente le vulnerabilità dei sistemi spaziali agli attacchi cyber[90]. Per certi versi, i primi colpi sparati prima ancora dell'alba del giorno dell'invasione del territorio ucraino sono stati virtuali e digitali. Ciò è avvenuto attraverso una combinazione di attacchi cyber all'infrastruttura network del fornitore di servizi satellitari KA-Sat (di proprietà dei colossi satellitari Viasat ed Eutelsat) e interferenze elettromagnetiche ai segnali di navigazione satellitare lungo il confine fino alla capitale Kyiv, con disturbi registrati dal Mar Nero al Baltico in direzione di Kaliningrad e ripercussioni anche sull'aviazione civile. I responsabili dell'attacco hanno sfruttato una vulnerabilità del sistema nota dal 2019, ma alla quale non si era provveduto con appositi miglioramenti in termini di cybersicurezza, con l'ultimo aggiornamento del sistema risalente al 2017. Ciò ha

[84] Mark Pomerleau, "US Military to Blend Electronic Warfare with Cyber Capabilities", cit.; Dylan Malyasov, "In Syria Spotted New Russian RB-341V 'Leer-3' Electronic Warfare System", in *Defence Blog*, 14 marzo 2016, https://defence-blog.com/in-syria-spotted-new-russian-rb-341v-leer-3-electronic-warfare-system.

[85] Catherine A. Theohary e John R. Hoehn, "Convergence of Cyberspace Operations and Electronic Warfare", cit.

[86] Intervento di Adolfo Urso al convegno "Una legge italiana per lo spazio", 16 dicembre 2022, https://webtv.camera.it/evento/21475.

[87] Brian Weeden e Victoria Samson (a cura di), *Global Counterspace Capabilities*, cit., p. 13-07.

[88] Beyza Unal, "Cybersecurity of NATO's Space-based Strategic Assets", cit., p. 6.

[89] Ibid., p. 6-7.

[90] Intervista, 2 dicembre 2022 b.

ISSN 2280-6164

quindi contribuito a creare un'opportunità di attacco[91]. Da un punto di vista militare questo attacco ha un grande valore simbolico, in quanto primo attacco (noto) a strutture necessarie per operazioni militari[92]. Pur essendo parte di una più larga operazione militare, l'attribuzione dell'attacco non è stata più immediata o facile, considerando che sono stati necessari 35 giorni per il gestore del network a dare evidenza pubblica dell'accaduto e 75 giorni per lo stato per accusare formalmente la Russia[93].

Il dominio spaziale e quello cyber hanno dunque aperto il primo fronte della guerra, considerato essenziale per ottenere alcuni vantaggi competitivi sull'avversario. In particolare, l'attacco a KA-Sat ha raggiunto l'obiettivo di interrompere i servizi e disabilitare i modem che permettono la connessione e comunicazione delle forze militari ucraine, creando così problemi al C2 della difesa nazionale, ma anche ripercussioni su alcune infrastrutture energetiche e di connettività ucraine ed europee[94].

In seguito all'attacco a KA-Sat, il vice primo ministro ucraino Mychajlo Fedorov ha chiesto supporto agli attori commerciali internazionali in grado di fornire una soluzione tempestiva alla *disruption* in corso. A dare seguito alla richiesta è stata SpaceX che, in 48 ore – complice l'avvio di negoziati precedenti al conflitto e l'appoggio delle istituzioni americane – ha completato la prima spedizione di terminali per connettere gli ucraini alla costellazione in orbita bassa Starlink. Una risposta rapida che è stata anch'essa colpita da tentati attacchi cyber russi volti a disabilitare i servizi, a cui sono seguiti sforzi e investimenti da parte di SpaceX per incrementare la difesa cyber degli assetti spaziali. Il coinvolgimento diretto nel conflitto della società privata statunitense ha suscitato notevole interesse, anche per via della popolarità dell'azienda stessa. Da notare le reazioni anche da parte cinese e russa, in particolare per quanto riguarda la possibilità di considerare gli assetti privati commerciali come obiettivi legittimi per ritorsioni russe rispetto al loro coinvolgimento nella guerra in Ucraina[95].

Attacchi sono stati registrati anche contro il sistema Delta sviluppato dagli stessi ucraini, nello specifico dal Defense Technology Innovation and Development Center del Ministero della Difesa di Kyiv. Il software militare Delta ha rappresentato

[91] Intervento di Sergio Antonio Scalese al seminario IAI "La minaccia cyber allo spazio", cit.

[92] Ibid.

[93] Katrina Manson, "The Satellite Hack Everyone Is Finally Talking About", in *Bloomberg*, 1 marzo 2023, https://www.bloomberg.com/features/2023-russia-viasat-hack-ukraine.

[94] Sul caso KA-Sat, si veda: Viasat, *KA-Sat Network Cyber Attack Overview*, 30 marzo 2022, https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview; Raphael Satter, "Satellite Outage Caused 'Huge Loss in Communications' at War's Outset- Ukrainian Official", in *Reuters*, 15 marzo 2022, https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15.

[95] "Russia Warns West: We Can Target Your Commercial Sites", in *Reuters*, 27 ottobre 2022, https://www.reuters.com/world/russia-says-wests-commercial-satellites-could-be-targets-2022-10-27; Zhanna L. Malekos Smith, "A New 'Bumper Sticker' for Space Satellites", in *CSIS Commentaries*, 22 agosto 2022, https://www.csis.org/node/66645.

ISSN 2280-6164

un modo efficace per ristabilire il comando e controllo lì dove necessario e per potenziare la *situational awareness* sul campo, tanto da essere stato approvato per l'utilizzo nelle forze armate del paese[96]. Delta utilizza anche dati e immagini satellitari e ha subito tentativi di intrusioni cyber da parte russa, costringendo gli sviluppatori e le istituzioni coinvolte a prendere parziali contromisure di sicurezza quali ad esempio porre il sistema in cloud esterni all'Ucraina[97].

Per quanto reversibili, gli attacchi cyber condotti in Ucraina hanno avuto largo riscontro in termini di effetti concreti, con decine di migliaia di modem disabilitati e attività di disturbo del segnale. Nonostante la risposta di Starlink, in molti casi recuperare le funzionalità operative è un'attività che può richiedere settimane e investimenti mirati. Per questo motivo, già da marzo 2022 negli Stati Uniti la Cybersecurity and Infrastructure Security Agency (Cisa) e il Federal Bureau of Investigation (Fbi) hanno incoraggiato i fornitori statunitensi di servizi satellitari ad aumentare le azioni di mitigazione dei rischi[98]. Ad un anno di distanza dall'avvio della guerra e dall'attacco, Viasat ha annunciato di aver sviluppato in collaborazione con i servizi di intelligence contromisure di cybersicurezza applicate a tutto il suo network globale, adottando un approccio "*zero trust*" incentrato su un *intrusion detection tool* in grado di rilevare con più efficacia ogni potenziale accesso e attacco[99].

6. Contesti internazionali: Ue e Nato

6.1 Unione europea

A livello comunitario la Commissione, in particolare tramite la Direzione generale Industria della difesa e spazio (*Directorate-General for Defence Industry and Space*, Dg Defis), sta mettendo a disposizione ingenti fondi per il finanziamento di progetti che riguardano la cybersicurezza e cyber-resilienza dei sistemi spaziali, nel contesto dell'Edf. Anche l'Agenzia europea per la difesa (*European Defence Agency*, Eda) ricopre un ruolo importante nell'offrire un forum ove la comunità spaziale e quella cyber possono relazionarsi e nell'identificare, insieme alle altre istituzioni europee competenti, le necessità più stringenti dell'Unione riguardo il proprio programma spaziale[100].

[96] Ministero della Difesa ucraino, *Government Approves Decision to Introduce Delta System in the Defense Forces*, 4 febbraio 2023, https://www.kmu.gov.ua/en/news/uriad-ukhvalyv-rishennia-shchodo-zaprovadzhennia-systemy-delta-v-sylakh-oborony.

[97] Ukrainian Military Center, *The Defense Forces of Ukraine to Introduce the Delta System*, 4 febbraio 2023, https://mil.in.ua/?p=189105.

[98] Cisa e Fbi, *Strengthening Cybersecurity of SATCOM Network Providers and Customers*, 17 marzo 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-076a.

[99] Sandra Erwin, "Viasat Deploying 'Zero Trust' Cybersecurity across Global Network", in *SpaceNews*, 14 marzo 2023, https://wp.me/p5sx4f-Cc1.

[100] Intervista, 6 dicembre 2022.

ISSN 2280-6164

Con la Decisione 698 del 2021[101] si registra un tentativo di rafforzare la posizione europea nel dominio operativo e come potenza spaziale mondiale, anche attraverso il riconoscimento della necessità di proteggere ciascun componente del Programma spaziale europeo[102]. La responsabilità della protezione del Programma risiede in capo al Consiglio dell'Ue e all'Alto Rappresentante/Vice Presidente della Commissione. Il mandato operativo è assegnato all'Agenzia dell'Unione europea per il programma spaziale (*EU Agency for the Space Programme*, Euspa), nata nel 2021 dall'evoluzione della *European Gnss Agency* (Gsa), e che vede la sicurezza del Programma come uno dei suoi *core task*. Insieme agli stati membri e tramite un *Security Accreditation Board* (Sab) indipendente, Euspa è responsabile della definizione e attuazione dei requisiti di sicurezza dei sistemi spaziali, fin dalla fase di design di un satellite. In aggiunta, l'Agenzia è responsabile del Galileo Security Monitoring Centre (Gsmc), in transizione verso un più ampio ruolo di *Security Operations and Monitoring Centre* (Som) con capacità rilevanti anche nel campo della cybersicurezza e prima linea di attivazione della catena di C2 prevista dalla Decisione 698[103].

Nel novembre 2022 il Parlamento europeo ha approvato la direttiva *Network and Information Security 2* (Nis2), che sostituisce la precedente Nis1[104]. Oltre ad alzare il livello di cybersicurezza per gli enti che si occupano di sicurezza di dati, la nuova direttiva riconosce lo spazio come infrastruttura critica e sancisce le attività di segnalazione di incidenti per effettuare opportuni resoconti di anomalie riscontrate nei sistemi.

Le direttive Nis1 e Nis2 rappresentano dei punti di riferimento anche nella definizione di standard di cybersicurezza comuni a tutti gli stati membri, per il settore spaziale e non solo. Nell'assicurare elevati standard di cybersicurezza l'Ue deve tuttavia prestare particolare attenzione affinché non vi siano conseguenze sui livelli di efficienza dei propri sistemi spaziali[105]. Al tempo stesso è necessario effettuare un'adeguata certificazione dei sistemi, ad esempio tramite *penetration test* o tecniche di *stressing*, al fine di verificarne la resilienza[106].

[101] Consiglio dell'Unione europea, *Decisione (PESC) 2021/698 del 30 aprile 2021 sulla sicurezza dei sistemi e servizi dispiegati, in funzione e usati nell'ambito del programma spaziale dell'Unione che possono incidere sulla sicurezza dell'Unione...*, http://data.europa.eu/eli/dec/2021/698/oj.

[102] Alessandro Marrone e Michele Nones, "Spazio e difesa: un legame crescente", cit., p. 11-12.

[103] Consiglio dell'Unione europea, *Decisione (PESC) 2021/698 del 30 aprile 2021*, cit.; intervista, 2 dicembre 2022 b.

[104] Parlamento europeo e Consiglio dell'Unione europea, *Direttiva (UE) 2022/2555 del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione...* (direttiva NIS 2), http://data.europa.eu/eli/dir/2022/2555/oj. Si veda anche il sito di Cyber Risk GmbH: *The NIS 2 Directive*, https://www.nis-2-directive.com; e il sito Enisa: *NIS Directive*, https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new.

[105] Intervista, 6 dicembre 2022.

[106] Interviste, 1 dicembre 2022; 2 dicembre 2022 b.

DOCUMENTI IAI 23 | 06 - MARZO 2023 ISSN 2280-6164

Un ulteriore sviluppo rilevante è avvenuto a novembre 2022 con la presentazione, da parte della Commissione e dell'Alto Rappresentante Josep Borrell, della comunicazione "La politica di ciberdifesa dell'Ue"[107]. Il documento sottolinea il labile confine tra dimensione civile e militare del dominio cyber, menzionando anche gli attacchi contro assetti spaziali, ed evidenzia la necessità di un maggior coordinamento tra le comunità di attori coinvolti, e all'interno di ognuna di esse, vista anche la frammentazione di strumenti e piattaforme esistente oggi. Tra gli obiettivi della comunicazione vi è anche quello di aumentare la protezione delle infrastrutture critiche, ivi incluso lo spazio, con lo sviluppo di scenari e valutazione di rischio. Il documento riconosce inoltre la criticità dei servizi spaziali e la gravità dell'attacco contro il network KA-Sat – esempio di minaccia portata a detrimento della disponibilità e continuità dei servizi satellitari. Attenzione è posta infine sull'intenzione di attuare a livello europeo un investimento tale da permettere all'Ue di ottenere un presidio tecnologico e, di conseguenza, raggiungere un più alto livello di autonomia nel settore.

6.1.1 Una nuova Strategia spaziale

La comunicazione richiama l'importanza della Strategia spaziale dell'Ue per la sicurezza e la difesa (Eusssd), già prevista nella Bussola strategica adottata dagli stati membri Ue a marzo 2022, pensata per indicare le azioni necessarie per aumentare la resilienza e sicurezza dei sistemi spaziali e individuare anche le misure per dissuadere e rispondere alle minacce, tra cui quella cyber[108].

La negoziazione e definizione della Strategia spaziale Ue è stata affidata al Servizio europeo per l'azione esterna (Seae), ed è stata pubblicata durante la presidenza svedese del Consiglio dell'Ue[109]. Il documento rappresenta un *unicum* nel quadro spaziale europeo ed è basato sull'ambizioso obiettivo di affrontare in modo olistico l'*outer space*, inclusi rischi e minacce associate, così come la resilienza dei sistemi coinvolti – sia europei che nazionali – e le capacità spaziali necessarie a supporto della sicurezza e difesa comune. Fondamentale nella nuova strategia è il concetto di resilienza[110].

Il documento era particolarmente atteso per la sua rilevanza nel prossimo futuro del programma spaziale dell'Ue, considerando ad esempio la protezione di Galileo, pronto a un'evoluzione verso la seconda generazione di satelliti e l'avvio del Prs entro la fine del 2023, nonché l'espansione del programma Copernicus e l'annuncio di un nuovo componente del programma spaziale europeo: un sistema

[107] Commissione europea e Servizio europeo per l'azione esterna, *La politica di ciberdifesa dell'UE* (JOIN/2022/49), 10 novembre 2022, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52022JC0049.

[108] Per maggiori informazioni sulla Bussola strategica, si veda il sito della Cyber Risk GmbH: *The Strategic Compass of the European Union*, https://www.strategic-compass-european-union.com.

[109] Intervista, 2 dicembre 2022 a.

[110] Intervista, 1 dicembre 2022; Commissione europea, *Strategia spaziale dell'Unione europea per la sicurezza e la difesa*, cit.

ISSN 2280-6164

di connessione e comunicazioni sicure denominato *Infrastructure for Resilience, Interconnectivity and Security by Satellite* (Iris²) recentemente adottato dal Parlamento europeo[111].

La Strategia anticipa una legge spaziale Ue, con requisiti significativi per ciò che riguarda il principio del "*secure by design*" che assicuri elevati standard di sicurezza già dalle prime fasi dello sviluppo di un satellite[112]. In particolare, la Strategia riconosce la specifica vulnerabilità delle infrastrutture spaziali ad attacchi cyber, sia per quanto riguarda sistemi in orbita che a terra. In aggiunta, la Commissione prevede la necessità di aumentare la consapevolezza delle minacce e di facilitare lo scambio di *best practices* su misure di resilienza pertinenti anche il dominio cyber. Per questo motivo la Strategia annuncia la creazione di un centro di condivisione e analisi delle informazioni europeo (*Information Sharing and Analysis Centre*, Isac). Peraltro, la diffusione di requisiti, standard e procedure di cybersicurezza è prevista sia come parte della futura legge spaziale europea, sia come implementazione della direttiva Nis2 e del prossimo *Cyber Resilience Act*. Quest'ultimo è in fase di negoziazione ed è stato proposto per definire dei requisiti orizzontali applicabili a prodotti digitali parte della *supply chain* spaziale.

La strategia prevede inoltre la possibilità di attivare l'Articolo 42.7 e la clausola di assistenza reciproca qualora una minaccia o un incidente spaziale arrivino a equivalere a un attacco armato. Nel complesso la Eusssd rafforza l'architettura di sicurezza spaziale europea con un chiaro consolidamento del perimetro d'azione di Euspa, agenzia fondata appositamente sul *core task* della sicurezza per facilitare una rivoluzione copernicana europea in materia. L'Agenzia basata a Praga è infatti il fulcro tecnico e operativo della *Space Threat Response Architecture* (Stra) prevista dalla Decisione 2021/698, ed è identificata come principale attore per quanto riguarda il monitoraggio e le operazioni di sicurezza spaziale dell'Unione.

Nella nuova Strategia sono presenti inoltre riferimenti a training ed esercitazioni comuni, importanti per garantire una conoscenza condivisa in ambito europeo delle minacce cui sono soggetti assetti e infrastrutture spaziali[113]. A ridosso della sua pubblicazione l'Ue ha condotto l'esercitazione Stra 2023, svoltasi per testare il meccanismo di risposta europeo in caso di una anomalia cyber in un satellite Galileo[114]. L'esercitazione dunque ha testato le componenti della risposta, coinvolgendo tutti gli attori istituzionali rilevanti e anche l'Italia in qualità di nazione ospitante il Centro di controllo di Galileo presso il centro spaziale nel Fucino. Scenari testati in tempo reale anche nel corso dell'esercitazione spaziale

[111] Commissione europea, *Adoption by the European Parliament of IRIS², Europe's New Infrastructure for Resilience, Interconnection & Security by Satellites*, 14 febbraio 2023, https://defence-industry-space.ec.europa.eu/node/433_en.

[112] Sul concetto di *secure-by-design* si veda, tra gli altri: Alessandro Marrone, Ester Sabatino e Ottavia Credi, "L'Italia e la difesa cibernetica", cit.

[113] Intervista, 1 dicembre 2022.

[114] Seae, *Space: EU Tests Its Response Mechanism to Threats*, 15 marzo 2023, https://www.eeas.europa.eu/node/427136.

ISSN 2280-6164

AsterX 2023 promossa dalla Francia, integrata in una più ampia esercitazione militare multi-dominio Orion 23 e che ha sviluppato risposte specifiche anche a scenari di minaccia cyber contro sistemi spaziali[115]. Il Comando delle Operazioni Spaziali (Cos) italiano ha preso parte insieme a Belgio, Germania e Stati Uniti all'esercitazione testando "le procedure operative per la condotta di operazioni spaziali atte a contrastare un'ampia gamma di minacce" inclusa quella cyber e fornendo "supporto con numerosi prodotti e servizi spaziali"[116].

6.2 Nato

Mentre l'Ue ha anche propri assetti in orbita, non avviene lo stesso per la Nato, che conta esclusivamente sui sistemi spaziali degli Alleati. L'Alleanza possiede alcuni sistemi di terra (ad esempio sistemi di comunicazione satellitare) che, previa autorizzazione dei Paesi che controllano i satelliti, possono ricevere informazioni provenienti da questi ultimi[117]. È comune, tuttavia, la minaccia cyber ai sistemi spaziali, che deve essere affrontata con attenzione e decisione da entrambi gli attori[118].

Complessivamente, la posizione della Nato nello spazio è ancora in fase di definizione, in particolare dopo il riconoscimento dello spazio come dominio operativo nel 2019 e il lancio di alcune iniziative, tra cui un Centro di eccellenza dedicato con base a Tolosa. Nel gennaio 2022 la Nato ha pubblicato una "*Overarching Space Policy*" contenente l'esposizione dei principi cardine dell'approccio alleato al nuovo dominio, inclusa una valutazione delle minacce in cui rientra quella cyber, l'applicazione dell'Articolo 5 e, in generale, il ruolo che l'organizzazione può assumere come forum politico-militare[119]. Il Concetto strategico approvato dai capi di stato e di governo nel vertice di Madrid a giugno 2022 ha inserito pienamente e ufficialmente sia il dominio spaziale che quello cyber nella postura complessiva di deterrenza e difesa Nato, elevandone l'importanza e ponendo le basi per ulteriori sviluppi dottrinali e organizzativi[120]. Il Concetto strategico sancisce anche la necessità per una deterrenza e difesa efficace di mantenere un accesso sicuro e privo di restrizioni agli ambienti spaziale e cyber[121].

[115] Nato, *French Space Exercise AsterX Builds on Realistic Scenario and Integration*, 9 marzo 2023, https://ac.nato.int/archive/2023/FRA_AsterX23.

[116] Ministero della Difesa, *Il Comando delle Operazioni Spaziali partecipa alla AsterX 2023*, 13 marzo 2023, https://www.difesa.it/SMD_/Eventi/Pagine/Il_Comando_delle_Operazioni_Spaziali_partecipa_alla_AsterX_2023.aspx.

[117] Beyza Unal, "Cybersecurity of NATO's Space-based Strategic Assets", cit., p. 9.

[118] Intervista, 1 dicembre 2022.

[119] Nato, *NATO's Overarching Space Policy*, 17 gennaio 2022, https://www.nato.int/cps/en/natohq/official_texts_190862.htm.

[120] Alessandro Marrone, "NATO's New Strategic Concept: Novelties and Priorities", in *IAI Commentaries*, n. 22|30 (luglio 2022), https://www.iai.it/it/node/15667.

[121] Nato, *NATO 2022 Strategic Concept*, 29 giugno 2022, https://www.nato.int/cps/en/natohq/topics_210907.htm.

ISSN 2280-6164

Infine, nel corso della conferenza *NATO Cyber Defence Pledge* tenutasi a Roma nel novembre 2022 e co-organizzata dall'Italia, il Segretario generale Jens Stoltenberg ha evidenziato la credibilità della minaccia cyber contro i sistemi spaziali, richiamando i casi concreti delle operazioni condotte in Ucraina[122].

7. Questioni aperte e spunti di riflessione

7.1 Un problema da non sottovalutare

Nonostante numerose componenti spaziali attuino già misure di cybersicurezza per garantire disponibilità, confidenzialità e integrità delle informazioni, l'attuale livello complessivo di cybersicurezza di gran parte delle infrastrutture satellitari esistenti non è soddisfacente[123]. Le politiche esistenti a livello internazionale, siano esse relative al dominio spaziale o a quello cyber, non sono all'altezza delle sfide cui gli stati Ue e Nato andranno incontro negli anni a venire[124].

La cybersicurezza dei sistemi spaziali dovrebbe essere considerata tema prioritario da affrontare con urgenza, soprattutto se si considerano, da un lato, le crescenti capacità tecniche e tecnologiche dimostrate da attori (statali e non) ritenuti ostili e, dall'altro, il livello di dipendenza delle società avanzate rispetto ai servizi offerti da questi sistemi[125]. Ciò in aggiunta al fatto che esiste un frequente problema di obsolescenza dei software presenti nei satelliti attualmente in orbita, creati in epoca analogica, prima dell'affermazione dell'approccio della *security by design*, e quindi intrinsecamente vulnerabili[126]. In altre parole, occorre approcciarsi allo spazio come al Mediterraneo: non si può pensare di conseguire i propri interessi e ottenere vantaggi senza prima garantire la sicurezza[127]. A riconoscimento della necessità specifica di condividere principi di cybersicurezza dei sistemi spaziali è intervenuta anche la *Space Policy Directive-5* (Spd-5), pubblicata dalla Casa Bianca nel settembre 2020[128].

Anche gli standard che proteggono assetti e infrastrutture spaziali non sono ritenuti sufficienti[129]. È necessario elaborare standard di cybersicurezza e cyber difesa più alti e definiti, condivisi anche partendo da un livello minimo comune,

[122] Nato, *NATO Secretary General Warns of Growing Cyber Threat*, 10 novembre 2022, https://www.nato.int/cps/en/natohq/news_208889.htm.

[123] Intervista, 1 dicembre 2022; Brian Weeden e Victoria Samson (a cura di), *Global Counterspace Capabilities*, cit., p. 13-07.

[124] Brandon Bailey et al., *Defending Spacecraft in the Cyber Domain*, cit., p. 1.

[125] Ibid., p. 7.

[126] Interventi di Gianluca Galasso e Domitilla Benigni al seminario IAI "La minaccia cyber allo spazio", cit.

[127] Intervento di Carmine Masiello al seminario IAI "La minaccia cyber allo spazio", cit.

[128] White House, *Memorandum on Space Policy Directive-5 – Cybersecurity Principles for Space Systems*, 4 settembre 2020, https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems.

[129] Brandon Bailey et al., *Defending Spacecraft in the Cyber Domain*, cit., p. 1.

ISSN 2280-6164

se si vogliono evitare aggressioni o si voglia, perlomeno, assicurare una maggiore resilienza dei sistemi spaziali. Altrettanto insufficienti sono le misure di *governance* che riguardano le connessioni tra dominio spaziale e cyber[130].

Nella fattispecie dei sistemi spaziali cosiddetti *dual use*, vale a dire impiegabili sia per fini civili che militari, si registra l'esigenza di aumentare il livello di cybersicurezza, al fine di assicurare una protezione adeguata da attacchi cyber soprattutto durante il loro impiego per operazioni militari[131]. Particolare attenzione dovrebbe inoltre essere posta sui sistemi informatici a bordo degli assetti spaziali[132].

7.2 Un impegno collettivo

Per incrementare la resistenza dei sistemi spaziali ad attacchi cyber è fondamentale un'azione comune che coinvolga governi, industrie e organizzazioni internazionali. Nell'Ue si osserva in molti casi la propensione a portare avanti conversazioni parallele riguardo la minaccia cyber alle infrastrutture spaziali a terra e a quelle in orbita, quando tali riflessioni dovrebbero avvenire in modo integrato e concertato[133]. Vi è inoltre la tendenza, da parte di alcuni decisori politici, di voler mantenere separati i diversi settori coinvolti nelle attività spaziali, ad esempio quello militare e quello commerciale, a danno di entrambi vista l'estrema interdipendenza in essere.

A livello europeo è necessario investire maggiori risorse ed energie nell'analisi e contrasto della minaccia cyber ai sistemi spaziali, cercando di evitare un approccio a compartimenti stagni e riconoscendo che lo spazio è un dominio condiviso, dove attori diversi operano in contemporanea[134]. È importante che le istituzioni europee assicurino trasparenza rispetto allo stato dell'arte delle proprie capacità spaziali verso il settore privato, coinvolgendolo nelle decisioni che avvengono a livello governativo[135]. Soprattutto considerato come il settore privato è spesso in grado di contribuire con delle competenze e una velocità di azione che, nel quarto e quinto dominio, spesso le istituzioni nazionali e internazionali non possono assicurare[136]. Sarà necessaria una stabile collaborazione tra decisori politici, tecnici e programmatori al fine di garantire sinergia tra politiche e applicazioni tecniche[137]. Allo stesso tempo, è importante che gli *end user* istituzionali dei sistemi spaziali valutino attentamente i rischi e i benefici che derivano dall'utilizzo di sistemi commerciali[138]. Gli assetti civili, infatti, fatti salvi sistemi altamente strategici come

130 Ibid., p. 4.
131 Beyza Unal, "Cybersecurity of NATO's Space-based Strategic Assets", cit., p. 7.
132 Brandon Bailey et al., *Defending Spacecraft in the Cyber Domain*, cit., p. 7.
133 Intervista, 2 dicembre 2022 a.
134 Ibid.; intervista, 6 dicembre 2022.
135 Intervista, 6 dicembre 2022.
136 Intervento di Carmine Masiello al seminario IAI "La minaccia cyber allo spazio", cit.
137 Brandon Bailey et al., *Defending Spacecraft in the Cyber Domain*, cit., p. 1.
138 Intervista, 7 dicembre 2022; intervento di Sergio Antonio Scalese al seminario IAI "La minaccia cyber allo spazio", cit.

ISSN 2280-6164

ad esempio i componenti della costellazione Galileo, sono soggetti a meno controlli di sicurezza rispetto a quelli militari, e sono quindi potenzialmente più esposti ad attacchi cyber[139]. Potenzialmente dirompente potrebbe essere l'espansione nel settore spaziale dei servizi in cloud, forniti da giganti tecnologici statunitensi quali Amazon e Microsoft, che coinvolgono sia attori commerciali che istituzionali e rappresentano un'opportunità ma anche alcuni rischi nella condivisione di dati sensibili. In questo senso, la cybersicurezza dei sistemi spaziali deve essere considerata il punto di arrivo di un compromesso basato su un'attenta valutazione del rischio[140].

In prospettiva, un ruolo attivo e rilevante a livello europeo è giocato dall'Esa, che ha implementato un proprio *Security Framework* approvato dai suoi 22 stati membri e permette di portare avanti un discorso comune di sicurezza applicato in maniera olistica[141]. L'obiettivo infatti è mettere in sicurezza tutte le missioni spaziali dell'Agenzia, non solo i programmi classificati, attraverso un processo di certificazione e accreditamento prima in fase di design e successivamente in fase di test per assicurare un profilo di rischio accettabile per il livello operativo del sistema. Il tema non rappresenta un elemento di novità per l'Esa che infatti si sta dotando di un *Cyber-Security Operations Centre* (C-Soc) sotto la responsabilità del Security Office dell'Agenzia e realizzato da un consorzio guidato da Leonardo[142]. Il Centro peraltro si inserisce in un più ampio progetto di cybersicurezza e resilienza per il monitoraggio della sicurezza dei segmenti spaziale e di terra, basato su una piattaforma dove poter analizzare le vulnerabilità ma anche condurre test ed esercitazioni. Il progetto prevede anche una piattaforma di operazioni portatile in grado di permettere il collegamento protetto in remoto agli stati membri e che sarà consegnato in una prima versione operativa dal 2024 agli utenti, tra cui ad esempio anche l'Agenzia per la Cybersicurezza Nazionale e il Ministero della Difesa.

Segnali positivi arrivano anche da alcune importanti iniziative attualmente in corso a livello Ue. Tra queste si segnala la possibilità di stabilire un *Computer Incident Response Centre* per il dominio spaziale, per facilitare lo scambio di informazioni confidenziali, anche riguardo attacchi cyber a sistemi spaziali[143]. La condivisione di informazioni rappresenta infatti una condizione fondamentale ai fini dell'incremento della sicurezza – anche cyber – dell'Italia, dunque un elemento al quale dedicare particolare attenzione e sul quale investire adeguate risorse[144].

[139] Intervento di Danilo Figà al seminario IAI "La minaccia cyber allo spazio", cit.

[140] Intervista, 9 febbraio 2023.

[141] Intervista, 23 marzo 2023.

[142] Esa, *New Cyber-Security Centre Will Safeguard ESA Assets and Missions*, 22 dicembre 2021, https://www.esa.int/Space_Safety/New_cyber-security_centre_will_safeguard_ESA_assets_and_missions2.

[143] Intervista, 7 dicembre 2022.

[144] Intervista, 9 febbraio 2023.

ISSN 2280-6164

Per poter gestire le sfide che quarto e quinto dominio si trovano ad affrontare sarà necessario, sia a livello nazionale che europeo, garantire una leadership stabile e competente, in grado di pensare e operare in ottica multi-dominio[145]. Ciò apre la questione delle risorse umane, tema problematico per la Difesa, che si trova a competere con un settore – quello privato – che spesso rappresenta per molti un'attraente alternativa, e al quale occorre che la Pubblica Amministrazione risponda con creatività[146].

Come evidenziato in precedenza, lo spettro di tecniche utilizzate per condurre attacchi cyber contro sistemi spaziali è destinato ad aumentare[147]. Se il ritmo di sviluppo tecnologico favorisce sicuramente l'evoluzione delle minacce cyber, i sistemi spaziali vivono di un cambiamento relativamente più lento e graduale. Ne consegue che le misure di cybersicurezza applicate allo spazio devono essere calibrate, oltre che su aggressioni ritenute fattibili al giorno d'oggi, anche su minacce che si reputano possibili nel medio termine[148].

aggiornato 4 aprile 2023

ISSN 2280-6164

145 Intervento di Carmine Masiello al seminario IAI "La minaccia cyber allo spazio", cit.

146 Ibid.

147 Brian Weeden e Victoria Samson (a cura di), *Global Counterspace Capabilities*, cit., p. 13-01.

148 Intervista, 2 dicembre 2022 b.

Lista degli acronimi

C2	Comando e controllo
Cisa	Cybersecurity and Infrastructure Security Agency
Cots	Commercial off the Shelf
C-Soc	Cyber-Security Operations Centre
DDoS	Distributed Denial of Service
Dew	Directed Energy Weapons
Dg Defis	Directorate-General for Defence Industry and Space
Eda	European Defence Agency
Edf	European Defence Fund
Enisa	European Union Agency for Cybersecurity
Esa	European Space Agency
Euras	EU Radio Navigation Solution
Euspa	EU Agency for the Space Programme
Eusssd	EU Space Strategy for Security and Defence
Ew	Electronic Warfare
Fbi	Federal Bureau of Investigation
Geode	Galileo for EU Defence
Gnss	Global Navigation Satellite System
GovSatCom	Governmental Satellite Communication
Gps	Global Positioning System
Gsa	European Gnss Agency
Gsmc	Galileo Security Monitoring Centre
Iris2	Infrastructure for Resilience, Interconnectivity and Security by Satellite
Isac	Information Sharing and Analysis Centre
Mitm	Man-in-the-Middle
Nasa	National Aeronautics and Space Administration
Navwar	Navigation Warfare
Nis	Network and Information Security
Pesco	Permanent Structured Cooperation
Pil	Prodotto interno lordo
Pnt	Position Navigation and Timing
Prs	Public Regulated Service
Rf	Radiofrequenza
Sab	Security Accreditation Board
Sda	Space Development Agency
Seae	Servizio europeo per l'azione esterna

© 2023 IAI
ISSN 2280-6164
DOCUMENTI IAI 23 | 06 - MARZO 2023

Som	Security Operations and Monitoring Centre
Spd-5	Space Policy Directive-5
Ssf	Strategic Support Force
Stra	Space Threat Response Architecture
Tt&c	Telemetry, Tracking and Command
Ue	Unione europea

ISSN 2280-6164

Programma del seminario "La minaccia cyber allo spazio"

Roma, 14 marzo 2023

Saluti di benvenuto

Ferdinando Nelli Feroci, Presidente, Istituto Affari Internazionali (IAI)

Introduzione

Ottavia Credi, Ricercatrice, Programmi Difesa e Sicurezza, IAI

Giancarlo La Rocca, Ricercatore Junior, Programmi Difesa e Sicurezza, IAI

Relatori

Domitilla Benigni, Direttore Generale e Amministratore Delegato, Elettronica

Gianluca Galasso, Responsabile Servizio Operazioni, Agenzia per la cybersicurezza nazionale

Marco Florissi, Office of the Executive Director, EU Agency for the Space Programme

Carmine Masiello, Sottocapo di Stato Maggiore della Difesa

Danilo Figà, Capo di Stato Maggiore, Comando delle Operazioni Spaziali

Antonio Scalese, Comandante, Comando per le Operazioni in Rete

Modera

Karolina Muti, Responsabile di ricerca, Programmi Difesa e Sicurezza, IAI

Conclusioni

Adolfo Urso, Ministro delle Imprese e del Made in Italy con delega alle politiche spaziali e aerospaziali

ISSN 2280-6164

ISSN 2280-6164

Istituto Affari Internazionali (IAI)
L'Istituto Affari Internazionali (IAI) è un think tank indipendente, privato e non-profit, fondato nel 1965 su iniziativa di Altiero Spinelli. Lo IAI mira a promuovere la conoscenza della politica internazionale e a contribuire all'avanzamento dell'integrazione europea e della cooperazione multilaterale. Si occupa di temi internazionali di rilevanza strategica quali: integrazione europea, sicurezza e difesa, economia internazionale e *governance* globale, energia e clima, politica estera italiana; e delle dinamiche di cooperazione e conflitto nelle principali aree geopolitiche come Mediterraneo e Medioriente, Asia, Eurasia, Africa e Americhe. Lo IAI pubblica una rivista trimestrale in lingua inglese (*The International Spectator*), una online in italiano (*AffarInternazionali*), due collane di libri (*Global Politics and Security* e *IAI Research Studies*) e varie collane di paper legati ai progetti di ricerca (*Documenti IAI*, *IAI Papers*, ecc.).

Via dei Montecatini, 17 - I-00186 Roma, Italia
T +39 06 6976831
iai@iai.it
www.iai.it

Ultimi DOCUMENTI IAI

Direttore: Alessandro Marrone (a.marrone@iai.it)

23 | 06 Ottavia Credi, Giancarlo La Rocca e Alessandro Marrone, *Il dominio spaziale e la minaccia cyber*

23 | 05 Alessandro Marrone e Elio Calcagno, *Sistemi di combattimento navali: sviluppi e sfide*

23 | 04 Nicolò Fasola et al., *Space – Exploring NATO's Final Frontier*

23 | 03 Leo Goretti and Irene D'Antimo, *Italy between the Draghi and Meloni Governments*

23 | 02 Ilaria Bertocchini, *Women and Conflicts: What Role for Women Mediator Networks?*

23 | 01 Alessandro Marrone and Elio Calcagno (eds), *Naval Combat Systems: Developments and Challenges*

22 | 08 Akram Ezzamouri, *Connectivity, Value Chains and the Green Transition: Promoting Multilateralism and Sustainable Growth across the Shared Mediterranean Space*

22 | 07en Ottavia Credi and Camilla Vianini, *Short Range Air Defence: Operational and Technological Developments*

22 | 06 Ottavia Credi et al., *Difesa aerea ravvicinata: sviluppi operativi e tecnologici*

22 | 06 Elio Calcagno, Alessandro Marrone e Michele Nones, *La Bussola strategica Ue e dodici sfide per l'Italia*