Istituto Affari Internazionali

© 2024 IAI

ISSN 2280-6164

DOCUMENTI IAI 24 | 07 - LUGLIO 2024

Le minacce cyber ed elettromagnetiche alle infrastrutture spaziali

di Elio Calcagno, Alessandro Marrone,
Maria Vittoria Massarin, Michele Nones e Gaia Ravazzolo

ABSTRACT

I sistemi spaziali stanno diventando sempre più numerosi e vitali per il funzionamento della società, rivestendo un ruolo cruciale anche nelle operazioni militari. Con l'espansione della *space economy* e la crescente rilevanza assunta dai dati forniti dai satelliti, questi ultimi sono inevitabilmente diventati obiettivi appetibili per attacchi o sabotaggi non cinetici, che includono minacce cyber e operazioni nello spettro elettromagnetico. In tale scenario, si rivela sempre più urgente dotarsi di normative a livello europeo e nazionale che consentano sia di sfruttare le potenzialità del settore spaziale, sia di garantire il corretto funzionamento degli assetti in orbita. La resilienza dei sistemi spaziali può essere raggiunta, infatti, attraverso un approccio olistico che consideri sia la componente tecnologica, adottando il principio del "*secure by design*", sia quella umana, con particolare attenzione alla formazione del personale in ambito cyber. Allo stesso tempo, per il sistema paese è fondamentale che ci si doti di una strategia nazionale che definisca in modo chiaro le competenze e agisca in sinergia con il comparto industriale.

keywords

Spazio | *Difesa* | *Sicurezza informatica* | *Infrastrutture* | *Satelliti* | *Unione europea* | *Italia*

Le minacce cyber ed elettromagnetiche alle infrastrutture spaziali

di Elio Calcagno, Alessandro Marrone, Maria Vittoria Massarin, Michele Nones e Gaia Ravazzolo*

1. Le minacce non cinetiche alle infrastrutture spaziali

1.1 Inquadramento della minaccia

I sistemi spaziali svolgono un ruolo cruciale nell'assicurare il funzionamento efficiente e ininterrotto di ogni settore della società, inclusa la difesa. La *space economy*, definita dall'Organizzazione per la cooperazione e lo sviluppo economico come "l'insieme delle attività e dell'uso delle risorse spaziali che creano valore e benefici per l'umanità nel corso dell'esplorazione, comprensione, gestione e utilizzo dello spazio"[1], è infatti in crescita e in evoluzione. Gli oltre 9.000 satelliti oggi in orbita (pronti a diventare più di centomila nel prossimo decennio)[2] rendono possibile lo sviluppo di diversi servizi, che a loro volta consentono nuove applicazioni in numerosi settori quali la meteorologia, l'energia, le telecomunicazioni, l'agricoltura, le assicurazioni, i trasporti terrestri e marittimi, l'aviazione e la finanza. Per avere un'idea della portata del settore, basti pensare che si stima che il mercato spaziale globale valesse circa 464 miliardi di dollari nel 2022 e si prevede che raggiungerà gli oltre 737 miliardi di dollari entro neanche un decennio[3].

[1] Organizzazione per la cooperazione e lo sviluppo economico, *OECD Handbook on Measuring the Space Economy*, Parigi, OECD Publishing, 2012, p. 19, https://doi.org/10.1787/9789264169166-en.

[2] Jeffrey Kluger, "Scientists Sound the Alarm over a Growing Trash Problem in Space", in *Time*, 13 marzo 2023, https://time.com/6262389/space-junk-increasing-problem.

[3] Euroconsult, *Value of Space Economy Reaches $464 Billion in 2022 Despite New Unforeseen Investment Concerns*, 9 January 2023, https://www.euroconsult-ec.com/?p=13695.

* Elio Calcagno è ricercatore nel programma "Difesa" dell'Istituto Affari Internazionali (IAI). Alessandro Marrone è responsabile del Programma Difesa dello IAI. Maria Vittoria Massarin è ricercatrice junior nei programmi "Difesa" e "Sicurezza" dello IAI. Michele Nones è vicepresidente e consigliere scientifico dello IAI. Gaia Ravazzolo è ricercatrice junior nel programma "Difesa" dello IAI. Gli autori ringraziano Alessio Guidi, Ilenia Bruseghello e Adrian Vulcano per il prezioso contributo e supporto nella realizzazione dello studio.

Questo studio è stato preparato per il seminario "Cyber, guerra elettronica e spettro elettromagnetico: implicazioni per lo spazio" organizzato dallo IAI presso la sede dell'Istituto il 16 maggio 2024 con il supporto di ELT Group, ed è stato rivisto alla luce del dibattito ivi svoltosi.

© 2024 IAI

ISSN 2280-6164

Per le forze armate i singoli satelliti e le costellazioni sono un elemento fondamentale per le operazioni negli altri quattro domini operativi poiché forniscono servizi abilitanti, quali l'osservazione della Terra (*Earth Observation*, Eo), servizi di posizionamento, navigazione e tempo (*Positioning, Navigation and Timing*, Pnt), comunicazioni satellitari (*Satellite Communications*, SatCom) e applicazioni di intelligence, sorveglianza e ricognizione (*Intelligence, Surveillance and Reconnaissance*, Isr), quali l'allarme missilistico precoce (*missile early warning*) e lo spionaggio di segnali elettromagnetici (*Signal Intelligence*, SigInt)[4]. La sicurezza nello spazio e sulla Terra sono, pertanto, inestricabilmente legate e lo sviluppo di sistemi satellitari avanzati è fondamentale per il supporto alle attività terrestri di operatori militari, istituzionali e commerciali.

La crescente centralità dei servizi spaziali li rende quindi inevitabilmente obiettivi più appetibili ad attacchi o sabotaggi. Diventa perciò sempre più prioritario promuovere e garantire la resilienza e la protezione di questi sistemi da attacchi cinetici e non-cinetici, identificando soluzioni in grado di trasformare le risorse spaziali da potenziali vulnerabilità ad asset più resilienti[5].

Nello spazio gli attacchi cinetici volti a danneggiare o neutralizzare fisicamente assetti in orbita sono possibili ma non costituiscono un metodo ideale per tre ragioni principali. La prima è che il Trattato sullo spazio extra-atmosferico (*Outer Space Treaty*, Ost) pone dei limiti alla presenza di armi nello spazio[6], e che condurre degli attacchi cinetici potrebbe portare a una sua violazione poiché, secondo il trattato, le attività svolte nello spazio extra atmosferico devono necessariamente essere condotte con scopi pacifici. Vi è poi la certezza che un attacco tramite l'uso di missili anti-satellite produca un grande quantitativo di detriti orbitali (*debris*) pericolosi per altri satelliti e assetti in orbita e dunque anche per l'infrastruttura spaziale dello stesso attaccante. Infine, attacchi di questo tipo sono più facilmente attribuibili di quelli non-cinetici. Le minacce non-cinetiche risultano perciò generalmente più economiche, accessibili e di difficile attribuzione, e vengono quindi scelte più spesso dagli attaccanti. Queste minacce possono essere dirette verso tutti e tre gli elementi costituivi dei sistemi spaziali: il *ground segment* (segmento terrestre), lo *space segment* (segmento spaziale) e il *data link segment* (a indicare tutto ciò che c'è tra *space* e *ground segment*). Le principali tipologie di minacce non-cinetiche sono due: da un lato quelle cyber, e dall'altro quelle che si traducono in operazioni nello spettro elettromagnetico (*Electromagnetic Spectrum Operations*, Emso).

[4] 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.

[5] Emanuele Galtieri, "Il business nell'era del cyber-spazio", in *Formiche*, 2 febbraio 2023, https://formiche.net/?p=1530210.

[6] All'articolo 4 del Trattato si stabilisce che: "La luna e gli altri corpi celesti saranno utilizzati da tutti gli Stati Parte del Trattato esclusivamente per scopi pacifici". Si veda: *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 1966, https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html.

DOCUMENTI IAI 24 | 07 - LUGLIO 2024 ISSN 2280-6164
© 2024 IAI

© 2024 IAI

ISSN 2280-6164

1.2 Le minacce cyber agli assetti spaziali

I satelliti sono controllati da terminali situati a terra, dove gli operatori si servono di sistemi informatici per controllare gli assetti in orbita, trasmettendo e ricevendo informazioni sotto forma di dati, nonché istruzioni ai satelliti relative alle loro manovre e attività, quali la *collision avoidance* o l'utilizzo di sensori. Come ogni sistema computazionale, i satelliti sono vulnerabili alle intrusioni informatiche durante tutte le fasi: progettazione, implementazione e operazioni[7].

Gli attacchi cyber sono quindi utilizzabili per compromettere e/o manipolare i sistemi informatici e le reti associate alle risorse spaziali. Ciò può riguardare satelliti, stazioni di controllo a terra[8] e reti di comunicazione. Tale tipo di attacchi interessa un'ampia superficie di attacco che è composta dalle reti, dal software, dai servizi forniti e dai sistemi che compongono l'infrastruttura stessa[9].

Un sistema spaziale militare è nel suo insieme tendenzialmente chiuso e dunque inaccessibile da reti esterne[10]. Perciò, nell'ambito militare, l'introduzione di virus all'interno di un sistema può generalmente avvenire soltanto attraverso terminali situati nel *ground segment* e sfruttando l'errore umano. Per i satelliti commerciali, tendenzialmente connessi alla rete internet, la superficie di attacco è giocoforza più ampia e i fattori di rischio più numerosi, anche perché spesso non vi è consapevolezza di queste minacce. Inoltre, per abbattere i costi i produttori di satelliti utilizzano in molti casi tecnologie standardizzate e non dedicate, correndo il rischio di aumentarne le vulnerabilità nei confronti di attacchi non cinetici, specie se in assenza di processi formali di verifica e certificazione dell'hardware e del software[11].

Inoltre, i sistemi spaziali, civili e militari, sono spesso progettati per durare decenni. I più datati ancora in servizio sono di conseguenza maggiormente esposti ad attacchi cyber in quanto soggetti a limitazioni tecniche legate all'arretratezza dell'hardware, che può diventare obsoleto e non più in grado di supportare un software più recente che permetta di far fronte a minacce in continua evoluzione[12]. Non bisogna poi dimenticare i vincoli legati alle risorse a disposizione dell'assetto

[7] Brandon Bailey, "Protecting Space Systems from Cyber Attack", in *Aerospace TechBlog*, 31 marzo 2022, https://medium.com/the-aerospace-corporation/protecting-space-systems-from-cyber-attack-3db773aff368.

[8] Greg Hadley, "'Backdoor' to Attack Satellites: CSO Sees Cyber Risks in Space Force Ground Systems", in *Air & Space Forces Magazine*, 31 gennaio 2023, https://www.airandspaceforces.com/?p=181062.

[9] Per un approfondimento su questo tema si veda: Ottavia Credi, Giancarlo La Rocca e Alessandro Marrone, "Il dominio spaziale e la minaccia cyber", in *Documenti IAI*, n. 23|06 (marzo 2023), https://www.iai.it/it/node/16806.

[10] Intervista, 5 marzo 2024.

[11] Walter Peeters, "Cyberattacks on Satellites: An Understimated Political Threat", in *LSE IDEAS Space Policy Publications*, 5 maggio 2022, https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites.

[12] Intervista, 19 febbraio 2024.

spaziale. Esso può avere infatti capacità computazionali limitate a causa delle restrizioni relative alla generazione di energia, al volume e al peso che possono rappresentare un ostacolo per l'attuazione di misure di sicurezza avanzate o per l'aggiornamento frequente del software[13]. I sistemi spaziali, inoltre, possono essere estremamente eterogenei e complessi, specialmente nei casi delle grandi costellazioni satellitari, composte da diversi elementi (a terra e/o in orbita) che vengono aggiunti nel tempo, anche a distanza di anni l'uno dall'altro. Si pone dunque il problema di dover salvaguardare la sicurezza di un intero sistema di sistemi senza che i nodi più obsoleti e vulnerabili compromettano l'integrità dell'insieme con un effetto domino[14]. D'altro canto, nelle costellazioni satellitari formate da più satelliti spesso identici le medesime vulnerabilità sono diffuse, aumentando l'impatto di possibili attacchi che sfruttino una stessa "breccia".

In un contesto globale dove la guerra ibrida diventa uno strumento sempre più diffuso, le tecnologie informatiche più accessibili ed economiche, gli attacchi cyber aventi come obiettivo i sistemi spaziali possono essere perpetrati da attori statuali e non statuali. Tuttavia, la guerra cibernetica applicata al dominio spaziale è un fenomeno piuttosto recente e, in quanto tale, non vanta ancora di dottrine d'impiego ben affermate, al contrario dei domini operativi tradizionali[15]. Le modalità d'attacco possibili sono molteplici e possono comprendere ad esempio l'intercettazione e manipolazione dei dati (a maggior ragione se il satellite è connesso a un network aperto ed aumenta così la sua vulnerabilità agli attacchi cyber)[16], il sequestro illegittimo del controllo di un sistema[17], l'interruzione dei sistemi di comunicazione, il disturbo dei segnali di controllo o l'iniezione di codici maligni nei sistemi spaziali per comprometterne la funzionalità.

Persino negli Stati Uniti, di gran lunga il Paese più capace all'interno della Nato in termini sia di operazioni cyber che di assetti nel dominio spaziale, i vertici della Space Force ammettono che le minacce cyber rappresentano un chiaro punto debole per le operazioni e le infrastrutture spaziali. Risulta infatti ancora difficile prevedere da dove futuri attacchi potranno provenire, che forma potrebbero prendere e quali componenti vorranno colpire[18].

Esistono diversi tipi di attacchi nel dominio cyber che hanno il potenziale di colpire i sistemi spaziali.

[13] Intervista, 5 marzo 2024.

[14] Intervista, 19 febbraio 2024.

[15] Intervista, 13 marzo 2024.

[16] Ottavia Credi, Giancarlo La Rocca e Alessandro Marrone, "Il dominio spaziale e la minaccia cyber", cit.

[17] Todd Harrison et al., "Space Threat Assessment 2020", in *CSIS Reports*, marzo 2020, https://www.csis.org/node/56019.

[18] Chris Gordon, "Cybersecurity Is the 'Soft Underbelly' of Space Operations, SpOC Comander Says", in *Air & Space Forces Magazine*, 14 ottobre 2022, https://www.airandspaceforces.com/?p=171742.

© 2024 IAI

ISSN 2280-6164

Tramite *l'intercettazione e la manipolazione* delle comunicazioni gli aggressori possono accedere ai dati trasmessi dai segnali di comunicazione tra stazioni di controllo a terra e assetti spaziali, e/o immettere comandi dannosi per l'intero sistema. In questo modo attori ostili possono ad esempio fornire informazioni false o fuorvianti agli operatori, in ambito militare potenzialmente con serie implicazioni per i processi decisionali basati sui dati satellitari e quindi per i risultati delle operazioni a terra e la vita stessa del personale in azione e dei civili coinvolti.

I *malware e i virus* invece possono essere utilizzati per compromettere i software dei satelliti o dei sistemi di controllo a terra, fornendo agli aggressori forme di accesso e controllo non autorizzate. A giugno 2023, ad esempio, un sistema di comunicazione satellitare al servizio dell'esercito russo è stato messo offline per un giorno da un attacco informatico condotto attraverso l'invio di un software dannoso ai terminali satellitari[19].

Gli *attacchi Denial of Service* (DoS) invece permettono di sovraccaricare i canali di comunicazione satellitari o i sistemi a terra per mezzo di volumi di traffico dati soverchianti che finiscono per sospendere i servizi stessi. Ciò può comportare l'interruzione delle comunicazioni o persino la perdita temporanea del controllo dei satelliti. Un esempio di attacco DoS è quello perpetrato dalla Russia (l'attribuzione è stata fatta da più di 20 Paesi diversi) nella prima fase dell'attacco "AcidRain", ovvero l'attacco informatico ai satelliti Ka-Sat dell'azienda statunitense Viasat in Ucraina del 24 febbraio 2022. L'attacco DoS, perpetrato contro i modem internet situati in territorio ucraino, ha permesso agli aggressori di entrare in una rete satellitare su cui funzionavano i Ka-Sat sfruttando la vulnerabilità in una rete virtuale privata (*virtual private network*, Vpn) Fortinet. Grazie all'accesso al sistema di gestione di questa rete, gli attaccanti hanno poi utilizzato un malware per scollegare i modem dalla rete Ka-Sat[20].

In questo quadro vi sono poi da considerare gli *attacchi alla catena di approvvigionamento (supply chain)*, dove l'accesso all'hardware, e soprattutto al software, del satellite per la sua compromissione è più facile rispetto a quando l'assetto è in orbita. In questo caso gli aggressori possono prendere di mira la catena di fornitura coinvolta nello sviluppo, nella produzione e nella manutenzione dei sistemi spaziali. La compromissione di componenti o l'introduzione di vulnerabilità durante il processo di produzione possono avere conseguenze di vasta portata. Un esempio di attacco di questo tipo, anche se non direttamente correlato allo spazio, è il "Big Hack" avvenuto nel 2018[21]. Questo attacco altamente

[19] Joseph Menn, "Cyberattack Knocks Out Satellite Communications for Russian Military", in *The Washington Post*, 30 giugno 2023, https://www.washingtonpost.com/technology/2023/06/30/satellite-hacked-russian-military.

[20] Kevin Poireault, "Five Takeaways from the Russian Cyber-Attack on Viasat's Satellites", in *Infosecurity Magazine*, 9 maggio 2023, https://www.infosecurity-magazine.com/news/takeaways-russian-cyberattack.

[21] Jordan Robertson e Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies", in *Bloomberg*, 4 ottobre 2018, https://www.bloomberg.com/news/features/2018-10-04/

© 2024 IAI
ISSN 2280-6164

sofisticato ha visto una cellula di intelligence militare cinese compromettere la catena di approvvigionamento attraverso l'inserimento di microchip sulle schede madre prodotte da Supermicro, una delle aziende leader nel campo delle schede madre per server. L'operazione ha portato all'infiltrazione in quasi trenta aziende statunitensi, tra cui anche Amazon e Apple.

È possibile, inoltre, arrivare alla *distruzione fisica di satelliti tramite mezzi informatici* manipolando i sistemi di controllo in modo da causare malfunzionamenti, cambi di traiettoria e quindi collisioni o *de-orbit* incontrollati. Quest'ultima tipologia di attacco si pone in qualche modo al confine con una azione cinetica, ma ancora sfrutta la maggiore difficoltà di attribuzione tipica di attacchi non-cinetici come quelli cyber.

Sono dunque diverse le criticità da superare per rendere gli attuali sistemi satellitari maggiormente resilienti a un attacco cyber, considerando che la maggior parte di questi non sono stati progettati e prodotti secondo il principio del "*secure by design*". Oltre ai rischi noti sul *ground segment* e sui data link, sul fronte della cybersicurezza è necessario fare i conti con il nuovo e rilevante fattore di rischio legato al concetto di "*global supply chain*". I sistemi satellitari presentano infatti vulnerabilità dovute alla mancanza di standard di sicurezza chiaramente tracciabili e alla diversità nel conformarsi alle politiche di cybersicurezza da parte dei fornitori. Questa complessità aumenta il rischio di vulnerabilità in un ecosistema aziendale interconnesso, ma non regolato uniformemente per quanto riguarda la consapevolezza del rischio cyber. Tale configurazione rende i sistemi spaziali, soprattutto quelli a scopi commerciali, suscettibili a vulnerabilità sconosciute durante l'assemblaggio dei componenti da parte degli integratori di sistema, facilitando eventuali attacchi cyber[22].

Anche l'integrazione dell'intelligenza artificiale riveste un ruolo fondamentale nell'ottimizzazione e nell'aggiornamento continuo dei sistemi, consentendo inoltre una maggiore autonomia e velocità nella rilevazione e nella neutralizzazione delle minacce[23]. I sistemi spaziali dovrebbero avere infatti la capacità di identificare una minaccia, dare l'allarme e possibilmente attuare una contromisura con crescente autonomia e velocità[24]. Le contromisure informatiche[25], infine, si concentrano sull'adozione di tecniche avanzate come i generatori di numeri casuali quantistici[26]

the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

[22] Emanuele Galtieri, "Il business nell'era del cyber-spazio", cit.

[23] Unshin Lee Harpley, "Space Force CTIO: AI Will Be 'Game-Changer' for Operational Space", in *Air & Space Forces Magazine*, 14 novembre 2023, https://www.airandspaceforces.com/?p=209126.

[24] Theresa Hitchens, "GEOST Sensors to Detect Interference Will Fly on SDA Satellites", in *Breaking Defense*, 13 settembre 2023, https://breakingdefense.com/?p=308418.

[25] John Thornhill, "A Global Satellite Blackout Is a Real Threat — Can Hackers Help?", in *Financial Times*, 8 giugno 2023, https://www.ft.com/content/d5df1e81-f126-4a48-9a42-5b4aca842dcb.

[26] ID Quantique, "Quantum Cyber Security for Satellites", in *IDQ*, 7 marzo 2023, https://www.idquantique.com/?p=34178.

© 2024 IAI
ISSN 2280-6164

o i sistemi di *quantum key distribution* (Qkd)[27] per rafforzare la sicurezza delle comunicazioni satellitari e prevenire attacchi hacker attraverso il rilevamento precoce delle vulnerabilità e l'attuazione di aggiornamenti costanti.

1.3 Le operazioni nello spettro elettromagnetico

Fin dalla prima metà del ventesimo secolo le operazioni militari hanno iniziato ad appoggiarsi in modo crescente a tecnologie che dipendono dalla trasmissione di informazioni tramite lo spettro elettromagnetico (*Electromagnetic Space*, Ems), portando a investimenti significativi in tecnologie come il radar, la navigazione satellitare e le comunicazioni wireless. A riconferma dell'importanza militare dell'ambiente elettromagnetico (*Electromagnetic Environment*, Eme) basti pensare che è stato riconosciuto dalla Nato come ambiente operativo (*operational environment*)[28].

L'avvento degli assetti spaziali ha poi accresciuto esponenzialmente l'utilità di queste tecnologie, sia nell'ambito civile quanto in quello militare, portando anche a soluzioni dual-use, come Galileo. Galileo è infatti un sistema civile che comprende anche un servizio robusto e ad accesso controllato per applicazioni autorizzate dai governi: il Galileo Public Regulated Service (Prs) che fornisce *position* e *timing*. Si tratta di un servizio di navigazione crittografato per utenti autorizzati dai governi degli stati membri dell'Ue e per applicazioni che richiedono elevata continuità, ad esempio per i servizi di polizia o in caso di emergenze[29]. Simile ai servizi Gnss (*Global Navigation Satellite System*) aperti e commerciali di Galileo, il Galileo Prs è più resiliente perché garantisce continuità di servizio anche quando l'accesso ad altri servizi di navigazione potrebbe essere degradato ed è più robusto in caso di interferenze dannose, rendendo così più costoso e difficile, grazie alla criptazione, attaccare i suoi segnali utilizzando ad esempio lo *spoofing*[30]. In generale lo *spoofing* contro sistemi Gnss rappresenta una seria minaccia – a causa dell'ampio utilizzo delle informazioni Gnss in diverse applicazioni, che vanno dai comuni smartphone ai satelliti – ed esistono diverse metodologie, più o meno complesse, come la tecnica "*break lock*" che ha l'obiettivo finale di far "agganciare" il ricevitore a un segnale di navigazione falso[31] (vedere tabella sottostante).

In un contesto che ha visto negli ultimi anni il crescente interesse del settore privato per l'utilizzo di frequenze tradizionalmente riservate ai militari, una grande evoluzione tecnologica e l'aumento della dipendenza globale dall'Ems,

[27] Enrico Frumento, "Quantum Key Distribution: cos'è e perché è utile a rendere inattaccabili i sistemi di cifratura", in *Cybersecurity360*, 23 giugno 2022, https://www.cybersecurity360.it/?p=55479.

[28] "NATO recognizes the Electromagnetic Environment as an operating Environment". Nato, *NATO Electronic Warfare Policy* (MC 64/11), 20 agosto 2018.

[29] European GNSS Service Centre, *Galileo Public Regulated Service*, https://www.gsc-europa.eu/node/5875.

[30] Ibid.

[31] Antonio De Maio, "Global Navigation Satellite System GNSS Spoofing", in *Emsopedia*, 23 marzo 2021, https://www.emsopedia.org/?p=2279.

ISSN 2280-6164
© 2024 IAI

si moltiplicano anche le sfide dovute alla sua natura dual-use. L'avvento delle tecnologie di comunicazione di quinta generazione (5G) ha infatti aumentato la richiesta di bande di frequenze diverse. Il Congresso americano ha risposto a questo aumento della domanda decidendo di rendere disponibili nuove frequenze per l'uso commerciale, in alcuni casi riassegnando a tal fine lo spettro utilizzato dalle agenzie federali. Questi sviluppi possono anche impattare sulle capacità militari[32] e richiedono che l'Ems sia trattato come un'infrastruttura critica internazionale, sottolineando l'importanza di proteggerlo e salvaguardarne l'accesso[33]. Lo spettro elettromagnetico ha dunque una valenza sempre più duale[34], testimoniata anche dall'uso o dal leasing di satelliti commerciali per scopi militari che è diventato sempre più frequente, esponendoli a nuove minacce in quanto possibili bersagli[35] e a conseguenze concrete[36] sul loro utilizzo sul campo di battaglia.

In ambito militare, le azioni volte al disturbo e alla salvaguardia del normale funzionamento di strumenti che sfruttano l'Ems rientrano nella categoria della guerra elettronica (*Electronic Warfare*, Ew) e operano nello spettro elettromagnetico (Emso). Gli attacchi elettromagnetici mirano nello specifico ai segnali a radiofrequenza (Rf) di un sistema e coesistono con la normale gestione dello spazio elettromagnetico in supporto alle operazioni militari – *in primis* quanto a trasmissioni[37]. La minaccia elettromagnetica è ritenuta tra le più probabili per i sistemi spaziali, a prescindere dalla resilienza e dalle misure di protezione di un satellite, ed è in grado di arrecare danni anche con strumenti poco sofisticati e relativamente economici[38].

La storia dell'Emso, come in altri ambiti delle operazioni militari, è fatta di una continua dinamica di misure e contromisure, che sono in rapida evoluzione e spesso convivono tra loro. Ne consegue che le misure difensive sono concepite e costruite a strati. L'obiettivo di una difesa stratificata, che agisce sullo spettro elettromagnetico stesso, ma anche sugli strati fisici e sui pacchetti di dati che

[32] Nel 2020, ad esempio, la Federal Communications Commission statunitense ha autorizzato la rete "Ligado 5G" che potrebbe influenzare i segnali radio del sistema di posizionamento globale Gps. John R. Hoehn, Jill C. Gallagher e Kelley M. Sayler, "Overview of Department of Defense Use of the Electromagnetic Spectrum", in *CRS Reports*, n. R46564 (10 agosto 2021), https://crsreports.congress.gov/product/details?prodcode=R46564.

[33] Giuseppe Sgamba, "Electro Magnetic Spectrum Operation (EMSO)", in *Emsopedia*, 24 marzo 2021, https://www.emsopedia.org/?p=1076.

[34] Intervista, 19 febbraio 2024.

[35] Kari A. Bingen, Kaitlyn Johnson e Zhanna Malekos Smith, "Russia Threatens to Target Commercial Satellites", in *CSIS Critical Questions*, 10 novembre 2022, https://www.csis.org/node/67711.

[36] Valerie Insinna, "SpaceX Beating Russian Jamming Attack Was 'Eyewatering': DoD Official", in *Breaking Defense*, 20 aprile 2022, http://breakingdefense.com/?p=218133; Marco Battaglia, "Starlink batte il jamming russo e dà lezioni al Pentagono", in *Formiche*, 21 aprile 2022, https://formiche.net/?p=1468293.

[37] US Air Force, *Electromagnetic Spectrum Operations*, Air Force Doctrine Publication 3-85, 14 dicembre 2023, https://www.doctrine.af.mil/Operational-Level-Doctrine/AFDP-3-85-Electromagnetic-Spectrum-Operations.

[38] Ottavia Credi, Giancarlo La Rocca e Alessandro Marrone, "Il dominio spaziale e la minaccia cyber", cit.

© 2024 IAI
ISSN 2280-6164

circolano in una rete, è quello di garantire un presidio dello spettro ramificato[39].

La guerra elettronica ricomprende dunque azioni condotte nello spettro elettromagnetico nell'ambito di operazioni militari. Lo stesso tipo di operazioni, se condotte in un contesto civile o governativo, sono più spesso trattate come interferenze anche se possono fare uso di metodi e strumenti analoghi[40]. Le varie tecniche di Ew hanno in comune l'obiettivo di impedire o ostacolare il libero utilizzo dello spettro elettromagnetico da parte dell'avversario. Se per chi attacca questi metodi si concentrano in una forma di attacco DoS ai danni del nemico, chi difende è obbligato a mettere in atto contromisure adeguate[41]. Da una prospettiva legata ai sistemi spaziali, le principali minacce ascrivibili all'Ew sono molteplici come sintetizzato nella tabella seguente.

Minaccia	Descrizione	Esempi
Jamming	Il disturbo delle comunicazioni che avvengono tramite segnale radio. Questo può interferire con i collegamenti di comando e controllo, i canali di comunicazione o i segnali di navigazione satellitare, rendendoli temporaneamente inutilizzabili per l'operatore che subisce l'attacco. Nel dettaglio, il *jamming* elettromagnetico consiste nell'immissione volontaria o riflessione di energia elettromagnetica per ridurre l'uso effettivo dell'Ems da parte dell'avversario. In ambito militare, con l'inserimento di energia elettromagnetica nei percorsi di trasmissione si possono anche degradare le capacità di combattimento del nemico[42].	Nel 2018 il Ministero della Difesa norvegese rivelò che la Russia aveva persistentemente disturbato i segnali Gps (*Global Positioning System*) con la tecnica *jamming* durante l'esercitazione Nato "Trident Juncture"[43]. Il disturbo, confermato anche da funzionari della Nato, puntava a compromettere l'efficacia operativa dell'esercitazione stessa.
Spoofing	L'attacco a sensori e/o ricevitori che risulta nella falsificazione delle informazioni ricevute. Si tratta di una tecnica che può avere	A fine 2023 circa venti aerei di linea Boeing sono stati ingannati con lo *spoofing* attraverso un falso segnale Gps

[39] Intervista, 19 febbraio 2024.

[40] Ottavia Credi, Giancarlo La Rocca e Alessandro Marrone, "Il dominio spaziale e la minaccia cyber", cit.; intervista, 13 marzo 2024.

[41] Intervista, 19 febbraio 2024.

[42] US Joint Chiefs of Staff, *Joint Electromagnetic Spectrum Operations*, Joint Publication 3-85, 22 maggio 2022, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf.

[43] Brooks Tigner, "Electronic Jamming between Russia and NATO Is Par for the Course in the Future, But It Has Its Risky Limits", in *New Atlanticist*, 15 novembre 2018, https://www.atlanticcouncil.

© 2024 IAI
ISSN 2280-6164

Minaccia	Descrizione	Esempi
Spoofing (continua)	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[44]. Lo *spoofing* è ottenuto attraverso la ripetizione di impulsi di interferenza, generati replicando un segmento memorizzato del segnale minaccioso. È infatti necessario rilevare e memorizzare la forma d'onda radar contro cui effettuare l'interferenza[45]. Potrebbe includere ad esempio l'invio di falsi segnali di navigazione per ingannare i sistemi di puntamento dei satelliti o la creazione di falsi bersagli sugli schermi radar. In ambito militare ciò può avere conseguenze sulla precisione dei sistemi d'arma, con potenziali danni collaterali nel caso di un bombardamento mal guidato da sistemi spaziali manipolati dall'avversario, per citare soltanto un esempio.	mandato da terra per entrare nello spazio aereo iraniano. Gli aerei stavano sorvolando il confine tra Iraq e Iran al momento dell'attacco e lo spoofing ha portato alla perdita della capacità di navigazione dei velivoli[46]. Grazie allo *spoofing*, nel 2019 la Russia ha manipolato i sistemi di navigazione globale con l'invio su vasta scala di dati falsi sulla posizione a navi civili o altri utenti, al fine di impedire a eventuali droni di avvicinarsi al presidente Putin e di volare nello spazio aereo russo. Sembrava infatti esserci una stretta correlazione tra i movimenti del presidente russo e gli eventi di *spoofing*: la manipolazione dei sistemi di navigazione satellitare spesso coincideva con le visite di Putin in località remote e si interrompeva a visita conclusa[47].
Intercettazione elettronica	I sistemi di Ew possono intercettare e spiare i segnali di comunicazione tra le stazioni a terra e i satelliti o tra questi ultimi in un'ottica di SigInt. Tale intercettazione può fornire preziose informazioni sulle attività e le intenzioni dell'assetto intercettato[48]. Inoltre, l'avversario può sfruttare il fatto che spesso	Nell'ottobre 2023 Slingshot Aerospace, una società americana di analisi di dati spaziali focalizzata sulla sicurezza dei voli spaziali, ha sfruttato l'intelligenza artificiale per rilevare manovre insolite da parte del satellite spia russo Luch Olymp-K-2, manovre che facevano temere attività di spio-

org/?p=113248.

[44] University of Texas at Austin, "UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea", in *UT News*, 29 luglio 2013, https://news.utexas.edu/?p=2116.

[45] Massimo Annulli, "Spoofing in Radar ECM", in *Emsopedia*, 23 March 2021, https://www.emsopedia.org/?p=765.

[46] Gaurav Thakur, "What Is GPS Spoofing That Has Misguided Around 20 Planes Near Iran-Iraq Border and How Dangerous Is This", in *Deccan Herald*, 1 ottobre 2023, https://www.deccanherald.com/2708342.

[47] Dan De Luce, "Russia 'Spoofing' GPS on Vast Scale to Stop Drones from Approaching Putin, Report Says", in *NBC News*, 26 marzo 2019, https://www.nbcnews.com/news/n987376.

[48] Greg Torode, "China's Efforts to Catch Up in Global Electronic Spying Race", in *Reuters*, 14 giugno 2023, https://www.reuters.com/world/china/chinas-efforts-catch-up-global-electronic-spying-race-2023-06-14.

© 2024 IAI
ISSN 2280-6164

Minaccia	Descrizione	Esempi
Intercettazione elettronica (continua)	non è facile riconoscere in tempo reale se la traiettoria di un satellite che rappresenta una potenziale minaccia cambi per una manovra intenzionale volta a intercettare un altro satellite o perché il sistema di tracciamento dei dati[49] restituisce una posizione inaccurata per errore.	naggio nello spazio. Già il suo predecessore, Luch-1, aveva destato sospetti nel 2015 posizionandosi per cinque mesi tra due satelliti per comunicazioni commerciali Intelsat[50].
Generazione di impulsi elettromagnetici (electromagnetic pulse, Emp)[51]	Gli impulsi elettromagnetici ad alta potenza generati dai sistemi di guerra elettronica possono potenzialmente danneggiare o distruggere le componenti elettroniche dei satelliti, causandone la perdita di funzionalità.	A febbraio è stata diffusa la notizia secondo cui la Russia starebbe cercando di sviluppare un'arma spaziale Emp nucleare antisatellite in grado di distruggere i satelliti creando una grande ondata di energia diretta, potenzialmente paralizzando i satelliti circostanti. L'arma, tuttavia, secondo quanto riferito dalla CNN[52], sarebbe ancora in fase di sviluppo e non in orbita.

Per contrastare le minacce Emso vengono impiegate diverse contromisure elettroniche attive o passive (*Electronic Counter-Countermeasures*, Eccm). Tra queste ultime, l'Anti-Ew *Jamming/Spoofing* si avvale di tecniche sofisticate, che sfruttano ad esempio la crittografia per l'autenticazione delle comunicazioni o l'alterazione delle frequenze (tecnica di modulazione, filtraggio delle onde, tecnica dello spettro diffuso)[53] per fronteggiare gli attacchi di *spoofing*.

La flessibilità delle frequenze e la capacità di adattamento sono ulteriori elementi chiave per rendere più pericolosi ed efficaci i tentativi di intercettazione e il disturbo dei segnali, soprattutto se si considera che gli avversari possono utilizzare sistemi di guerra elettronica ad agilità di frequenza in grado cambiare rapidamente

[49] Sandra Erwin, "Slingshot Aereospace Harnessing AI to Track Suspicious Satellites", in *SpaceNews*, 6 ottobre 2023, https://spacenews.com/?p=192876.

[50] Ibid.

[51] Steve Kates, "The Era of Space Warfare and the Growing Threat of EMP", in *KTARNews*, 18 agosto 2021, https://ktar.com/story/4639134; Peter Vincent Pry, *Russia: EMP Threat. The Russian Federation's Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack*, gennaio 2021, https://apps.dtic.mil/sti/citations/AD1124730.

[52] Katie Bo Lillis et al., "Exclusive: Russia Attempting to Develop Nuclear Space Weapon to Destroy Satellites with Massive Energy Wave, Sources Familiar with Intel Say", in *CNN*, 17 febbraio 2024, https://edition.cnn.com/2024/02/16/politics/russia-nuclear-space-weapon-intelligence/index.html.

[53] Zixiang Jia, "Anti-jamming Technology in Small Satellite Communication", in *Journal of Physics: Conference Series*, Vol. 960 (2018), Art. 012013, https://doi.org/10.1088/1742-6596/960/1/012013.

© 2024 IAI
ISSN 2280-6164

le frequenze operative[54].

Parallelamente, anche la riduzione della sezione radar dei satelliti e l'attuazione di sistemi di ridondanza all'interno delle costellazioni[55] contribuiscono a garantire una maggiore sopravvivenza e resilienza di fronte ad azioni di guerra elettronica. I collegamenti ottici inter-satellitari sono infatti fondamentali per la connettività tra i satelliti ed è fondamentale che i terminali di comunicazione ottica siano integrati nei sistemi terrestri e aerei per consentire l'invio e la ricezione di dati in un contesto operativo. Per poter operare su bande di frequenza, forme d'onda e livelli di sicurezza diversi, è necessario quindi disporre di terminali flessibili, in grado di effettuare il roaming senza soluzione di continuità tra le diverse reti governative e commerciali[56].

2. Quadro normativo e "lessons identified" in ambito europeo

2.1 Le lacune normative nell'era delle minacce non cinetiche

Dotarsi di regole per poter sfruttare al meglio il potenziale che il settore spaziale offre è fondamentale per assicurare la riuscita delle operazioni in orbita e il corretto funzionamento dei sistemi spaziali. Negli ultimi dieci anni si è molto discusso sulla creazione di standard di sicurezza spaziale, senza però alcun progresso effettivo. Il continuo sviluppo di *counter-space capabilities*[57] e le crescenti, dirompenti, applicazioni di tecnologie nuove e vecchie evidenziano l'urgente necessità di leggi più stringenti in materia[58]. Le molteplici direttrici in cui si ramifica il settore spaziale richiedono infatti un'attenzione particolare da parte del legislatore. La sicurezza dei sistemi spaziali si profila con forza fra le principali sfide che l'industria del settore spaziale si trova a dover affrontare attualmente e nel prossimo futuro. Specialmente per gli aspetti cyber sono richiesti solidi meccanismi di difesa contro attacchi sempre più sofisticati.

Guardando alle normative che regolano il comportamento degli attori statuali e non nello spazio, invece, si rileva che, sul piano internazionale, l'Ost è lo strumento

[54] "The Challenge of Achieving Robust LPD in Tactical Scenarios", in *Army Technology*, 24 luglio 2023, https://www.army-technology.com/?p=287090.

[55] Frederick Rawlins, Richard Baker e Ivan Martinovic, *Death by a Thousand COTS: Disrupting Satellite Communications Using Low Earth Orbit Constellations*, paper presentato al Workshop on Security of Space and Satellite Systems (SpaceSec) 2023, San Diego, 27 febbraio 2023, https://doi.org/10.14722/spacesec.2023.233980; Teona Patussi, *Space Warfare and the Weaponization of Outer Space*, tesi Charles University di Praga, agosto 2022, http://hdl.handle.net/20.500.11956/178403.

[56] Matthew Mowthorpe, "Space Resilience and the Importance of Multiple Orbits", in *The Space Review*, 3 gennaio 2023, https://www.thespacereview.com/article/4504/1.

[57] Esistono quattro tipi diversi di counter-space weapons: cinetiche, non cinetiche, elettroniche e cyber. Si veda Tyler Way, "Counterspace Weapons 101", in *Aereospace Security*, aggiornato al 14 giugno 2022, https://aerospace.csis.org/aerospace101/counterspace-weapons-101.

[58] Alessandro Marrone, Michele Nones (a cura di), "The Expanding Nexus between Space and Defence", cit.

© 2024 IAI
ISSN 2280-6164

giuridico più completo che regola il dominio spaziale[59]. L'Ost è il primo dei cinque cosiddetti "*core treaties*" che regolano lo spazio extra-atmosferico, che comprendono anche la Convenzione sull'immatricolazione degli oggetti spaziali, la Convenzione sulla responsabilità per danni causati da oggetti lanciati nello spazio, l'Accordo sul salvataggio e il rientro degli astronauti e il rientro degli oggetti lanciati nello spazio, e l'Accordo che regola le attività degli Stati sulla Luna[60].

L'Ost non tratta nel merito le minacce non-cinetiche, ma menziona le "comunicazioni via radio" e le "radiofrequenze" e alcuni dei principi in esso contenuti possono essere interpretati per essere applicati anche al dominio cyber. Tuttavia, è importante sottolineare che l'Ost non contiene previsioni direttamente connesse all'interazione tra cyber e spazio. La causa di questa lacuna è interamente da ricondurre al fatto che il Trattato sia stato ratificato nel 1967 e da allora la comunità internazionale non ha elaborato altri strumenti giuridici vincolanti per tutelare la sicurezza dello spazio e adeguarsi alla rapida evoluzione delle tecnologie. Questo ha negli anni portato a un'opera di deduzione da parte di studiosi e legislatori che, partendo dai principi contenuti nell'Ost, hanno tentato di estenderli al dominio cyber. Alcuni di essi, infatti, potrebbero ricomprendere anche situazioni che coinvolgono minacce non cinetiche nello spazio. Il principio dell'uso pacifico e quello di non interferenza nelle attività spaziali degli altri Stati, per esempio, possono essere interpretati come una proibizione di attività cyber dannose che possono disturbare o mettere fuori uso i sistemi spaziali[61]. Tali interpretazioni non sono però definitive e lasciano spazio a un'ambiguità purtroppo familiare nel campo normativo del dominio spaziale.

Una delle controversie più accese degli ultimi anni riguarda infatti la diversa interpretazione che gli Stati danno di alcuni dei concetti chiave contenuti nel Trattato. L'espressione "uso pacifico dello spazio extra atmosferico" è da molti intesa con un'accezione puramente non militare, mentre altri la inquadrano nell'ampio spettro dei comportamenti considerati come un'aggressione. Nell'Ost, inoltre, non si ravvisano disposizioni che trattino di armi convenzionali o di qualsiasi altro tipo di arma che non sia un'arma di distruzione di massa. In virtù del sempre maggiore numero di Stati che stanno sviluppando capacità cyber e di Ew questa lacuna deve essere colmata al più presto. Il carattere dual-use intrinseco dei sistemi spaziali e l'ambiguità dei trattati internazionali lasciano agli Stati ampio spazio d'azione nell'utilizzare tecnologie e capacità in modo malevolo[62]. Queste distinzioni ostacolano l'effettività dell'Ost, limitando il suo raggio d'azione quando

[59] Ad agosto 2023 il Trattato è stato firmato e ratificato da 114 paesi, mentre altri 22 paesi l'hanno sottoscritto ma non ancora ratificato.

[60] Ottavia Credi e Maria Vittoria Massarin, "L'Italia nello spazio: collaborazioni e prospettive future", in *Documenti IAI*, n. 23|21 (novembre 2023), https://www.iai.it/it/node/17753.

[61] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space*, cit.

[62] Rajeswari Pillai Rajagopalan, "A Consequence-based Approach Is Needed for Space Security", in *The Diplomat*, 19 ottobre 2023, https://thediplomat.com/2023/10/a-consequence-based-approach-is-needed-for-space-security.

© 2024 IAI
ISSN 2280-6164

si tratta di aspetti di guerra elettronica o cibernetica nello spazio[63].

Negli ultimi anni, gli sforzi per affrontare le sfide poste da comportamenti nel dominio cyber potenzialmente dannosi per i sistemi spaziali sono aumentati, riflettendo la progressiva rilevanza che il dominio sta assumendo. Ad esempio, il Centro di eccellenza per la difesa cibernetica cooperativa della Nato a Tallinn, e il Centro di eccellenza europeo per il contrasto alle minacce ibride a Helsinki sono importanti esempi di partenariato e cooperazione operativa fra istituzioni per il contrasto ai comportamenti malevoli nel settore cyber. Inoltre, nel 2016, l'Unione europea e la Nato hanno firmato un accordo tecnico sulla cooperazione informatica, che prevede lo scambio di informazioni e analisi, e lo svolgimento di attività di formazione ed esercitazioni nel dominio cibernetico. Sebbene l'obiettivo di questi sforzi non sia quello di proteggere le risorse spaziali da attacchi cyber, il miglioramento della sicurezza informatica e la creazione di resilienza dei sistemi possono giovare ai componenti delle infrastrutture spaziali che si trovano a terra o in orbita[64].

2.2 Quadro normativo Ue sulla cybersicurezza

Il quadro normativo Ue sulla cybersicurezza è in continua evoluzione per rispondere alle nuove minacce, incluse quelle nello spazio. È importante, da parte delle istituzioni europee, un impegno continuativo a collaborare per rafforzare la sicurezza delle infrastrutture spaziali e dei servizi da esse forniti.

Negli ultimi anni l'Ue ha adottato due direttive principali per rafforzare la cybersicurezza in vari settori: la direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva Nis) del 2016 e la direttiva sulla resilienza cibernetica (direttiva Nis2) del 2022, che assumono un ruolo fondamentale nella protezione delle infrastrutture spaziali da attacchi informatici. Entrambe, pur con differenti approcci, mirano a rafforzare la sicurezza informatica in vari settori e a creare una solida strategia per la cybersicurezza dei Paesi membri.

La direttiva Nis2 (che sostituisce la Nis del 2016) segna un significativo passo avanti nel rafforzamento della sicurezza informatica degli Stati membri, amplia l'ambito di applicazione della precedente normativa, impone misure di cybersicurezza più severe per le organizzazioni di vari settori e mira a colmare le carenze delle norme precedenti rendendole più adatte a esigenze attuali e future. A tal fine, la direttiva aggiunge alla precedente nuovi settori in base al loro grado di digitalizzazione e interconnessione e alla loro rilevanza per la società. Nonostante ciò, gli Stati membri hanno la possibilità di individuare entità aggiuntive rispetto ai settori

[63] Rajeswari Pillai Rajagopalan, "Electronic and Cyber Warfare in Outer Space", in *Space Dossiers*, n. 3 (maggio 2019), https://unidir.org/publication/electronic-and-cyber-warfare-in-outer-space.

[64] "Cybersecurity in Outer Space, a Q&A with Ambassador Sorin Ducaru", in *Digital Front Lines*, agosto 2023, https://digitalfrontlines.io/2023/08/23/cybersecurity-in-outer-space.

DOCUMENTI IAI 24 | 07 - LUGLIO 2024
ISSN 2280-6164
© 2024 IAI

delineati che, seppur più piccole, abbiano un elevato rischio per la sicurezza[65]. Da notare come la Nis2 includa lo spazio negli 11 "settori ad alta criticità" per i quali la cybersicurezza rappresenta un fattore chiave per cogliere a pieno i vantaggi della transizione digitale[66].

La Nis2, che abroga la precedente Nis, presenta quindi diverse opportunità per rafforzare la cybersicurezza delle infrastrutture spaziali attraverso standard armonizzati, miglioramento della gestione del rischio e della risposta agli incidenti e maggiore consapevolezza della rilevanza che i servizi spaziali ricoprono per gli Stati membri. L'implementazione della Nis2 nel contesto spaziale presenta alcune sfide, quali: 1) l'elevata complessità tecnica; 2) la necessità di un'ampia collaborazione internazionale; 3) il problema della allocazione delle risorse per finanziare il rispetto di nuovi livelli di sicurezza cibernetica per le infrastrutture spaziali.

Le entità cui si applica la Nis2 sono divise in due categorie sulla base della loro rilevanza: soggetti essenziali e soggetti importanti, che dipenderanno da diversi regimi di vigilanza. Gli enti pubblici e privati designati dagli Stati membri come operatori di servizi essenziali (*operators of essential services*, Oes) devono condurre una valutazione dei rischi legati alla sicurezza informatica e implementare misure di sicurezza adeguate e proporzionate. Inoltre, la Nis2 si occupa della sicurezza delle catene di approvvigionamento e delle relazioni con i fornitori, richiedendo alle singole imprese di gestire i rischi legati alla sicurezza informatica in entrambi gli ambiti. La Nis2 rafforza gli obblighi di segnalazione, i requisiti di risposta agli incidenti e i quadri di vigilanza ed elimina la separazione tra operatori di servizi essenziali e fornitori di servizi digitali, in cui rientrano anche i servizi di gestione dello spazio, ora esplicitata nella distinzione fra enti essenziali ed enti importanti[67].

Oltre alla Nis2, il quadro normativo Ue ha visto la pubblicazione, nel dicembre 2022, della direttiva sulla resilienza dei soggetti critici (direttiva Cer), che rafforza la *governance* della cybersicurezza nell'Ue e introduce misure per la gestione del rischio di incidenti informatici. Così come per la Nis2, il termine utile per l'attuazione della direttiva per i singoli Stati è ottobre 2024 ma, a differenza della prima, la direttiva Cer prevede che gli Stati individuino entro il 17 luglio 2026 i soggetti critici per ogni settore, sottosettore e categoria indicate dalla stessa. Sarà probabilmente proprio il delicato processo di identificazione delle entità critiche a rappresentare la sfida più grande che il nostro Paese dovrà affrontare. Fra questi rientrano anche lo spazio e gli operatori di infrastrutture *ground-based* gestite da Stati membri o da privati che supportano la fornitura di servizi spaziali. Va

[65] Parlamento europeo e Consiglio dell'UE, *Direttiva (UE) 2022/2555 del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione*, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32022L2555.

[66] Ibid., Allegato 1.

[67] Davide Maniscalco, "Strategia di integrazione tra cyber e spazio: il modello di resilienza europea", in *CyberSecurity360*, 28 aprile 2023, https://www.cybersecurity360.it/?p=65171.

© 2024 IAI
ISSN 2280-6164

inoltre evidenziato che le autorità nazionali competenti ai sensi delle direttive Cer e Nis2 dovranno cooperare e scambiarsi periodicamente informazioni pertinenti sui rischi, le minacce e gli incidenti informatici. Il gruppo di lavoro istituito nell'ambito della Nis2 dovrà riunirsi periodicamente ed è stabilito che almeno una volta all'anno convenga con il gruppo per la resilienza delle entità critiche istituito dalla direttiva Cer[68].

2.3 Quadro normativo italiano sulla cybersicurezza

Nell'ultimo decennio l'Italia ha adottato diverse misure normative e ha recepito le principali direttive europee per garantire la cybersicurezza del Paese. Già dal 2013, con la Direttiva sulla protezione cibernetica e la sicurezza informatica[69] il governo si è mostrato proattivo nel proteggere la sicurezza dei propri assetti. Quest'ultima, poi aggiornata con il decreto n. 7 del 2017, si poneva l'obiettivo di "rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali"[70]. Con il decreto legislativo n. 65 del 2018 è stata recepita nell'ordinamento italiano la direttiva Nis e il 24 febbraio 2024 è stata pubblicata nella Gazzetta Ufficiale la legge delega per il recepimento delle Direttive Nis2 e Cer[71]. Come accennato in precedenza, proprio nella Nis2 l'Unione Europea ha identificato lo spazio come un'infrastruttura critica in quanto fattore che contribuisce alla crescita e al funzionamento delle società[72], e quindi la legge delega per il recepimento di tale Direttiva ha un impatto diretto sul settore spaziale.

Nel 2019, è stato istituito il Perimetro di sicurezza cibernetica per garantire la sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale o la fornitura di un servizio essenziale per lo Stato e dal cui malfunzionamento, interruzione, anche parziali o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale[73].

[68] Parlamento europeo e Consiglio dell'UE, *Direttiva (UE) 2022/2557 del 14 dicembre 2022 relativa alla resilienza dei soggetti critici*, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32022L2557.

[69] Presidenza del Consigli dei Ministri, *Decreto del 24 gennaio 2013: Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*, https://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg.

[70] Presidenza del Consigli dei Ministri, *Decreto del 17 febbraio 2017: Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*, https://www.gazzettaufficiale.it/eli/id/2017/04/13/17A02655/sg.

[71] Legge 21 febbraio 2024, n. 15: *Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea*, https://www.gazzettaufficiale.it/eli/id/2024/02/24/24G00027/sg.

[72] Ottavia Credi, "Lo spazio è più vulnerabile agli attacchi cyber", in *AffarInternazionali*, 13 marzo 2023, https://www.affarinternazionali.it/?p=5334.

[73] Sito del Ministero delle Imprese e del Made in Italy: *Perimetro sicurezza cibernetica*, https://atc.mise.gov.it/index.php/sicurezza/perimetro-sicurezza.

© 2024 IAI
ISSN 2280-6164

Fra i soggetti pubblici e privati che rientrano nel Perimetro è compreso anche il settore dello spazio e dell'aerospazio, le cui Amministrazioni competenti sono tenute a compilare un elenco annuale degli assetti considerati strategici per la fornitura di servizi e delle funzioni essenziali. In relazione a tali assetti, è previsto che vengano adottate misure per garantire standard di sicurezza e segnalare eventuali incidenti al Computer Security Incident Response Team (Csirt) operativo presso l'Agenzia per la cybersicurezza nazionale (Acn). Quest'ultima è stata istituita con il decreto n. 82 del 2021[74].

3. Questioni aperte e spunti di riflessione

Gli attacchi rispettivamente nel dominio cyber e nello spazio elettromagnetico sono di per sé minacce impegnative per il funzionamento dei sistemi spaziali, e non sono minacce eludibili. È quindi fondamentale l'adozione di un approccio orientato al *risk management* per adeguare l'infrastruttura spaziale e i servizi a essa legati all'inevitabilità delle minacce e per aumentarne la resilienza.

Attacchi di questo tipo diventano potenzialmente ancora più pericolosi se sferrati insieme in maniera coordinata. Nel prossimo futuro, infatti, l'integrazione di tecnologie elettroniche, elettromagnetiche e cibernetiche, insieme allo sviluppo di armi a energia diretta (*direct energy weapons*), si indirizzerà sempre più verso i sistemi spaziali, con potenziali risvolti sull'intensità della competizione spaziale e delle operazioni militari in orbita[75]. È utile, infatti, vedere le Emso e la guerra cyber come appartenenti a una macrocategoria di azioni chiamate *cyber electromagnetic activities* (Cema) in modo da poter concepire le capacità offensive e difensive nei diversi campi sopracitati come complementari. Le forze armate di alcuni Paesi Nato stanno già agendo per contrastare tali minacce, come negli Stati Uniti dove è in atto un processo evolutivo che vede l'integrazione di capacità *jammer* avanzate con strategie di impiego operativo congiunto di azioni cyber e di Ew[76]. In Russia tali capacità trovano espressione in particolare nel sistema di Ew "Leer-3" che vede l'utilizzo di droni in grado di bloccare le comunicazioni in porzioni di territorio e inviare false informazioni[77].

[74] Sull'istituzione di Acn e Perimetro si veda tra gli altri: 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.

[75] Ottavia Credi, Giancarlo La Rocca e Alessandro Marrone, "Il dominio spaziale e la minaccia cyber", cit.

[76] 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, http://breakingdefense.com/?p=39684; Catherine A. Theohary, "Convergence of Cyberspace Operations and Electronic Warfare", in *CRS In Focus*, n. IF11292 (13 agosto 2019), https://crsreports.congress.gov/product/details?prodcode=IF11292.

[77] 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/?p=12453.

© 2024 IAI
ISSN 2280-6164

In tale contesto risulta dunque potenzialmente vantaggioso plasmare le strutture di comando rilevanti, come quelle legate alle attività di Ew, cyber sicurezza/difesa, SigInt e *Communication Intelligence* (ComInt), di modo da non creare separazioni artificiali, anche in termini normativi, tra l'impiego di strumenti complementari tra loro e che spesso hanno obiettivi simili dal punto di vista operativo[78].

La resilienza dei sistemi spaziali di fronte a minacce cyber e nello spazio elettromagnetico si raggiunge con un approccio olistico che guarda sì alla componente tecnologica, ma anche a quella umana, ovvero dedicando particolare attenzione alla formazione del personale sia in un'ottica di capacità di innovazione, in fase di progettazione e aggiornamento dei sistemi, sia di comunicazione di rischi e vulnerabilità al personale che opera quotidianamente su questi sistemi[79]. Allo stesso tempo è fondamentale che a livello nazionale continui sistematicamente lo studio delle minacce così da poterle anticipare e contrastare al meglio prima che arrechino gravi danni all'infrastruttura spaziale[80]. In assenza di una strategia nazionale che definisca in modo chiaro il ruolo in questo ambito non solo dell'intelligence e dell'Acn, ma anche delle forze armate, il sistema paese non potrà beneficiare di strumenti già esistenti se non in maniere frammentata. Tale mancanza rischia di avere riscontri negativi anche sull'abilità del settore di sfruttare al meglio le competenze e i talenti che in Italia scarseggiano. Si dovrebbero inoltre sviluppare ulteriormente le sinergie con l'industria nazionale in modo da favorire un approccio alle operazioni, ma anche alla ricerca e allo sviluppo, che sia quanto più collaborativo.

La Difesa italiana è fra le poche in occidente che affida gran parte della gestione operativa dei propri assetti spaziali a personale militare, appoggiandosi all'industria in un ruolo di supporto, manutenzione e aggiornamento dopo l'acquisizione[81]. Questa configurazione è evidente guardando al Centro Interforze di Gestione e Controllo (Cigc) Sicral di Vigna di Valle, che gestisce le attività di SatCom e il controllo in orbita dei satelliti[82]. Se da una parte tale approccio richiede uno sforzo considerevole da parte della Difesa, dall'altra la arricchisce di competenze tecniche che possono migliorare significativamente la capacità militare di fissare requisiti per i sistemi spaziali e di lavorare con l'industria per soddisfarli al meglio. Anche per questo risulta quanto mai essenziale l'abilità delle forze armate di individuare, attirare, formare e mantenere in servizio profili idonei così da poter contare su personale adatto per definire requisiti operativi e operare in questo dominio in modo sempre più sostenibile.

78 Intervista, 19 febbraio 2024.
79 Ibid.
80 Ibid.
81 Intervista, 5 marzo 2024.
82 Sito del Ministero della Difesa: *I reparti*, https://www.difesa.it/smd/covi/cos/reparti/25437.html.

DOCUMENTI IAI 24 | 07 - LUGLIO 2024 ISSN 2280-6164 © 2024 IAI

Al di là di un inderogabile processo che porti a maggiore cooperazione a livello europeo sulla resilienza dei sistemi spaziali, come delineato dalla Strategia spaziale per la sicurezza e la difesa[83], l'Italia e i partner europei devono raggiungere dove possibile una sovranità tecnologica lungo tutta la catena di approvvigionamento per contare in modo incrementale sulle tecnologie più avanzate per rafforzare la sicurezza e resilienza dei propri sistemi spaziali. Nel contesto delle minacce cyber questo richiede uno sforzo notevole nello sviluppo di quelle tecnologie dirompenti, come l'intelligenza artificiale e il *quantum computing*, che possono aiutare i sistemi spaziali a rispondere velocemente ed efficacemente ad attacchi cyber quando ad esempio l'input dell'operatore umano viene interrotto da operazioni di Ew. La dipendenza da fornitori lontani per la componentistica informatica presenta inoltre una grossa vulnerabilità se mal gestita, come dimostrato dal "Big Hack" del 2018 dove un attacco pianificato da attori ostili ha compromesso la sicurezza di decine di aziende ed entità governative statunitensi. L'importanza del corretto e indisturbato funzionamento dei sistemi spaziali esige che si possa contare sull'integrità delle forniture estere dove queste risultano essere inevitabili. È perciò fondamentale che la base industriale europea riesca a consolidare gli investimenti, attualmente frammentati, verso una comunità d'intenti volta al raggiungimento di un più alto livello di autonomia tecnologica – a partire da chip e componentistica informatica. Questo approccio deve anche andare oltre alla semplice componentistica e interessare i codici sorgente e gli algoritmi di prodotti importati, assicurandone il controllo e la gestione.

La vocazione duale di un gran numero di sistemi spaziali fa sì che tutti, anche quelli destinati principalmente a uso civile, debbano puntare a rispettare norme di sicurezza chiare e frequentemente aggiornate per far fronte a minacce emergenti e in continua evoluzione. Se per quel che riguarda le minacce cyber i sistemi spaziali possono contare su un certo livello, sebbene ancora insufficiente[84], di copertura normativa attraverso misure europee come la Nis2, la situazione è diversa nel caso delle minacce nello spettro elettromagnetico, dove invece vi è una grossa lacuna e la resilienza resta a discrezione perlopiù dell'industria e degli operatori che fissano i requisiti. Questo vuoto andrebbe colmato al più presto da normative europee basate sul concetto di *security-by-design*, con l'obiettivo di rendere anche le infrastrutture a uso civile, ma essenziali per il funzionamento delle nostre società, più sicure e resilienti fin dallo stadio della progettazione.

Nonostante il perseguimento di trattati internazionali che regolino il comportamento degli attori spaziali nello spazio oltre ai vecchi regimi come l'Ost resti una politica rilevante, non si può non prendere atto del fatto che, in un clima di sempre crescente competizione globale, diversi attori potenzialmente ostili

[83] 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.

[84] Ottavia Credi, Giancarlo La Rocca e Alessandro Marrone, "Il dominio spaziale e la minaccia cyber", cit.

DOCUMENTI IAI 24 | 07 - LUGLIO 2024 ISSN 2280-6164
© 2024 IAI

verso l'Europa si siano dotati di capacità *counter-space* e che siano disposti a usarle. Da tale consapevolezza dovrebbe scaturire una riflessione sull'esigenza di sviluppare in Europa capacità offensive non-cinetiche in un'ottica di deterrenza che troppo spesso risulta controversa, al di là di Stati Uniti e pochi altri Paesi Nato come Francia e Regno Unito. Qualsiasi nuova contromisura volta alla resilienza dei sistemi verrà inevitabilmente superata da nuove ed evolute capacità offensive da parte dell'avversario; ciò significa che la prevenzione, da sola, non può essere sufficiente a proteggere i sistemi più essenziali e strategici da attacchi nella zona grigia tra pace e guerra. Un deterrente credibile nel dominio spaziale, come d'altronde in quello cyber, richiede che l'avversario sia obbligato a misurare il potenziale guadagno di un attacco del genere confrontandolo con le possibili conseguenze di una risposta adeguata da parte di chi lo subisce.

aggiornato 9 luglio 2024

© 2024 IAI
ISSN 2280-6164

Riferimenti

Massimo Annulli, "Spoofing in Radar ECM", in *Emsopedia*, 23 March 2021, https://www.emsopedia.org/?p=765

Brandon Bailey, "Protecting Space Systems from Cyber Attack", in *Aerospace TechBlog*, 31 marzo 2022, https://medium.com/the-aerospace-corporation/protecting-space-systems-from-cyber-attack-3db773aff368

Marco Battaglia, "Starlink batte il jamming russo e dà lezioni al Pentagono", in *Formiche*, 21 aprile 2022, https://formiche.net/?p=1468293

Kari A. Bingen, Kaitlyn Johnson e Zhanna Malekos Smith, "Russia Threatens to Target Commercial Satellites", in *CSIS Critical Questions*, 10 novembre 2022, https://www.csis.org/node/67711

Katie Bo Lillis et al., "Exclusive: Russia Attempting to Develop Nuclear Space Weapon to Destroy Satellites with Massive Energy Wave, Sources Familiar with Intel Say", in *CNN*, 17 febbraio 2024, https://edition.cnn.com/2024/02/16/politics/russia-nuclear-space-weapon-intelligence/index.html

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

Ottavia Credi, "Lo spazio è più vulnerabile agli attacchi cyber", in *AffarInternazionali*, 13 marzo 2023, https://www.affarinternazionali.it/?p=5334

Ottavia Credi, Giancarlo La Rocca e Alessandro Marrone, "Il dominio spaziale e la minaccia cyber", in *Documenti IAI*, n. 23|06 (marzo 2023), https://www.iai.it/it/node/16806

Ottavia Credi e Maria Vittoria Massarin, "L'Italia nello spazio: collaborazioni e prospettive future", in *Documenti IAI*, n. 23|21 (novembre 2023), https://www.iai.it/it/node/17753

Dan De Luce, "Russia 'Spoofing' GPS on Vast Scale to Stop Drones from Approaching Putin, Report Says", in *NBC News*, 26 marzo 2019, https://www.nbcnews.com/news/n987376

Antonio De Maio, "Global Navigation Satellite System GNSS Spoofing", in *Emsopedia*, 23 marzo 2021, https://www.emsopedia.org/?p=2279

Sandra Erwin, "Slingshot Aereospace Harnessing AI to Track Suspicious Satellites", in *SpaceNews*, 6 ottobre 2023, https://spacenews.com/?p=192876

© 2024 IAI

ISSN 2280-6164

Euroconsult, *Value of Space Economy Reaches $464 Billion in 2022 Despite New Unforeseen Investment Concerns*, 9 January 2023, https://www.euroconsult-ec.com/?p=13695

Sydney J. Freedberg Jr., "Russian Robots: Fear Jammers, Not Terminators", in *Breaking Defense*, 5 ottobre 2017, http://breakingdefense.com/?p=39684

Enrico Frumento, "Quantum Key Distribution: cos'è e perché è utile a rendere inattaccabili i sistemi di cifratura", in *Cybersecurity360*, 23 giugno 2022, https://www.cybersecurity360.it/?p=55479

Emanuele Galtieri, "Il business nell'era del cyber-spazio", in *Formiche*, 2 febbraio 2023, https://formiche.net/?p=1530210

Chris Gordon, "Cybersecurity Is the 'Soft Underbelly' of Space Operations, SpOC Comander Says", in *Air & Space Forces Magazine*, 14 ottobre 2022, https://www.airandspaceforces.com/?p=171742

Greg Hadley, "'Backdoor' to Attack Satellites: CSO Sees Cyber Risks in Space Force Ground Systems", in *Air & Space Forces Magazine*, 31 gennaio 2023, https://www.airandspaceforces.com/?p=181062

Unshin Lee Harpley, "Space Force CTIO: AI Will Be 'Game-Changer' for Operational Space", in *Air & Space Forces Magazine*, 14 novembre 2023, https://www.airandspaceforces.com/?p=209126

Todd Harrison et al., "Space Threat Assessment 2020", in *CSIS Reports*, marzo 2020, https://www.csis.org/node/56019

Theresa Hitchens, "GEOST Sensors to Detect Interference Will Fly on SDA Satellites", in *Breaking Defense*, 13 settembre 2023, https://breakingdefense.com/?p=308418

John R. Hoehn, Jill C. Gallagher e Kelley M. Sayler, "Overview of Department of Defense Use of the Electromagnetic Spectrum", in *CRS Reports*, n. R46564 (10 agosto 2021), https://crsreports.congress.gov/product/details?prodcode=R46564

ID Quantique, "Quantum Cyber Security for Satellites", in *IDQ*, 7 marzo 2023, https://www.idquantique.com/?p=34178

Valerie Insinna, "SpaceX Beating Russian Jamming Attack Was 'Eyewatering': DoD Official", in *Breaking Defense*, 20 aprile 2022, http://breakingdefense.com/?p=218133

Zixiang Jia, "Anti-jamming Technology in Small Satellite Communication", in *Journal of Physics: Conference Series*, Vol. 960 (2018), Art. 012013, https://doi.org/10.1088/1742-6596/960/1/012013

© 2024 IAI

ISSN 2280-6164

Steve Kates, "The Era of Space Warfare and the Growing Threat of EMP", in *KTARNews*, 18 agosto 2021, https://ktar.com/story/4639134

Jeffrey Kluger, "Scientists Sound the Alarm over a Growing Trash Problem in Space", in *Time*, 13 marzo 2023, https://time.com/6262389/space-junk-increasing-problem

Legge 21 febbraio 2024, n. 15: *Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea*, https://www.gazzettaufficiale.it/eli/id/2024/02/24/24G00027/sg

Dylan Malyasov, "In Syria Spotted New Russian RB-341V 'Leer-3' Electronic Warfare System", in *Defence Blog*, 14 marzo 2016, https://defence-blog.com/?p=12453

Davide Maniscalco, "Strategia di integrazione tra cyber e spazio: il modello di resilienza europea", in *CyberSecurity360*, 28 aprile 2023, https://www.cybersecurity360.it/?p=65171

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

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

Joseph Menn, "Cyberattack Knocks Out Satellite Communications for Russian Military", in *The Washington* Post, 30 giugno 2023, https://www.washingtonpost.com/technology/2023/06/30/satellite-hacked-russian-military

Matthew Mowthorpe, "Space Resilience and the Importance of Multiple Orbits", in *The Space Review*, 3 gennaio 2023, https://www.thespacereview.com/article/4504/1

Organizzazione per la cooperazione e lo sviluppo economico, *OECD Handbook on Measuring the Space Economy*, Parigi, OECD Publishing, 2012, https://doi.org/10.1787/9789264169166-en

Parlamento europeo e Consiglio dell'UE, *Direttiva (UE) 2022/2555 del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione*, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32022L2555

Parlamento europeo e Consiglio dell'UE, *Direttiva (UE) 2022/2557 del 14 dicembre 2022 relativa alla resilienza dei soggetti critici*, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32022L2557

Teona Patussi, *Space Warfare and the Weaponization of Outer Space*, tesi Charles University di Praga, agosto 2022, http://hdl.handle.net/20.500.11956/178403

© 2024 IAI

ISSN 2280-6164

Walter Peeters, "Cyberattacks on Satellites: An Understimated Political Threat", in *LSE IDEAS Space Policy Publications*, 5 maggio 2022, https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites

Rajeswari Pillai Rajagopalan, "A Consequence-based Approach Is Needed for Space Security", in *The Diplomat*, 19 ottobre 2023, https://thediplomat.com/2023/10/a-consequence-based-approach-is-needed-for-space-security

Rajeswari Pillai Rajagopalan, "Electronic and Cyber Warfare in Outer Space", in *Space Dossiers*, n. 3 (maggio 2019), https://unidir.org/publication/electronic-and-cyber-warfare-in-outer-space

Kevin Poireault, "Five Takeaways from the Russian Cyber-Attack on Viasat's Satellites", in *Infosecurity Magazine*, 9 maggio 2023, https://www.infosecurity-magazine.com/news/takeaways-russian-cyberattack

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

Presidenza del Consigli dei Ministri, *Decreto del 24 gennaio 2013: Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*, https://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg

Presidenza del Consigli dei Ministri, *Decreto del 17 febbraio 2017: Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*, https://www.gazzettaufficiale.it/eli/id/2017/04/13/17A02655/sg

Peter Vincent Pry, *Russia: EMP Threat. The Russian Federation's Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack*, gennaio 2021, https://apps.dtic.mil/sti/citations/AD1124730

Frederick Rawlins, Richard Baker e Ivan Martinovic, *Death by a Thousand COTS: Disrupting Satellite Communications Using Low Earth Orbit Constellations*, paper presentato al Workshop on Security of Space and Satellite Systems (SpaceSec) 2023, San Diego, 27 febbraio 2023, https://doi.org/10.14722/spacesec.2023.233980

Jordan Robertson e Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies", in *Bloomberg*, 4 ottobre 2018, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Giuseppe Sgamba, "Electro Magnetic Spectrum Operation (EMSO)", in *Emsopedia*, 24 marzo 2021, https://www.emsopedia.org/?p=1076

© 2024 IAI

ISSN 2280-6164

Gaurav Thakur, "What Is GPS Spoofing That Has Misguided Around 20 Planes Near Iran-Iraq Border and How Dangerous Is This", in *Deccan Herald*, 1 ottobre 2023, https://www.deccanherald.com/2708342

Catherine A. Theohary, "Convergence of Cyberspace Operations and Electronic Warfare", in *CRS In Focus*, n. IF11292 (13 agosto 2019), https://crsreports.congress.gov/product/details?prodcode=IF11292

John Thornhill, "A Global Satellite Blackout Is a Real Threat — Can Hackers Help?", in *Financial Times*, 8 giugno 2023, https://www.ft.com/content/d5df1e81-f126-4a48-9a42-5b4aca842dcb

Brooks Tigner, "Electronic Jamming between Russia and NATO Is Par for the Course in the Future, But It Has Its Risky Limits", in *New Atlanticist*, 15 novembre 2018, https://www.atlanticcouncil.org/?p=113248

Greg Torode, "China's Efforts to Catch Up in Global Electronic Spying Race", in *Reuters*, 14 giugno 2023, https://www.reuters.com/world/china/chinas-efforts-catch-up-global-electronic-spying-race-2023-06-14

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, 1966, https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html

University of Texas at Austin, "UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea", in *UT News*, 29 luglio 2013, https://news.utexas.edu/?p=2116

US Air Force, *Electromagnetic Spectrum Operations*, Air Force Doctrine Publication 3-85, 14 dicembre 2023, https://www.doctrine.af.mil/Operational-Level-Doctrine/AFDP-3-85-Electromagnetic-Spectrum-Operations

US Joint Chiefs of Staff, *Joint Electromagnetic Spectrum Operations*, Joint Publication 3-85, 22 maggio 2022, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf

Tyler Way, "Counterspace Weapons 101", in *Aereospace Security*, aggiornato al 14 giugno 2022, https://aerospace.csis.org/aerospace101/counterspace-weapons-101

© 2024 IAI

ISSN 2280-6164

Lista degli acronimi

5G	Quinta generazione
Acn	Agenzia per la cybersicurezza nazionale
Cema	Cyber Electromagnetic Activities
ComInt	Communication intelligence
Csirt	Computer Security Incident Response Team
DoS	Denial of Service
Eccm	Electronic Counter-Countermeasures
Eme	Electromagnetic Environment
Emp	Electromagnetic Pulse
Ems	Electromagnetic Space
Emso	Electromagnetic Spectrum Operations
Eo	Earth Observation
Gps	Global Positioning System
Isr	Intelligence, Surveillance and Reconnaissance
Nato	North Atlantic Treaty Organization
Nis	Network and Information Security
Nis2	Network and Information Security 2
Oes	Operators of Essential Services
Ost	Outer Space Treaty
Prs	Public Regulated Service
Qkd	Quantum Key Distribution
Rf	Radiofrequenza
SatCom	Satellite Communications
SigInt	Signal Intelligence
Ue	Unione europea
Vpn	Virtual Private Network

© 2024 IAI
ISSN 2280-6164

© 2024 IAI

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 (*Trends and Perspectives in International Politics* 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)