#06

ICT Security MAGAZINE

SPACE SECURITY

PREFAZIONE DI

GEN. C.A. FRANCO FEDERICI

Consigliere Militare del Presidente del Consiglio dei Ministri

2024

QUADERNI DI CYBER INTELLIGENCE

WWW.ICTSECURITYMAGAZINE.COM

WWW.SOCINT.ORG

FORUM ICT SECURITY

23-24 OTTOBRE 2024

AUDITORIUM DELLA TECNICA, ROMA

Iscriviti alla newsletter di ICT Security Magazine
per conoscere l'agenda e partecipare alla
22ª Edizione del Forum ICT Security

ICT Security MAGAZINE

ICT SECURITY MAGAZINE

1° rivista italiana di sicurezza informatica, attiva da oltre 20 anni, dedicata in forma esclusiva alla cyber security e alla business continuity, si pone l'obiettivo di coinvolgere i più importanti attori del settore, aziende e istituzioni pubbliche, per la diffusione degli elementi conoscitivi legati a tutti gli aspetti della information security.

SOCIETÀ ITALIANA DI INTELLIGENCE

SOCINT è un'associazione scientifica senza fini di lucro, il cui obiettivo è quello di promuovere la cultura e lo studio dell'intelligence in Italia.

QUADERNI DI CYBER INTELLIGENCE

La presente collana, frutto della collaborazione tra ICT Security Magazine e la Società Italiana di Intelligence (SOCINT), inaugura una serie di contenuti volti ad arricchire e approfondire il dibattito scientifico sulla Cyber Intelligence.

Indice

PREFAZIONE

Fino alla fine dello scorso decennio, lo spazio è stato percepito come una sorta di "santuario" rispetto alle dinamiche più o meno violente osservate negli altri ambienti operativi.

Tale visione dell'ambiente spaziale ha influenzato le politiche dei governi, determinando un duplice effetto: se da un lato ha favorito la nascita di virtuosi programmi di cooperazione internazionale nel settore della scienza e dell'esplorazione, nonché di una fiorente economia dello spazio, dall'altro ha portato alla sottovalutazione della dimensione di sicurezza delle attività spaziali, percepita più come un limite allo sviluppo di un mercato commerciale che come una reale esigenza.

Oggi, complice un contesto di crescenti tensioni internazionali, tale percezione è destinata a tramontare. La libertà di accesso e di uso dello spazio, divenuto oramai risorsa imprescindibile per il funzionamento efficiente e ininterrotto di ogni settore della società, risultano seriamente minacciate da numerosi fattori di rischio.

Numerosi eventi di cronaca testimoniano, infatti, come i satelliti siano ormai soggetti ad una molteplicità di attività ostili con caratteristiche e livelli di intensità estremamente variabili.

In particolare, in un contesto globale dove la guerra ibrida diventa sempre più diffusa, l'e-

levato livello di digitalizzazione e di dipendenza dallo spettro elettromagnetico rende i sistemi spaziali particolarmente suscettibili ad azioni di tipo cibernetico e di Guerra Elettromagnetica (GE).

Dal 2014, la segnalazione di incidenti legati all'impiego di misure di GE e cyber a danno di infrastrutture spaziali, anche quelle destinate ad uso civile, è stata persistente soprattutto nei territori della Federazione Russa, della Crimea, dell'Ucraina orientale e della Siria. Fattori quali la facilità di accesso, l'economicità, la flessibilità in termini di impiego e di effetti generabili, non ultima la possibilità di ottenere effetti transitori in luogo di conseguenze di lungo termine associate all'impiego di azioni cinetiche, come la creazione di detriti spaziali, inducono a ritenere che tali azioni di GE e cyber di origine terrestre continueranno a intensificarsi ed evolversi in una prospettiva di sempre maggiore convergenza, sincronizzazione e complementarietà, come peraltro già avviene in parte oggi nel caso di attività di spoofing a danno dei sistemi globali di navigazione satellitare.

Questo tipo di sviluppo è favorito anche dal vantaggio asimmetrico offerto da tali soluzioni di "soft-kill": le quali, sfruttando l'esposizione pressoché globale dei satelliti rispetto a potenziali minacce terrestri come conseguenza del loro orbitare attorno alla Terra, consentono di disporre di una credibile capacità anti-satellite anche a Stati senza particolari ambizioni di proiezione di potenza.

Nel caso della minaccia cyber – oltre ai rischi per i satelliti, le stazioni di controllo a terra e i data link di interconnessione tra i vari segmenti dell'infrastruttura spaziale – è necessario fare i conti con il nuovo e rilevante fattore di rischio legato alla catena di approvvigionamento (c.d. supply chain). I sistemi spaziali presentano infatti vulnerabilità dovute all'estrema interconnessione dell'ecosistema industriale e alla mancanza di uniformità, in termini di standard di sicurezza cibernetica, tra i vari operatori che compongono la supply chain.

Tale condizione rende i sistemi spaziali, soprattutto quelli commerciali, particolarmente suscettibili alla minaccia cyber durante le fasi di produzione e assemblaggio.

In aggiunta alla minaccia terrestre, rappresentata dagli attacchi informatici ed elettromagnetici, la sicurezza dei sistemi spaziali è oggi minacciata da un nuovo fenomeno noto come "weaponization of outer space", inteso come il dispiegamento e l'uso di armi nello spazio. Indicativo, in tal senso, il recente allarme lanciato dal governo statunitense circa un possibile dispiegamento da parte della Russia di un'arma nucleare antisatellite nello spazio.

La tecnologia associata ad armamenti anti-

satellite di tipo space-based continuerà verosimilmente a rappresentare, nel prossimo futuro, una preoccupazione emergente piuttosto che un reale fattore di minaccia. Il vantaggio operativo derivante dalla distruzione di un satellite nello spazio mediante soluzioni "hard-kill" potrebbe, infatti, non risultare sufficientemente pagante nella misura in cui questo tipo di azione può essere più facilmente attribuibile e la stessa capacità di operare nello spazio di chi la perpetra sarebbe messa a rischio a causa degli effetti generati (detriti spaziali), andando pertanto a configurare una sorta di deterrenza esistenziale.

La sicurezza e la resilienza delle infrastrutture spaziali nazionali costituiscono una questione indifferibile, multisettoriale e globale che necessita di un approccio sistemico che guardi sì alla componente tecnologica (es. capacità di apprezzamento della situazione del dominio spaziale e capacità di condurre operazioni spaziali di difesa attiva e passiva) ma anche a una dimensione regolamentare, di governance e umana. In tale prospettiva risulta fondamentale che a livello nazionale si continui a lavorare per l'adozione di una "legge quadro spaziale", quale imprescindibile strumento di supporto alla sostenibilità e alla sicurezza delle attività spaziali.

Altrettanto fondamentale è l'aspetto relativo all'adeguamento della governance, sia in termini di organismi di policy che di organizzazioni/strutture deputate alle attività di supporto informativo (Space Intelligence e Cyber Intelligence), di implementazione delle misure discendenti dall'adozione delle direttive europee CER e NIS2 e di attivazione dei meccanismi di protezione e risposta in caso di attacco alle infrastrutture spaziali nazionali.

Al di là di un inderogabile processo che porti a una maggiore cooperazione a livello europeo in materia di sicurezza e resilienza dei sistemi spaziali, in linea con quanto delineato dalla recente Strategia spaziale per la sicurezza e la difesa dell'UE, l'Italia e i partner europei dovranno perseguire – dove possibile – una sovranità tecnologica lungo l'intera catena di approvvigionamento, valorizzando il contributo delle tecnologie emergenti e dirompenti (es. Intelligenza Artificiale, computazione quantistica, ecc.) quali strumenti per rafforzare ulteriormente la sicurezza e la resilienza delle infrastrutture spaziali sia lungo la supply chain che lungo l'intera catena delle operazioni, dal lancio fino all'erogazione/sfruttamento dei relativi servizi.

Gen. C.A. Franco Federici, *Consigliere Militare del Presidente del Consiglio dei Ministri*

BIOGRAFIA

Gen. C.A. Franco Federici

Il Generale di Corpo d'Armata Franco FEDERICI è nato a Tolmezzo (UD) nel 1965.

Entrato in Accademia a Modena nel 1984 per la frequenza del 166° Corso, ne è uscito con il grado di sottotenente nel 1986, conseguendo, nel 1988, al termine dell'iter formativo presso la Scuola di Applicazione di Torino, la laurea in Scienze Strategiche.

Nel 1988, viene assegnato, quale Cte di plotone alpini, al battaglione alpini "Morbegno" in Vipiteno (BZ), inquadrato nella disciolta Brigata Alpina "Orobica". Tra il 1989 e il 1995, ha espletato le funzioni di Comandante di compagnia alpini presso il 5° rgt. alp. e il 8° rgt.alp). Durante questo periodo, ha conseguito le qualifiche di istruttore militare di sci e di alpinismo e di combattimento in montana.

Dal 1995 al 1997, ha comandato, presso l'Accademia Militare di Modena, la 1^ compagnia allievi del 175° Corso. Dopo aver frequentato il Corso di Stato Maggiore, nel 1997, è stato assegnato all'Ufficio Piani del

Comando del 4° Corpo d'Armata Alpino prendendo parte alla missione NATO in Bosnia con la Multinational Brigade North in Sarajevo, in qualità di Capo Cellula Piani.

Dal 1998 al 2000, ha frequentato il Joint War College in Germania (Führungsakademie del Bundeswehr in Amburgo).

Con la promozione al grado di Maggiore, nel 2001, viene assegnato alla Divisione J5 Piani del Comando Operativo di Vertice Interforze (COI) di Roma.

Dopo aver comandato, nel grado di Tenente Colonnello, il battaglione Alpini "L'Aquila" tra il 2003 e il 2004, è stato nuovamente assegnato alla Divisione Piani del COI di ROMA.

Nel 2007, ha prestato servizio presso il Dipartimento delle operazioni di Peacekeeping dell'ONU, quale Ufficiale di Staff, presso la Cellula di Strategia Militare di UNIFIL (United Nations Interim Force in Lebanon) a New York.

Nel 2009, ha assunto il Comando del 9° rgt. alp. in L'Aquila e viene dispiegato, tra aprile e ottobre 2010, quale Cte della Task Force South (Regional Command West) a Farah in Afghanistan, nell'ambito dell'Operazione ISAF.

Tra il novembre 2010 e il settembre 2014, presta nuovamente servizio presso il COI, quale Capo Divisione J5 Piani.

Promosso Generale di Brigata, viene assegnato allo Stato Maggiore dell'Esercito quale Vice Capo Reparto Impiego delle Forze / Capo Area Operazioni.

Nel marzo 2015, assume il Comando della Brigata Alpina "Taurinense" e viene dispiegato in Libano quale Cte del Settore Ovest nell'ambito della missione UNIFIL.

Nel 2016, assume l'incarico di Capo del III Reparto Pianificazione Generale dello Stato Maggiore dell'Esercito. Il 01 gennaio 2018, viene promosso Generale di Divisione. Nello stesso anno, frequenta il Generals', Flag Officers' and Ambassadors' Course presso il Nato Defence College in Roma.

Dal 4 marzo 2019, è trasferito presso il Comando Operativo di Vertice Interforze, e svolge gli incarichi di Capo Reparto Operazioni e, successivamente, di Capo Reparto Supporto Operativo.

Dal 16 novembre 2020 al 15 ottobre 2021, assume il Comando della KOSOVO FORCE nell'ambito dell'Operazione NATO "Joint Enterprise". Al suo rientro in Patria, ricopre l'incarico di Vice Comandante delle Forze Operative Terrestri e Comando Operativo Esercito, e contestualmente è nominato Presidente della Commissione di Valutazione per l'Avanzamento dei Marescialli.

Il 01 dicembre 2022 è nominato Consigliere Militare del Presidente del Consiglio dei Ministri, e il 01 gennaio 2023 viene promosso Generale di Corpo d'Armata.

Ha conseguito la Laurea in Scienze strategiche, con relativo Master, presso l'Università degli Studi di Torino. Parla inglese e tedesco.
In conseguenza del servizio prestato è stato insignito delle seguenti onorificenze:

- Cavaliere dell'Ordine Militare d'Italia (OMI);
- Croce d'Oro al Valore dell'Esercito;
- Croce d'Argento al Valore dell'Esercito;
- Cavaliere dell'Ordine al Merito della Repubblica Italiana;
- Medaglia Mauriziana al Merito di 10 lustri di Carriera Miliare;
- Medaglia al merito di lungo comando (20 anni);
- Ufficiale Generale della Legion of Merit degli Stati Uniti d'America;
- Médaille de la Dèfence Nationale della Repubblica Francese;
- The Presidential Military Medal del Presidente della Repubblica del Kosovo;
- Medal for International Cooperation del Ministro della Difesa Sloveno;
- Honor Medal dello Stato Maggiore della Difesa Ungherese;
- Emblem of Honor of Defence Staff dello Stato Maggiore della Difesa Rumena.

Il Generale Franco FEDERICI è sposato con la signora Monika e ha un figlio, Marco.

INTRODUZIONE

Siamo orgogliosi di presentarvi la sesta edizione del nostro quaderno tematico, coronamento di un anno ricco di successi

In questa occasione, la Commissione Cyber Threat Intelligence e Cyber Warfare (di seguito Commissione), parte integrante della SOCINT (Società Italiana di Intelligence), ha deciso di esplorare il tema della Sicurezza Spaziale o *"Space Security"*, un argomento che continua a catturare grande interesse per la sua complessità e rilevanza strategica a livello sia nazionale sia internazionale.

L'approccio adottato è altamente multidisciplinare, mirato ad affrontare la complessità del tema della Space Security da ogni angolazione: giuridica, tecnica – nell'ambito della Space Cyber Threat Intelligence – e tecnologica, con particolare attenzione alla convergenza tra sistemi terrestri e spaziali. Il nostro obiettivo è comprendere in profondità le dinamiche, i rischi e le conseguenze dell'applicazione di varie metodologie di sicurezza, affrontando le sfide che emergono nei diversi contesti operativi.

Arthur C. Clarke affermava: *«La terra è la culla dell'umanità, ma non si può vivere per sempre in una culla»*.

È fondamentale analizzare come l'interconnessione tra i vari sistemi spaziali abbia aumentato i rischi di attacchi cibernetici, influenzando notevolmente il rapporto tra costi e benefici. Questa crescente inter-

connessione, pur portando innovazione e progresso, ha esposto i sistemi spaziali a nuove vulnerabilità, richiedendo una gestione attenta e strategica per mitigare i rischi associati e garantire la sicurezza delle operazioni spaziali.

Il tema si è quindi spostato sulla complessità da gestire, intesa sia dal punto di vista dell'interconnessione dei sistemi terrestri e spaziali, sia dal punto di vista della geopolitica spaziale. Per poter comprendere come gestire tale complessità dobbiamo, a mio avviso, scomporre il problema in due grandi temi: la gestione della *supply chain* relativa ai sistemi terra/spazio e gli aspetti di *cyber diplomacy* legati alla tematica spaziale.

La gestione delle *supply chain* riguarda principalmente il monitoraggio e il controllo dei fornitori per ridurre il rischio cibernetico associato. È essenziale mantenere un controllo costante su chi possiede e gestisce le tecnologie, considerando che spesso tali tecnologie non sono fornite né sviluppate interamente a livello nazionale. Questo solleva la questione cruciale della sovranità nazionale in ambito tecnologico, richiedendo una *governance* efficace delle tecnologie per garantire la sicurezza e l'integrità delle infrastrutture spaziali.

Tuttavia, un efficace coordinamento a livello europeo è cruciale per affrontare queste sfide. La *cyber diplomacy* può giocare un ruolo fondamentale nel favorire una cooperazione più stretta tra i paesi membri, assicurando che le strategie di aggiornamento e gestione delle tecnologie spaziali siano allineate, riducendo così i rischi associati all'obsolescenza e migliorando la resilienza collettiva.

Negli ultimi 15 anni, l'integrazione tra mondo spaziale e cyber ci ha permesso di comprendere come le informazioni *"Cyber Threats"*, intese come vulnerabilità dei sistemi di comunicazione e dei satelliti, sono di fondamentale importanza per le organizzazioni. Senza tali informazioni, le organizzazioni si ritroverebbero sguarnite in termini di protezione, compromettendo la loro competitività nel mercato globale.

John F. Kennedy affermava: *«Scegliamo di andare sulla Luna non perché è facile, ma perché è difficile»*. Allo stesso modo, affrontare le sfide della sicurezza spaziale richiede un impegno deciso e strategico.

In questo contesto, la *Cyber Threat Intelligence* emerge come un elemento cruciale. La raccolta informativa sulle minacce cibernetiche e la comprensione delle vulnerabilità dei sistemi spaziali sono essenziali per prevenire attacchi e rafforzare le difese, specialmente in un contesto di *cyber warfare*.

La *Space Intelligence*, intesa come componente tecnologica, ha certamente supportato il settore pubblico e privato nella previsione e prevenzione dei rischi.

Purtroppo, ad oggi, non ha garantito un adeguato livello di ritorno sugli investimenti (ROI), rappresentando una sfida costante per le aziende del settore spaziale. Aziende come Thales Alenia Space e Avio Aerospace, contributori di questo quaderno tematico, si trovano quotidianamente ad affrontare questa problematica, cercando soluzioni innovative per dare maggiore impulso al settore e migliorare la sostenibilità economica delle loro attività nel campo della sicurezza spaziale.

Concludiamo parafrasando la famosa frase di **Star Trek**: *"Spazio: ultima frontiera. Questi sono i viaggi della nave stellare Enterprise. La sua missione quinquennale: esplorare strani, nuovi mondi, cercare nuove forme di vita e nuove civiltà, arrivare coraggiosamente là dove nessun uomo è mai giunto prima."*

Allo stesso modo, la nostra missione nel campo della sicurezza spaziale è esplorare nuovi orizzonti, sviluppare soluzioni innovative e garantire la protezione delle nostre risorse spaziali, arrivando coraggiosamente là dove nessuno è mai giunto prima in termini di sicurezza e resilienza.

Mattia Siciliano, *Presidente Commissione Studi Cyber Threat Intelligence & Cyber Warfare*

BIOGRAFIA

Mattia Siciliano

L'ing. Siciliano ha oltre 15 anni di esperienza in Cyber Security e Cyber Intelligence. Attualmente è Co-Direttore del Corporate Cybersecurity HUB della Luiss Business School. In passato ha lavorato come Business Director per una società internazionale con sede negli Emirati Arabi Uniti.

Partner e co-fondatore di DeepCyber, una società boutique focalizzata sulla Cyber Threat Intelligence e manager in diverse società di consulenza come EY e KPMG. Docente presso l'Università degli Studi di Napoli Federico II e la Luiss Business School. Consulente per il Ministero della Difesa (Innova Difesa), agenzie di intelligence e forze dell'ordine. Presidente della Commissione di Studio in Cyber Threat Intelligence e Cyber Warfare della Società Italiana di Intelligence.

Spazio e cyber, un intreccio per le nuove dinamiche di potere

Come ben noto a chiunque segua anche marginalmente le notizie provenienti dal mondo – e come anche trattato in precedenti numeri di questa pubblicazione – negli anni recenti si è assistito all'aumento dei piani, o canali, su cui interagiscono e si confrontano gli Stati di tutto il mondo.

Il cyberspace è sicuramente il più rivoluzionario tra questi.

Il concetto di geopolitica del cyberspazio è stato diffuso già prima degli anni duemila nel dibattito scientifico francese, sulla rivista intitolata *Hérodote*, che nel 1997 prefigurava una "internettizzazione della geopolitica". All'epoca era stata fatta una previsione, ossia: "*Internet moltiplicherà i conflitti di natura geopolitica, portando a una strategia di dominio con la partecipazione di paesi con interessi divergenti. È un'arma di importanza strategica per la sicurezza nazionale*" (Douzet F.), che si può affermare si sia concretizzata a tutti gli effetti.

Già all'epoca, quindi, si ipotizzava il ruolo che il nuovo dominio avrebbe potuto giocare nello scenario internazionale.

Un altro storico campo di confronto geopolitico è stato (ed è ancora oggi) lo spazio, considerato tale già dai tempi della Guerra Fredda. La *Space Race* fu infatti uno degli aspetti in cui si concretizzò la tensione tra Stati Uniti e Unione Sovietica, che correva sul doppio binario della supremazia tecnologica – con possibili applicazioni militari e di spionaggio, data la natura *dual use* della tecnologia spaziale – e della propaganda ideologica.

Oggi lo spazio sta vivendo una seconda centralità, forse proprio grazie al *cyberspace*.

L'intersezione tra spazio fisico e cyber, al di là delle valutazioni tecniche e diplomatiche, è data dal fatto che le funzioni vitali per la società moderna dipendono da questi due domini, senza la disponibilità dei quali molti aspetti della società che conosciamo non esisterebbero. (https://www.nato.int/cps/en/natohq/official_texts_190862.htm)

Spazio e *cyberspace* sono inoltre sfruttati dai singoli Stati per raggiungere i propri obiettivi strategici. Questi possono essere di varia natura, tra cui:

1. **Sicurezza nazionale e difesa**: gli Stati utilizzano satelliti per il monitoraggio delle attività militari e la sorveglianza dei confini. La capacità di condurre operazioni di *intelligence*, sorveglianza e ricognizione dallo spazio è fondamentale per mantenere la sicurezza nazionale. Allo stesso modo, il *cyberspace* è un campo di battaglia dove le nazioni difendono le proprie reti e infrastrutture critiche da attacchi cibernetici e possono condurre operazioni offensive per neutralizzare minacce esterne.
2. **Comunicazioni globali**: i satelliti sono essenziali per le comunicazioni globali, inclusi ad esempio internet e telefonia. Questo consente agli Stati di mantenere connessioni strategiche e operative su

scala mondiale. Anche il *cyberspace* ha un ruolo cruciale nel campo della comunicazione, per la capacità di diffusione di informazioni in tempo reale e a qualsiasi distanza.

3. **Navigazione e gestione del traffico**: i sistemi di navigazione satellitare come il GPS sono fondamentali per la navigazione militare e civile, nonché per la gestione del traffico aereo e marittimo. Questi sistemi dipendono da infrastrutture informatiche per la loro operatività e sicurezza.
4. **Meteorologia e monitoraggio ambientale**: i satelliti monitorano il clima e forniscono dati critici per le previsioni meteorologiche e la gestione dei disastri naturali. Le infrastrutture del *cyberspace* elaborano e distribuiscono queste informazioni, supportando decisioni tempestive e informate.
5. **Sviluppo economico**: l'esplorazione e lo sfruttamento delle risorse spaziali, come l'estrazione di minerali dagli asteroidi, rappresentano nuove frontiere anche in campo economico. Le tecnologie cyber sono cruciali per il controllo e la gestione di queste operazioni remote.

Il rapporto tra i due domini è inoltre connotato da una mutua dipendenza intrinseca. Il *cyberspace* è un dominio artificiale, ormai riconosciuto nelle dinamiche di potere, che ha anche la caratteristica di creare interdipendenze tra gli altri domini operativi. Da notare che lo spazio è stato riconosciuto dalla NATO come dominio operativo nel 2019 e una politica aggiornata in materia è stata pubblicata nel 2022.

Questa interdipendenza si manifesta in diversi modi.

- **Interconnessione delle infrastrutture**: le reti di comunicazione spaziali e terrestri sono strettamente collegate. La gestione e il controllo dei satelliti avvengono attraverso reti informatiche, rendendo queste infrastrutture vulnerabili ad attacchi che possono avere ripercussioni su larga scala.
- **Supporto reciproco**: le tecnologie spaziali forniscono piattaforme fisiche per sensori e trasmettitori utilizzati per svariati ambiti di applicazione. Allo stesso tempo, le infrastrutture di comunicazione informatiche offrono i mezzi per elaborare e distribuire i dati raccolti dallo spazio, rendendoli utilizzabili per una vasta gamma di applicazioni.
- **Resilienza e continuità operativa**: la dipendenza reciproca tra spazio e *cyberspace* implica che la compromissione di uno dei due domini può avere effetti devastanti sull'altro. Pertanto, la protezione e il rafforzamento delle infrastrutture critiche in entrambi i domini sono essenziali per garantire la continuità operativa e la resilienza complessiva.

Questa mutua dipendenza rende indispensabile un approccio integrato alla sicurezza e alla gestione delle risorse spaziali e cyber. Solo attraverso una stretta collaborazione e una strategia coordinata è possibile affrontare le sfide complesse che emergono da questa intersezione cruciale.

Al pari di ogni altra infrastruttura critica digita-

lizzata, come anticipato, anche quella spaziale è vulnerabile ad attacchi cyber. Ciò pone rischi importanti non solo per l'infrastruttura stessa, ma per tutte le ulteriori infrastrutture e funzioni "a terra" che su di essa si appoggiano.

Si tratta di un'architettura molto complessa, che va quindi protetta in ogni sua parte. Infatti può essere colpita da vari tipi di attacchi, dal *command injection* (che potrebbe manipolare i controlli dei veicoli spaziali) ai *denial of service*, o ancora alle intercettazioni. Un attacco cyber potrebbe anche sfruttare l'infrastruttura spaziale come ponte per infettare una infrastruttura terrestre.

Ogni componente chiave, a qualsiasi livello, deve dunque essere hardenizzato ed adeguatamente difeso.

Sul tema della difesa delle infrastrutture spaziali si è di fronte, però, a un doppio problema: da un lato i sistemi spaziali più *legacy*, con protezioni molto basilari, dall'altro la crescente commercializzazione dello spazio, che ha aumentato la superficie d'attacco. Si può pensare a un parallelismo con il mondo IoT, il cui numero è esploso negli ultimi anni e dove strumenti più datati devono essere difesi e poter convivere con altri più moderni.

Anche sul fronte dell'*intelligence* questa interdipendenza tra domini assume una importanza notevole.

L'*intelligence* ha, come sappiamo, un ruolo fondamentale, in quanto raccoglie informazioni vitali per la sicurezza nazionale.

Come dichiarato da Sorin Ducaru, direttore del SatCen (European Union Satellite Centre), l'*intelligence* geospaziale fornisce informazioni a Stati, organizzazioni internazionali e varie altre entità. Si tratta quindi di un'attività per entità *ground-based*, che utilizzano il prodotto dell'*intelligence* per prendere decisioni. Va da sé dunque la criticità legata alla sicurezza e all'affidabilità dei dati provenienti da sensori spaziali, per garantire le quali è necessario un approccio che tenga in debita considerazione la cybersecurity dell'infrastruttura.

Un esempio concreto – e anche abbastanza vicino a noi – dell'importanza di questi aspetti e in generale dell'infrastruttura spaziale è stato dato dalla guerra russo-ucraina, dove gli attacchi cyber da parte della Russia contro il sistema ViaSat hanno dimostrato la possibilità di disabilitare il sistema stesso, facilitando lo spostamento di truppe e rendendo di fatto "cieca" una parte del sistema di *intelligence*. Sempre nello stesso scenario, la comunicazione satellitare fornita da Starlink si è rivelata preziosa: quando le infrastrutture di comunicazione terrestri sono state compromesse dal conflitto in corso, le immagini satellitari hanno fornito informazioni sulla posizione degli *asset* militari e sono state utilizzate durante le fasi di pianificazione delle difese.

Da queste osservazioni si evince come ci si trovi davanti a uno scenario in cui la *space dominance* sarà un tema centrale, che sarà raggiungibile solamente in presenza di forti capacità di *cyber disruption* verso il dominio spaziale stesso. La corsa per la supremazia nello spazio non è solo una questione tecnologica, ma riflette le dinamiche di potere terrestri tra Stati, influenzate da interessi politici, economici e anche militari.

Guardando al futuro, la *space dominance* non si limiterà alla competizione tra nazioni ma coinvolgerà anche attori commerciali, il cui ruolo sarà importante per l'incremento e il rafforzamento

delle infrastrutture spaziali. Le aziende private stanno già contribuendo significativamente con innovazioni e investimenti che riducono i costi e aumentano l'accessibilità delle tecnologie legate allo spazio.

Questa evoluzione, però, porta con sé la necessità di una robusta *cyber deterrence* nel dominio spaziale. La possibilità di attacchi cyber che possano disabilitare infrastrutture spaziali critiche sottolinea l'urgenza di sviluppare strategie di difesa avanzate. L'implementazione di politiche di sicurezza rigorose e la collaborazione internazionale saranno essenziali per proteggere queste infrastrutture da minacce crescenti.

Diventa fondamentale, inoltre, considerare le implicazioni etiche e legali di tali capacità di *disruption*. L'equilibrio tra sicurezza nazionale e stabilità internazionale dipenderà dalla capacità degli Stati e delle organizzazioni sovranazionali di sviluppare norme e accordi che regolino l'uso delle tecnologie spaziali e cyber.

Pertanto la strada verso una *space dominance* sostenibile richiederà non solo avanzamenti tecnologici, ma anche una visione strategica globale che promuova la cooperazione e la sicurezza condivisa. Solo attraverso un approccio integrato e multilaterale sarà possibile affrontare le sfide future e sfruttare appieno le opportunità offerte dalla convergenza tra spazio e *cyberspace*.

Andrea Leoni, *Cyber Security Manager, Segretario Commissione Studi Cyber Threat Intelligence & Cyber Warfare di SOCINT*

BIOGRAFIA

Andrea Leoni

Andrea Leoni è cyber security manager presso una società multinazionale nel settore del credit and business information, è specializzato in governance e ambito GRC, con esperienza pluriennale di security advisory verso realtà nazionali ed internazionali.

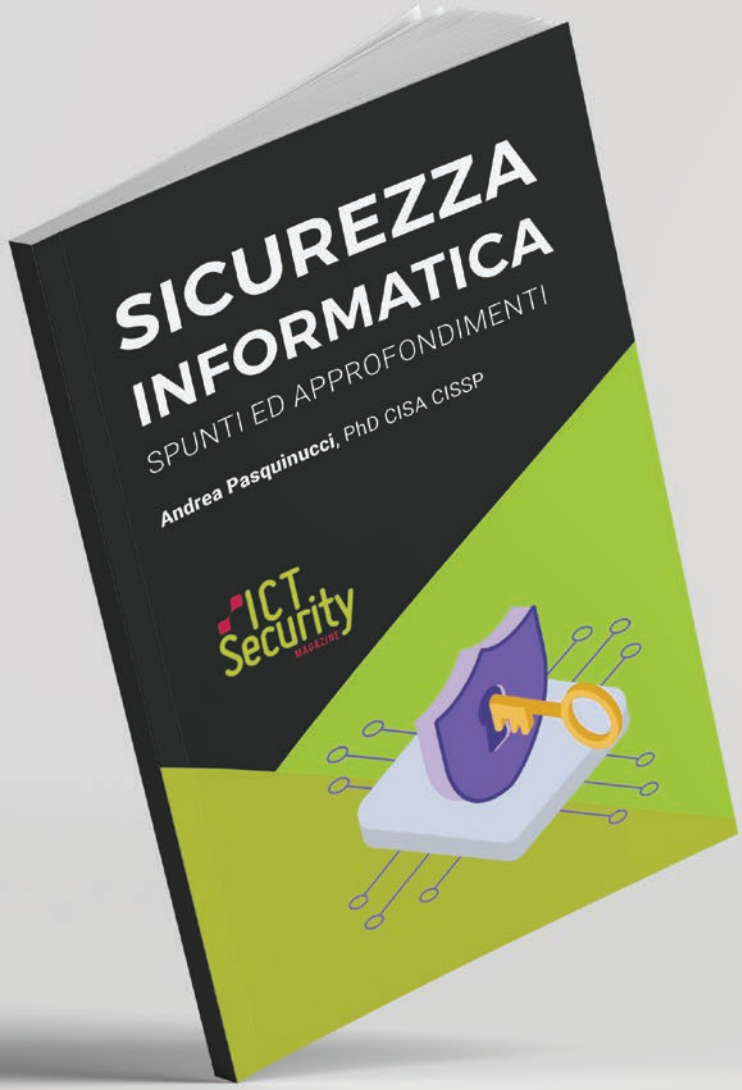
Già ricercatore di intelligence presso il Laboratorio di Intelligence dell'Università della Calabria, presso cui ha conseguito un Master di II livello in Intelligence, si è occupato anche di politica e geopolitica e del loro rapporto col dominio cyber.

Attualmente, presso la Società Italiana di Intelligence, è Segretario della Commissione Studi Cyber Threat Intelligence & Cyber Warfare.

Libro in versione **cartacea** ed **eBook**

SICUREZZA INFORMATICA

SPUNTI ED APPROFONDIMENTI



Il libro è distribuito gratuitamente a tutti gli iscritti alla newsletter di ICT Security Magazine

Sicurezza oltre l'Orizzonte: affrontare le sfide della cybersecurity nelle missioni spaziali. Strategie e rischi

Il crescente rischio di utilizzo dei satelliti come mezzi per attacchi deliberati a infrastrutture spaziali evidenzia l'escalation delle minacce cyber in un dominio tradizionalmente considerato immune. Attraverso l'esplorazione delle complesse sfide legate alla protezione delle missioni spaziali dalle minacce cibernetiche, con un focus particolare sugli attacchi satellite-to-satellite, questo articolo analizza il panorama delle minacce emergenti evidenziando come l'accessibilità di tecnologie avanzate e servizi basati su cloud abbia ampliato il campo di azione per potenziali aggressori, rendendo gli attacchi tra satelliti una realtà tangibile e preoccupante.

L'obiettivo è fornire una panoramica sullo stato attuale della cybersecurity spaziale e proporre vie di azione per garantire la sicurezza delle future esplorazioni e operazioni nello spazio, sostenendo che la soluzione passi anche attraverso una visione condivisa e un impegno globale, tramite il quale sarà possibile proteggere questo ambiente cruciale per l'avanzamento umano.

INTRODUZIONE

L'era moderna dell'esplorazione e dell'utilizzo dello spazio si trova a un punto di svolta, con le infrastrutture spaziali che giocano un ruolo cruciale non solo nella sicurezza nazionale e globale ma anche nella vita quotidiana delle persone.

Satelliti per comunicazioni, osservazione terrestre, navigazione e scoperte scientifiche formano la spina dorsale di numerosi servizi essenziali, dalla previsione meteorologica alla connettività internet globale. Tuttavia, questa crescente dipendenza dalle tecnologie spaziali porta con sé nuove vulnerabilità e sfide, in particolare in termini di cybersecurity. L'evoluzione delle minacce cibernetiche nello spazio esige quindi una riflessione approfondita e l'adozione di strategie di difesa innovative per proteggere queste infrastrutture critiche dagli attacchi deliberati.

Con l'avvento di tecnologie spaziali più accessibili e l'emergere di servizi per il *ground segment* basati su *cloud*, il panorama delle minacce si è ampliato, esponendo le missioni spaziali a rischi senza precedenti[1]. Gli attacchi ai satelliti tramite altri satelliti, un tempo considerati scenari quasi fantascientifi-

1. Falco G. (2020) "When satellites attack: satellite-to-satellite cyber attack, defense and resilience." In: Proceedings of the ASCEND 2020 ASCEND. Reston, VA: American Institute of Aeronautics and Astronautics.

ci, ora rappresentano una possibilità tecnica concreta, sollevando questioni urgenti sulla sicurezza e la sovranità nello spazio.

La risposta a queste minacce richiede un approccio coordinato che integri tecnologie avanzate di cybersecurity, collaborazione internazionale e politiche di sicurezza olistiche. L'adozione di framework consolidati come quello proposto dal *National Institute of Standards and Technology (NIST)*[2] fornisce una base solida per l'identificazione, la protezione, il rilevamento, la risposta e il ripristino dalle minacce cibernetiche. Tuttavia, l'unicità dell'ambiente spaziale e la complessità delle operazioni richiedono soluzioni "su misura" che considerino le specificità tecniche e operative delle infrastrutture spaziali.

La collaborazione internazionale emerge come un pilastro fondamentale nella lotta contro le minacce alla cybersecurity spaziale. La condivisione delle informazioni sulle minacce, lo sviluppo di *best practices* comuni e l'elaborazione di politiche e normative condivise sono essenziali per creare un ambiente spaziale sicuro e resiliente. Solo attraverso un impegno collettivo sarà possibile navigare le sfide della nuova era spaziale, garantendo che lo spazio rimanga una frontiera di opportunità e innovazione per l'umanità.

In questo contesto, il presente articolo si propone di esplorare le dimensioni critiche della *cybersecurity* spaziale, analizzando le minacce emergenti, discutendo le strategie di mitigazione e sottolineando l'importanza delle iniziative normative e tecniche per la protezione delle missioni spaziali nell'era digitale.

FONDAMENTI DELLA CYBERSECURITY SPAZIALE

L'avanzamento tecnologico ha trasformato lo spazio in una frontiera critica per la sicurezza globale, evidenziando l'importanza di un solido framework di cybersecurity per proteggere queste vitali infrastrutture.

La cybersecurity nello spazio, però, va oltre la semplice protezione dei dati, affrontando sfide uniche date dall'ambiente operativo estremamente ostile e dalle complesse interazioni tra componenti terrestri e orbitanti.

Questi attacchi, che possono essere tanto *Nation-State* quanto provenire da attori non statali, minacciano infatti non solo la sicurezza delle informazioni ma anche l'integrità fisica dei satelliti e delle infrastrutture spaziali connesse, potendo causare conseguenze devastanti per le missioni operative e, congiuntamente, per la sicurezza nazionale e la vita quotidiana.

Nel contesto della cybersecurity spaziale, uno degli scenari di minaccia più preoccupanti e tecnologicamente avanzati è rappresentato dagli attacchi ai satelliti perpetrati tramite altri satelliti. Questa tipologia di attacco evidenzia la complessità e la sofisticazione delle minacce emergenti nello spazio, richiedendo approcci di mitigazione specifici e altamente specializzati.

Gli attacchi satellitari contro altri satelliti rappresentano una frontiera relativamente nuova nelle minacce cibernetiche, sollevata da studi recenti come *"When Satellites Attack: Satellite-to-Satelli-*

2. NIST Interagency Report (2023) "NIST IR 8270 – Introduction to Cybersecurity for Commercial Satellite Operations" (https://doi.org/10.6028/NIST.IR.8270)

te Cyber Attack, Defense and Resilience"[3] nonché dalle ricerche del prof. Zatti[4] sugli attacchi documentati ai satelliti, inclusi quelli che hanno portato a perdite di controllo e danni ai sensori.

Questi attacchi possono variare in natura, includendo l'interferenza diretta nelle operazioni di un satellite bersaglio, l'alterazione o lo *spoofing* dei dati trasmessi e ricevuti, o persino l'uso di tecniche di guerra elettronica per degradare le capacità di comunicazione e navigazione.

La fattibilità tecnica di tali attacchi è stata amplificata dalla crescente congestione dell'orbita terrestre bassa (LEO) e dall'aumento del numero di satelliti, dovuto anche all'accessibilità e al costo ridotto dei c.d. *"cubesat"*, nonché alla disponibilità di servizi di *ground segment* basati su *cloud*. Questi sviluppi hanno abbassato significativamente la barriera all'ingresso per la realizzazione di operazioni spaziali, consentendo a un ampio spettro di attori – inclusi quelli con intenzioni malevole – di dispiegare e gestire satelliti in orbita[5].

Per contrastare efficacemente questi attacchi, è fondamentale adottare misure di difesa che vanno oltre le soluzioni convenzionali di cybersecurity. Ciò include lo sviluppo di algoritmi avanzati per il rilevamento e la neutralizzazione di interferenze e attacchi di *spoofing*, la progettazione di satelliti con capacità di resilienza e auto-ripristino migliorate e l'implementazione di protocolli di comunicazione sicuri che possano resistere agli attacchi di guerra elettronica. Inoltre, la crittografia *end-to-end* dei dati trasmessi tra satelliti e stazioni di terra gioca un ruolo cruciale nella protezione dell'integrità e della confidenzialità delle informazioni scambiate.

Un altro aspetto fondamentale nella difesa contro gli attacchi satellitari è rappresentato dalla *Space Situational Awareness* (SSA): ossia la capacità di monitorare l'ambiente spaziale in tempo reale per identificare potenziali minacce e attori ostili. Ciò richiede investimenti significativi in tecnologie di sorveglianza e tracciamento degli oggetti spaziali, nonché la collaborazione internazionale per la condivisione delle informazioni relative alla posizione e al comportamento dei satelliti.

In merito a questo, è essenziale riconoscere il ruolo della collaborazione internazionale e dell'istituzione di norme comportamentali condivise per la condotta delle operazioni spaziali. L'elaborazione di un quadro normativo e di politiche condivise, come vedremo di seguito, può contribuire a prevenire gli attacchi satellitari, stabilendo principi di responsabilità e trasparenza per gli operatori spaziali.

In sintesi, il panorama degli attacchi cyber nello spazio presenta sfide uniche e in continua evoluzione, che richiedono un'attenzione costante e un impegno proattivo da parte di tutti gli *stakeholder* coinvolti. La comprensione delle minacce e delle vulnerabilità esistenti, unita all'implementazione di strategie di difesa e resilienza basate su un ap-

3. Vedasi nota 1

4. Zatti S. (2017) "The Protection of Space Missions: Threats and cyber threats." In: Proceedings of the International Conference on Information Systems Security. A launchpad for satellite cyber-security 15 Computer Science. New York, NY: Springer International Publishing

5. Vedasi nota 1

proccio olistico[6] e collaborativo, è fondamentale per garantire la sicurezza e la continuità delle operazioni spaziali critiche. Come verrà ulteriormente esplorato nelle sezioni seguenti, la collaborazione internazionale e l'adozione di framework consolidati, come quello proposto dal NIST, giocano un ruolo cruciale nel rafforzare le difese contro gli attacchi cyber nello spazio, proteggendo così le infrastrutture spaziali vitali per la società moderna, tenendo bene a mente le eccezioni del caso.

VULNERABILITÀ E MINACCE

Come visto nel paragrafo 2, nell'ecosistema spaziale la proliferazione di tecnologie avanzate e l'accesso "democratizzato" allo spazio hanno esponenzialmente aumentato il numero di vettori di attacco potenziali, esponendo le missioni spaziali a un panorama di minacce sempre più complesso. La cybersecurity spaziale deve quindi affrontare non solo le tradizionali minacce informatiche ma anche scenari specifici del dominio spaziale, che includono attacchi diretti ai satelliti, interferenze e sfruttamento delle vulnerabilità nelle comunicazioni tra terra e orbita.

Storicamente i satelliti hanno beneficiato di una sorta di *"security through obscurity"*, in base alla quale la complessità del sistema e i costi delle apparecchiature dissuadono tutti tranne gli avversari più sofisticati. Gli effetti combinati dei componenti e delle costellazioni *"Commercial Off-The-Shelf"* (COTS), con migliaia di satelliti identici, significano che è improbabile che questa diversità e complessità di implementazione perduri nel tempo.

La motivazione generale per danneggiare i satelliti è ben studiata e intuitiva. In un contesto militare, i sistemi spaziali sono alla base delle capacità di comando, controllo, comunicazione, computer, *intelligence*, sorveglianza e ricognizione (C4ISR)[7][8]. Gli avversari, che cercano di "livellare il campo di gioco" contro le grandi potenze, hanno forti incentivi a minare queste capacità danneggiando i sistemi spaziali[9].

La società civile dipende invece dai satelliti per i servizi essenziali di navigazione, comunicazione e meteorologia. Gli aggressori motivati dallo scopo di provocare sconvolgimenti sociali possono quindi considerare i satelliti come attraenti *"single point of failure"* nelle infrastrutture critiche[10].

Oltre a capire "chi" potrebbe essere interessato

6. Pavur J., Martinovic I. (2022) "Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight." Journal of Cybersecurity, 2022, 1–17

7. Grant ME. (2005) "Space dependence - a critical vulnerability of the net-centric operational commander." Technical report. Naval War College

8. Lungerman J. (2014) "What happens if they say no? Preserving access to critical commercial space capabilities during future crises." Air Space Power J 2014; 28:103–116

9. Pavur J., Martinovic I. (2019) "The cyber-ASAT: on the impact of cyber weapons in outer space." In: Proceedings of the 2019 Eleventh International Conference on Cyber Conflict (CyCon), vol. 900 Tallinn

10. Falco G. (2018) "The vacuum of space cyber security." In: Proceedings of the 2018 AIAA SPACE and Astronautics Forum and Exposition. Orlando, FL: American Institute of Aeronautics and Astronautics

a danneggiare le infrastrutture spaziali, è importante considerare "come" potrebbe farlo.

Un punto di partenza di alto livello può essere trovato nei campi degli studi sulla sicurezza e delle relazioni internazionali, dove la modellazione degli scenari è una componente comune dell'analisi strategica.

La *European Space Agency* (ESA) ha identificato diverse categorie di vulnerabilità e minacce che variano in base alla natura della missione spaziale, sottolineando come la sicurezza dallo spazio possa influenzare direttamente la sicurezza sulla Terra[11].

Queste minacce non sono solo teoriche: incidenti passati hanno dimostrato la capacità degli aggressori di interrompere le operazioni dei satelliti, come nel caso dell'intrusione nel sistema del telescopio spaziale germano-statunitense "ROSAT", che ha subito danni irreversibili a seguito di un attacco informatico.

L'importanza di una comprensione approfondita delle vulnerabilità specifiche e dei meccanismi di attacco potenziali diventa quindi sempre più essenziale.

Pavur e Martinovic (2022)[12] individuano una matrice che associa le vulnerabilità ai mezzi tecnici, alle capacità degli aggressori e al contesto empirico, al fine di chiarire meglio quale organizzazione ha la responsabilità di difendersi da quali minacce, nonché quali competenze tecniche sono richieste per la ricerca sulla sicurezza dei sistemi in ogni dominio.

Tali vulnerabilità sono intuitivamente distinte in:

1. difese in orbita che richiedono competenze sui sistemi *embedded* e di controllo;
2. difesa dei segnali che richiede competenze di rete e radio;
3. difesa delle stazioni e dei sistemi di terra che sfruttano le tradizionali prospettive della *Operation Technology* (OT) e della *Information Technology* (IT).

In merito al punto 3, la vulnerabilità del *ground segment*, come evidenziato nel documento di Bailey (2020)[13], sottolinea un ulteriore livello di rischio. Le infrastrutture di terra, responsabili del controllo e della gestione dei satelliti, possono diventare bersagli privilegiati per gli attacchi, consentendo agli aggressori di prendere il controllo dei satelliti o di interrompere le comunicazioni o ancora perpetrare attacchi *satellite-to-satellite*.

La protezione di questi asset richiede un approccio di sicurezza a più livelli che includa la *defence in depth*, la segregazione della rete, il rafforzamento degli *endpoint* e la gestione proattiva delle vulnerabilità.

Per contrastare efficacemente queste minacce è fondamentale adottare un approccio di gestione del rischio olistico, che preveda l'identificazione proattiva delle vulnerabilità, la valutazione dei ri-

11. Vedasi nota 4

12. Vedasi nota 6

13. Bailey B. (2020) "Establishing Space Cybersecurity Policy, Standards, and Risk Management Practices", El Segundo, CA: Aerospace Corporation

schi e l'implementazione di contromisure appropriate.

Questo approccio, insieme a un impegno per la ricerca continua e lo sviluppo di nuove tecnologie di sicurezza, è essenziale per garantire la resilienza delle missioni spaziali contro le minacce cibernetiche emergenti.

STRATEGIE DI MITIGAZIONE E FRAMEWORK DI SICUREZZA

Come abbiamo visto, la complessa natura delle minacce cibernetiche nel settore spaziale richiede un approccio integrato per lo sviluppo di strategie di mitigazione e framework di difesa robusti. Tali strategie devono essere allineate non solo con le migliori pratiche e standard del settore ma anche con le specifiche esigenze e vulnerabilità delle missioni spaziali.

Il framework fornito dal *NIST* e le analisi sulla protezione delle missioni spaziali presentate da Zatti offrono una solida base per la creazione di un ambiente spaziale sicuro e resiliente. Purtuttavia vedremo che, proprio a causa della complessità del sistema spaziale, alcune semplificazioni potrebbero risultare troppo approssimative; per cui introdurremo degli spunti di riflessione utili a lasciare al lettore i successivi approfondimenti.

Implementazione del Framework del NIST

La pubblicazione del NIST[14] mette in evidenza l'importanza dell'ingegnerizzazione dei sistemi basata sulla gestione del rischio per la sicurezza dei sistemi spaziali. Implementare il framework del NIST significa adottare un approccio sistemico che inizia con l'identificazione delle risorse critiche, la valutazione delle minacce e la definizione dei requisiti di sicurezza specifici per ogni fase del ciclo di vita di una missione spaziale. La protezione deve essere concepita per garantire la confidenzialità, l'integrità e la disponibilità delle informazioni e dei sistemi attraverso l'uso di autenticazione e crittografia efficaci, la protezione contro *jamming* e *spoofing*, nonché la sicurezza operativa e fisica delle infrastrutture di terra.

L'implementazione del framework del NIST rappresenta una pietra miliare fondamentale per la sicurezza cibernetica nel dominio spaziale.

Originariamente progettato per migliorare la cybersecurity nelle infrastrutture critiche, il framework, si basa su un approccio strutturato intorno a cinque funzioni chiave: *Identify*, *Protect*, *Detect*, *Respond*, *Recover*. La sua applicazione nel contesto spaziale implica l'adattamento di queste funzioni per affrontare le sfide uniche e gli elevati rischi associati alle operazioni spaziali.

La funzione *Identify* richiede un'accurata comprensione e catalogazione delle risorse spaziali critiche – dai satelliti alle stazioni di terra – e delle relative vulnerabilità. Questo processo non solo stabilisce il perimetro della sicurezza ma fornisce anche le basi per la valutazione dei rischi e la pianificazione delle misure di protezione.

La funzione *Protect* mira a implementare controlli preventivi per salvaguardare le risorse identificate. Nel contesto spaziale, ciò può includere l'*hardening* dei sistemi di comunicazione satellitare contro l'interferenza e lo *spoofing*, la sicurezza fisica sia dei componenti critici dei satelliti sia delle sta-

14. Vedasi nota 2

zioni di terra e l'uso di crittografia per proteggere i dati trasmessi.

La funzione *Detect* si concentra sul monitoraggio continuo delle risorse spaziali per identificare tempestivamente eventuali attività sospette o violazioni della sicurezza. Ciò implica la creazione di un sistema di allarme che possa efficacemente segnalare tentativi di intrusione o malfunzionamenti che potrebbero indicare un attacco cibernetico.

La funzione *Respond* descrive le procedure e le azioni da intraprendere in risposta a un incidente di sicurezza. Questo include protocolli per la valutazione dell'incidente, il contenimento dei danni, l'eliminazione della minaccia e la comunicazione efficace con le parti interessate. La capacità di risposta rapida è cruciale per minimizzare l'impatto degli attacchi sui sistemi spaziali e sulla sicurezza terrestre.

La funzione *Recover* si focalizza sul recupero delle funzioni e dei servizi compromessi, ripristinando le operazioni normali nel minor tempo possibile. Nel settore spaziale ciò può richiedere la reimpostazione remota dei satelliti, il ripristino dei *backup* sicuri dei dati e la revisione dei protocolli di sicurezza per prevenire futuri incidenti.

Al di là dell'intuizione tecnica sull'uso dei controlli NIST e di strumenti generici di gestione delle informazioni e degli eventi di sicurezza, parlando principalmente dal punto di vista del mondo accademico aerospaziale, alcuni professori e ricercatori[15] sostengono che *"l'affermazione che i controlli esistenti proteggeranno dal rischio è talvolta accettata senza ragionevoli dati di supporto o, peggio ancora, è accettata quando la mancanza di dati viene utilizzata come prova"*.

Questo concetto viene ulteriormente esaltato da Falco (2018)[16], il quale sostiene che i tentativi di mappare la sicurezza informatica tradizionale nel dominio spaziale abbiano creato dannose lacune di conoscenza tecnica e scoraggiato la specializzazione.

In merito a ciò, Falco individua sei ragioni per cui la sicurezza informatica satellitare richiede prospettive tecniche uniche, non soddisfatte dalle pratiche di sicurezza dello *status quo*:

1. i satelliti rappresentano un *single point of failure* per altre infrastrutture critiche, aumentando il numero e le capacità dei *threat actor* che potrebbero essere interessati a danneggiarli al di là di quanto ovviamente rilevante per la funzione della missione;

2. la scarsa regolamentazione, anche tecnica, che guida la sicurezza informatica satellitare crea incertezza riguardo ai controlli appropriati per un determinato sistema. Ciò, è ulteriormente avvalorato da Fidler (2018)[17] che, all'interno di un *think-tank* sulla politica delle relazioni internazionali, sostiene che le mappature degli standard IT applicate ai sistemi spaziali equivalgano a poco più che

15. Byrne DJ., Morgan D., Tan K. et al. (2014) "Cyber defense of space-based assets: verifying and validating defensive designs and implementations." Conference on Systems Engineering Research

16. Vedasi nota 10

17. Fidler D. (2018) "Cybersecurity and the new era of space activities." Technical report. Council on Foreign Relations

"shuffling...paper around";

3. la complessità della *Supply Chain* non solo dà origine a rischi di *backdoor*, ma rende difficile anche l'assegnazione della responsabilità organizzativa per le pratiche di sicurezza. Ad eccezione dei maggiori, gli operatori satellitari non controllano l'intero ciclo di vita della missione. I veicoli di lancio, l'iniezione orbitale, il funzionamento e il ritiro sono spesso gestiti da entità distinte e inoltre molte organizzazioni distinte possono condividere alcune risorse del dispositivo (e.g., i sistemi di comunicazione, i sistemi di comando e controllo, ecc.), mentre ne gestiscono altre in modo indipendente (e.g., i sensori di bordo);

4. l'uso diffuso di hardware COTS integrato con sistemi su misura crea una situazione unica in cui le vulnerabilità probabilmente si applicano a molte piattaforme, ma l'applicazione di *patch* può richiedere modifiche su misura;

5. la natura specializzata del settore aerospaziale fa sì che poche persone nel settore della sicurezza informatica comprendano i satelliti a sufficienza per contestualizzare adeguatamente le minacce e la difesa. Il c.d. *"expertise vacuum"* di Falco è ampiamente riconosciuto come un ostacolo significativo. I componenti di nicchia dei sistemi satellitari mancano di equivalenti diretti in ambito terrestre (e.g., gli inseguitori stellari), compromettendo lo sviluppo di un corpo generale di conoscenze per la protezione di questi dispositivi;

6. i satelliti sono dispositivi con risorse limitate e i compromessi fra sicurezza e prestazioni sono più acuti rispetto ai sistemi terrestri.

In definitiva, i sistemi spaziali sono molto più che semplici *"computers in the sky"*[18].

Le pratiche di sicurezza terrestre ben considerate spesso non riescono a essere trasferite ai sistemi spaziali, per ragioni poco intuitive che richiedono un'ampia gamma di competenze per essere superate. L'esperienza nella crittografia, ad esempio, potrebbe non essere direttamente utile senza ulteriori conoscenze hardware e astrofisiche, poiché la radiazione extraterrestre può indurre *bit-flip* casuali nella memorizzazione delle chiavi crittografiche e richiede pertanto un'attenzione speciale[19].

Misure di sicurezza specifiche per le missioni spaziali

Partendo dalle considerazioni del precedente paragrafo, le misure di sicurezza specifiche per le missioni spaziali rappresentano un elemento critico per assicurare la resilienza e il controllo delle operazioni in un contesto caratterizzato da minacce cibernetiche sempre più sofisticate e pervasi-

18. Vedasi nota 6

19. Banu R., Vladimirova T. (2006) "On-board encryption in Earth observation small satellites." In: Proceedings of the Fortieth Annual 2006 International Carnahan Conference on Security Technology. Lexington, KY: IEEE, 2006. p. 203–208

ve. Ciò viene particolarmente sottolineato da Zatti (2017)[20], il quale sostiene che la categorizzazione delle missioni in base ai livelli di rischio e ai requisiti specifici di sicurezza sia fondamentale per l'elaborazione di strategie difensive mirate.

La sicurezza di una missione spaziale inizia con una valutazione approfondita dei potenziali vettori di attacco e delle vulnerabilità specifiche del sistema. Questo include la considerazione di tutti gli aspetti della missione, dai componenti fisici – come i satelliti e le stazioni di terra – ai sistemi di comunicazione e ai dati trasmessi. Una volta identificate le minacce, è possibile sviluppare contromisure specifiche che vanno dalla protezione fisica dei componenti spaziali alla sicurezza informatica dei sistemi di comunicazione e controllo.

Una strategia difensiva efficace per le missioni spaziali deve includere la crittografia dei dati trasmessi, per proteggere le informazioni sensibili e garantire la confidenzialità delle comunicazioni tra i satelliti e le stazioni di terra. Questo aspetto – sempre tenendo a mente le unicità dell'ambiente spaziale – è particolarmente critico per le missioni il cui *payload* è rappresentato da dati classificati, o che operano nei contesti della sicurezza nazionale.

Inoltre è essenziale implementare sistemi di autenticazione robusti per i comandi inviati ai satelliti, al fine di prevenire l'accesso non autorizzato e l'esecuzione di operazioni di controllo delle orbite pregiudizievoli per le altre infrastrutture spaziali. I sistemi di controllo di terra devono essere dotati di protocolli di sicurezza avanzati per identificare e respingere tentativi di intrusione, oltre a monitorare costantemente la salute e lo stato dei satelliti per rilevare anomalie che potrebbero indicare un attacco in corso.

La protezione contro attacchi di tipo *jamming* e *spoofing* è altrettanto critica, richiedendo l'adozione di tecnologie capaci di discriminare tra segnali legittimi e tentativi di interferenza. Questo include lo sviluppo di algoritmi sofisticati per il rilevamento delle anomalie e la validazione dei segnali ricevuti, assicurando l'integrità e l'affidabilità delle comunicazioni satellitari.

Infine, la resilienza del sistema gioca un ruolo chiave nella difesa delle missioni spaziali. Questo implica la capacità di mantenere le operazioni *mission-critical* in presenza di attacchi o guasti, attraverso la progettazione di sistemi ridondanti, la pianificazione delle soluzioni di continuità operativa e la preparazione per il ripristino rapido delle funzioni compromesse.

L'implementazione di misure di difesa specifiche per le missioni spaziali richiede, quindi, un approccio integrato e multidisciplinare che combini competenze tecniche avanzate in cybersecurity, ingegneria spaziale, analisi del rischio; e che sviluppi protocolli di sicurezza adattivi, capaci di rispondere dinamicamente alle minacce emergenti.

Solo attraverso un impegno proattivo e con la collaborazione tra le agenzie spaziali, i fornitori commerciali e la comunità internazionale sarà possibile garantire la sicurezza e la resilienza delle infrastrutture spaziali nell'era digitale.

Progettazione e sviluppo sicuro

La sicurezza deve essere integrata nella progettazione e nello sviluppo dei sistemi spaziali, conformemente ai principi di *"security by design"*. Que-

20. Vedasi nota 4

sto significa considerare la cybersecurity fin dalle prime fasi di concezione di una missione, implementando controlli di sicurezza robusti e testando proattivamente i sistemi contro possibili vulnerabilità. La resilienza dei sistemi spaziali, ovvero la loro capacità di resistere agli attacchi e ripristinare rapidamente le operazioni normali, deve essere un obiettivo chiave in tutte le fasi di sviluppo.

Un primo passo fondamentale nello sviluppo di un framework di sicurezza per la progettazione e lo sviluppo sicure dei sistemi satellitari è definirne l'ambito di applicazione. Cunningham (2016)[21] sostiene che il modo migliore per farlo è dividere le missioni satellitari in cinque grandi fasi e collegare ogni fase a una distinta *"cybersecurity overlay"*, che promuove la sicurezza fin dalla progettazione.

Un inquadramento alternativo, che permette di avere vantaggi nella fase di modellazione delle minacce, è quello proposto da Zatti (2017)[22], in cui i controlli di sicurezza satellitari sono legati a specifici tipi di missione con l'aggiunta di alcuni controlli generici comuni a tutte le missioni.

Il CCSDS[23] suggerisce un approccio ibrido, rimediando alle carenze giurisdizionali di un approccio puramente *mission-class*, fornendo al contempo una modellazione delle minacce più chiara. Questo approccio incorpora una considerazione esplicita della probabilità di attacco, basata sulla missione mappata, che non rappresenta un quadro esaustivo ma è comunque tra gli esempi tecnicamente più completi fino ad oggi.

L'approccio più comunemente suggerito, tuttavia, è quello di mappare i controlli di sicurezza cyber sulla base di framework preesistenti, sebbene questi raramente includano mappature specifiche che – come rilevato da Knez (2016)[24] – sono legate all'unicità dell'ambiente operativo spaziale, determinando complessità e approssimazioni significative. Un esempio è legato alla gestione degli account utente e delle password, che nei sistemi satellitari raramente trovano riscontro, non incorporando questi il concetto di "utente" e "account".

In questo modo si rischia di ignorare ampie porzioni di standard o di richiedere costose riscritture del software, che aumentano la complessità del sistema senza garantire vantaggi significativi in termini di sicurezza. Inoltre, i controlli per la cybersecurity presuppongono cicli di vita del sistema relativamente statici, ma le proprietà di sicurezza dei satelliti cambiano in modo significativo tra le varie fasi del loro ciclo di vita. I controlli legati all'accesso fisico, ad esempio, sono rilevanti per i satelliti in fase di progettazione e assemblaggio ma privi di significato quando in volo orbitale.

---

21. Cunningham D., Palavincini G., Romero-Mariona J. (2016) "Towards effective cybersecurity for modular, open architecture satellite systems". In: Proceedings of the AIAA/USU Conference on Small Satellites AIAA.

22. Vedasi nota 4

23. CCSDS (2015) "Security threats against space missions. Report concerning space data system standards".

24. Knez C., Llansó T., Pearson D. et al. (2016) "Lessons learned from applying cyber risk management and survivability concepts to a space mission." In: Proceedings of the 2016 IEEE Aerospace Conference.

Adottando questi principi fin dalle prime fasi di progettazione, è possibile creare sistemi spaziali che non solo resistano agli attacchi cibernetici ma siano anche capaci di ripristinare rapidamente le funzionalità operative essenziali, garantendo così la continuità delle missioni spaziali critiche in un ambiente operativo sempre più ostile.

Ad ogni modo, l'adozione di principi di *"security by design"* permette di affrontare efficacemente le sfide poste alla sicurezza *cyber* nell'ambiente spaziale; e, se trattiamo gli standard tecnici come il NIST più come un punto di partenza per la sicurezza che un modello pienamente operativo, è possibile costruire un ambiente spaziale più sicuro e resiliente alle minacce emergenti[25].

CONSIDERAZIONI GIURISDIZIONALI E NORMATIVE

La sicurezza cibernetica nello spazio non è solo una questione tecnica ma anche politica e normativa. Il contesto internazionale richiede un impegno condiviso tra nazioni, agenzie spaziali e attori del settore privato per stabilire standard di sicurezza, pratiche condivise e meccanismi di *governance* che possano regolare efficacemente la sicurezza delle infrastrutture spaziali.

La collaborazione internazionale – come evidenziato dalla necessità di condivisione delle informazioni e delle pratiche di formazione – estende il suo raggio d'azione anche alle politiche e alle normative che possono facilitare o ostacolare questi sforzi condivisi: come sostenuto da Bailey (2020)[26], che sottolinea l'importanza di integrare la cybersecurity in tutte le fasi dello sviluppo dei sistemi spaziali, in linea con le direttive politiche quali la *"Space Policy Directive-5" (SPD-5)*.

Questo approccio normativo enfatizza la necessità di un quadro politico che sostenga la sicurezza spaziale come priorità nazionale e internazionale, promuovendo l'adozione di standard di sicurezza globali.

Inoltre, la varietà di minacce e le specifiche esigenze di protezione delle diverse categorie di missioni spaziali richiedono un approccio flessibile e adattabile alla regolamentazione, in grado di accogliere le esigenze uniche di ogni missione pur mantenendo un elevato standard di sicurezza. Le politiche devono quindi essere in grado di evolversi in risposta alle minacce emergenti e alla rapida evoluzione della tecnologia spaziale.

Le considerazioni politiche e normative, anche alla luce degli eventi recenti, devono anche affrontare la questione della sovranità e della giurisdizione nello spazio, definendo chiaramente le responsabilità in caso di incidenti cibernetici che coinvolgono infrastrutture spaziali internazionali. L'istituzione di un dialogo internazionale aperto e la collaborazione per la creazione di un framework legale comune possono contribuire a superare queste sfide, garantendo che lo spazio rimanga un ambiente sicuro e cooperativo per tutte le nazioni.

25. Tsamis N., Bailey B., Falco G. (2021) "Translating space cybersecurity policy into actionable guidance for space vehicles." In: Proceedings of the ASCEND 2021. Reston, VA: American Institute of Aeronautics and Astronautics

26. Vedasi nota 13

CONCLUSIONI

Le infrastrutture spaziali, fulcro di molteplici aspetti della vita quotidiana e della sicurezza nazionale, sono diventate bersagli appetibili e vulnerabili in un panorama di minacce cibernetiche in rapida evoluzione: la necessità di proteggerle non è mai stata così impellente.

L'analisi delle sfide poste dalla cybersecurity nello spazio, esaminata attraverso le lenti di minacce emergenti e strategie di difesa innovative, nonché evidenziando l'importanza cruciale della collaborazione internazionale, mette in luce la complessità e l'urgenza di affrontare questa dimensione critica della sicurezza globale. L'avvento di tecnologie accessibili – come i *Cubesat* – e la democratizzazione dell'accesso allo spazio hanno ampliato il campo di azione per potenziali aggressori, rendendo scenari un tempo considerati futuristici, come gli attacchi *satellite-to-satellite*, una realtà ormai concreta. La risposta a queste sfide non può essere affidata esclusivamente alle soluzioni tecnologiche ma richiede un approccio olistico che integri aspetti tecnici, politici e normativi.

La collaborazione internazionale emerge come un pilastro fondamentale, essenziale per lo sviluppo di un quadro di sicurezza spaziale condiviso e resiliente. La condivisione di informazioni sulle minacce, la cooperazione nello sviluppo di standard di sicurezza e la promozione di pratiche migliori possono significativamente elevare la soglia di sicurezza per tutte le nazioni attive nello spazio.

L'implementazione di framework di sicurezza come quello proposto dal NIST offre una struttura condivisa per affrontare le minacce in modo sistemico, promuovendo un ciclo continuo di miglioramento della sicurezza che va dall'identificazione delle risorse critiche alla risposta e al recupero dagli incidenti cibernetici. Tuttavia, l'adattamento di questi principi al contesto unico dello spazio richiede un impegno costante nella ricerca, nello sviluppo e nell'innovazione.

In conclusione, proteggere le missioni spaziali dalle minacce cibernetiche è un imperativo che richiede una visione lungimirante, un impegno condiviso a livello globale e una continua evoluzione delle strategie di difesa. Man mano che ci avventuriamo più a fondo nello spazio, la nostra capacità di garantire la sicurezza di queste preziose risorse spaziali definirà il futuro dell'esplorazione e dell'utilizzo dello spazio per le generazioni a venire.

Affrontare le sfide della cybersecurity spaziale non è solo una questione di protezione delle infrastrutture, ma un passo essenziale per mantenere lo spazio come una frontiera di opportunità, innovazione e cooperazione internazionale.

Flavio Marangi, *Partner di Balance S.r.l. e Leader della "Business Unit di Risk, Governance & Compliance"*

BIOGRAFIA

Flavio Marangi

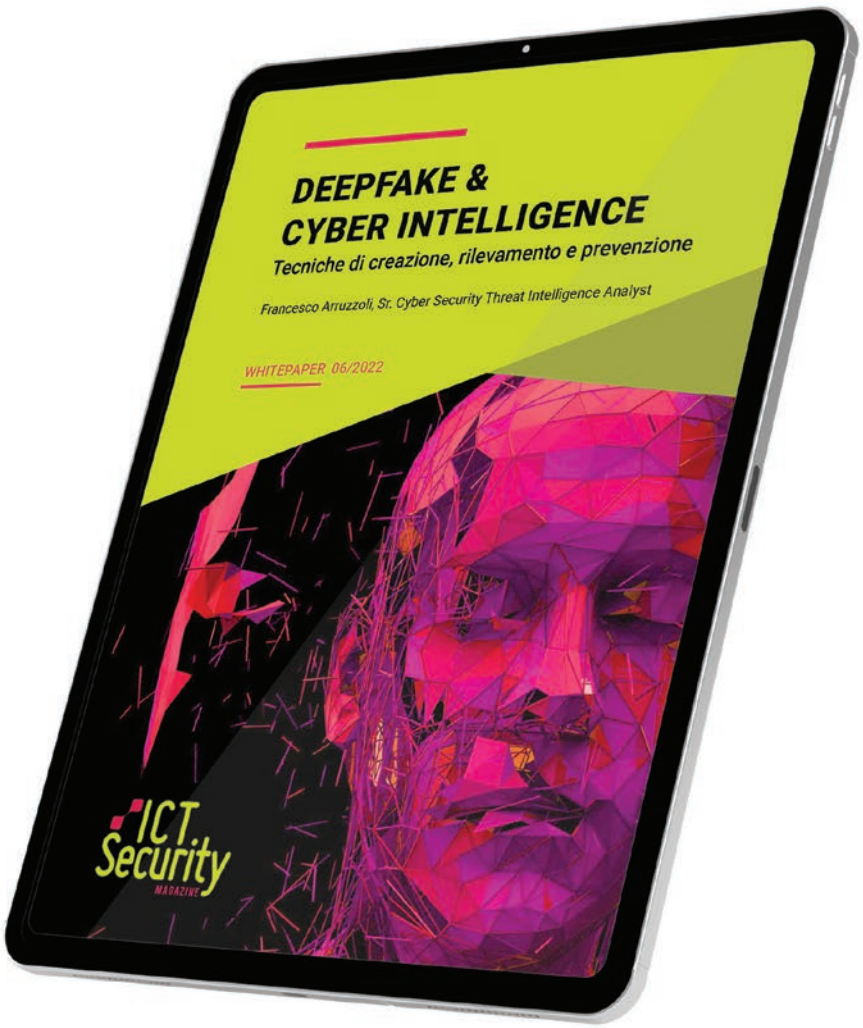
Esperto in materia di governance dei processi di security, con particolare rilevanza per quelli in ambito Network and Information, Golden Power e Intelligenza Artificiale, ha maturato significative esperienze in attività di indirizzo, coordinamento e controllo implementate sia nel settore delle istituzioni nazionali e internazionali sia nel settore privato.

In tali ambiti, grazie ad una solida e concreta preparazione anche post-universitaria, avendo frequentato corsi di specializzazione sia nella sfera della Business Administration che in ambiente accademico e della Difesa, sorretto da un vasto network relazionale, ha gestito rapporti interistituzionali e attività di ricerca, analisi ed elaborazione di informazioni, nel settore della sicurezza e delle strategie innovative, ai fini della tutela di know-how di rilevanza scientifica e industriale.

White Paper

DEEPFAKE & CYBER INTELLIGENCE

Download gratuito su www.ictsecuritymagazine.com



Spazio, Cybersecurity e Tecnologie Emergenti: sfide e strategie per l'autonomia spaziale italiana

Interdipendenze tra spazio e tecnologie ubiquitarie: IA, Quantum Technologies e cybersecurity. Prospettive e sfide per l'autonomia del settore spaziale nazionale

INTRODUZIONE

È indubbio come nella temperie attuale il termine "cyber" abbia subito una sorta di "migrazione terminologica", divenendo sinonimo di "digitale": un prefisso che coinvolge ormai tutte le aree della vita quotidiana, il che fornisce la reale portata della pervasività delle trasformazioni tecnologiche nella società attuale, dominata dalla tecnica (Ellul 1954; 1977)[1]. Da qui la cyber-società, la cyber-comunità, la cyber-economia, la cyber-politica, la cyber-cultura e finanche la cyber-spiritualità.

Si tratta del contesto definito dalle tecnologie che si possono definire ubiquitarie, in quanto pervasive e ovunque fruibili e disponibili; dapprima ha avuto luogo l'avvento della tecnologia digitale, con la rivoluzione elettronica e del computer intesa dal *mainframe* allo smartphone, fattore abilitante essenziale. Ora è arrivato il momento dell'Intelligenza Artificiale (IA) e delle *Quantum technologies* (QT), in particolare del *Quantum computing*.

Le tecnologie ubiquitarie così sinteticamente definite modelleranno lo sviluppo e la storia di questo mondo "cyber", il quale ha bisogno, per ragioni in ultima istanza etiche e politiche in senso alto, di una cybersecurity affidabile e abilitante.

È quindi chiaro che anche il sistema spaziale, inteso in senso olistico, non poteva non essere interessato a tali profonde trasformazioni.

In questo breve testo verrà svolta, dunque, un'iniziale riflessione su come gestire tale interdipendenza per salvaguardare la stabilità, la sovranità tecnologica e la sicurezza del Paese Italia.

CARATTERISTICHE GENERALI DEI SISTEMI SPAZIALI

In termini generali, un sistema spaziale è ciò che si impone alla nostra attenzione quando si abbandona la scala planetaria e si sposta lo sguardo verso il resto dell'universo. Esso può essere naturale – come il sistema solare – o artificiale, come quello che consentì la missione Apollo 11. Opportuno e interessante è osservare che, mentre il mondo "cyber" e le tecnologie ubiquitarie ad esso associate sono legate ai progressi della

1. La tecnica. Rischio del secolo, Giuffré, Milano, 1969 (La technique ou l'enjeu du siècle, Paris: Armand Colin, 1954). Il sistema tecnico, Jaca Book, Milano 2009 (Le Système technicien, Paris: Calmann-Lévy, 1977).

fisica su scala atomica e subatomica e quindi microscopica, per la quale si impone l'uso della meccanica quantistica, i sistemi spaziali (naturali o artificiali che siano) sono descritti dalle leggi fisiche della gravitazione, che è la forza dominante sulle grandi distanze; e si sviluppano su grandi dimensioni, di natura intrinsecamente almeno globale. Come si è accennato, un sistema spaziale naturale è esemplificato dal sistema solare ma anche da una galassia o da un ammasso di galassie, su scale via via crescenti. Un sistema spaziale artificiale è invece costituito da artefatti umani con i quali si sta occupando lo spazio circumterrestre ed esplorando quello esterno. Immediato dedurre l'impatto geopolitico di questa possibilità di osservare e comunicare "dall'alto", che modifica radicalmente il concetto di distanza e che si sottrae anche ai vincoli imposti dai normali confini fra Stati, ben definiti per terra, mare e aria.

Per la parte che qui interessa, è d'obbligo focalizzare l'attenzione sugli oggetti artificiali creati dalle capacità demiurgiche dell'essere umano.

Questi oggetti includono sostanzialmente quattro categorie principali:

1. satelliti che si considerano comprensivi delle sonde scientifiche, ivi comprese quelle dirette verso lo spazio esterno;
2. stazioni spaziali;
3. veicoli di accesso e rientro;
4. detriti.

Per quel che concerne la prima classe, si possono qui riportare alcune esemplificazioni:

- satelliti per telecomunicazioni, i quali forniscono servizi di comunicazione come la telefonia, la televisione, la trasmissione dati e l'accesso a internet;
- satelliti per l'osservazione del pianeta Terra, i quali monitorano l'ambiente terrestre, fornendo informazioni su clima, foreste, oceani e disastri naturali;
- satelliti di navigazione, i quali forniscono informazioni sulla posizione e la velocità agli utenti del *Global positioning system* (GPS);
- satelliti meteorologici, i quali procurano dati sulle condizioni meteorologiche e aiutano a prevedere il tempo;
- satelliti militari, i quali vengono utilizzati per la sorveglianza, la comunicazione e la navigazione militare.

Per quel che riguarda la seconda classe di oggetti artificiali, quella delle stazioni spaziali, esse si connotano per essere utilizzate per la ricerca scientifica, l'osservazione astronomica e la sperimentazione di nuove tecnologie. In genere si tratta di grandi strutture artificiali in orbita attorno alla Terra o ad altri corpi celesti: tra esse la Stazione spaziale internazionale (ISS) è la più famosa e attualmente operativa.

I veicoli di accesso e rientro, chiamati anche lanciatori, sono di estrema importanza in quanto abilitanti per ogni attività da svolgere nello spazio e fortemente connessi con le tecnologie missilistiche, inclusi gli *Intercontinental ballistic missile* (ICBM); ciò spiega il significato geopolitico e propagandistico della "corsa allo spazio" degli anni Sessanta.

I detriti spaziali costituiscono l'ultima classe di oggetti artificiali che, in quanto rifiuti o non più funzionanti, orbitano attorno alla Terra. La loro importanza deriva dalla considerazione che possono avere un grado di pericolosità elevata per i satelliti e le stazioni spaziali in orbita, anche perché la loro quantità sta crescendo a un livello esponenziale e ciò rappresenta – evidentemente – una minaccia per la sicurezza spaziale.

In quanto artefatti tecnologici creati dall'uomo per specifici usi, sia i satelliti sia le stazioni e, in generale, tutti i sistemi spaziali ricadono all'interno delle minacce cibernetiche. In buona sostanza, questi sono asset che esistono nello spazio circumterrestre o esterno oppure sistemi di controllo a terra, comprese le strutture utilizzate per il lancio di questi asset; va tenuto presente che queste ultime non sono strettamente collegate al tipo di sistemi in orbita e che i due sistemi, quello spaziale e quello per il lancio dello stesso, interagiscono solo durante la fase di lancio e di accesso allo spazio.

Essi sono solitamente suddivisi in quattro segmenti tecnologici e operativi:

1. il segmento spaziale;
2. il segmento di collegamento;
3. il segmento di terra;
4. il segmento di utenza.

Il segmento spaziale comprende uno o più satelliti in orbita: la numerosità dei satelliti può essere tale da garantire una copertura di tutto il pianeta. I veicoli di lancio progettati per rilasciare i satelliti nello spazio possono essere considerati, per quanto già detto, sistemi abilitanti complementari. Un satellite contiene un carico utile o *payload* – ovvero l'apparecchiatura progettata per svolgere la missione assegnata al satellite – e una piattaforma o *bus*, che ospita il carico utile e gli altri sottosistemi del satellite.

Il segmento di collegamento è costituito dai canali di trasmissione tra il satellite e la stazione di terra, nonché tra i satelliti.

Il segmento di terra è costituito da tutti gli elementi di terra dei sistemi spaziali e consente il comando, il controllo e la gestione di oggetti spaziali come i satelliti, nonché dei dati che arrivano dal carico utile e vengono consegnati agli utenti.

È importante notare che esiste anche il segmento di utenza dell'infrastruttura spaziale, che può essere considerato come un'estensione del segmento di terra per gli utenti finali di un servizio spaziale. Può trattarsi di un'infrastruttura distribuita che fornisce interfacce a varie applicazioni e servizi che possono interagire con i segnali satellitari direttamente o con altri sistemi del segmento di terra.

Utile osservare che esiste un'altra classificazione degli asset che compongono i sistemi spaziali artificiali; possono essere suddivisi in *upstream*, *midstream* e *downstream*, secondo una tassonomia molto in voga derivata dall'industria del petrolio, che assomiglia non poco a quella già presentata, più fisica e ingegneristica. Il settore *upstream* è, grosso modo e per sommi capi, costituito dal segmento spaziale e di collegamento, quello *midstream* dal segmento di terra e il *downstream* dal segmento di utenza. In campo petrolifero l'*upstream* consiste nell'esplorazione e nell'estrazione, il *midstream* nello stoccaggio e

nella distribuzione e il *downstream* nella petrolchimica e nella distribuzione.

È interessante rilevare qui, a fini geopolitici, la somiglianza concettuale fra i settori. L'*upstream* detiene le capacità strategiche e abilitanti in entrambi i casi in quanto vi sono coinvolte materie di assoluto rilievo economico, strategico e geopolitico: energia e spazio.

Ad esempio, considerando i *Global navigation satellite systems* (GNSS) come il GPS e Galileo, il segmento spaziale è costituito dalla costellazione di satelliti che coprono la superficie del pianeta, il segmento di collegamento dai link di telemetria e telecontrollo fra i satelliti e le basi di controllo e gestione, il segmento di terra da queste ultime e il segmento di utenza da tutti i possibili ricevitori per navigazione satellitare (moltissimi utenti hanno in tasca un pezzo del segmento di utenza di entrambi i GNSS citati, che risiede nel proprio smartphone). *Mutatis mutandis*, si possono applicare i concetti di *upstream*, *midstream* e *downstream*.

Tutti questi segmenti fanno uso di tecnologie digitali sia hardware sia software e, quindi, possono essere esposti a minacce cibernetiche; vi è una possibile – certa in prospettiva futura – interdipendenza capacitiva e funzionale con le altre tecnologie ubiquitarie (es. IA e QT), da considerare sviluppo del digitale e quindi anch'esse attaccabili in ottica cyber.

Le vulnerabilità informatiche, quindi, pongono seri rischi non solo per gli asset spaziali ma anche per le infrastrutture critiche terrestri dedicate alla loro gestione e controllo. La compromissione delle infrastrutture delle stazioni di terra è il modo più semplice per attaccare i sistemi spaziali, in quanto fornisce il software e l'hardware necessari per controllare e tracciare legittimamente gli oggetti spaziali utilizzando le reti e i sistemi terrestri esistenti.

In generale quanto noto, in termini di cybersecurity, per le infrastrutture critiche digitali terrestri (Paliotta 2024)[2] può essere applicato anche a quelle spaziali.

I sistemi spaziali, tuttavia, sono spesso un po' più complessi delle infrastrutture digitali terrestri dal punto di vista dello sviluppo tecnologico, della proprietà e della gestione.

Tale complessità viene amplificata dall'impatto dell'IA e delle QT; esse verranno utilizzate nei sistemi spaziali sia come componenti e strumenti, sia come fattori abilitanti per la definizione, lo studio e il progetto dei predetti sistemi. Non si avrà però solo una maggiore complessità nella cybersecurity dei sistemi spaziali e delle modalità di approccio agli stessi accademiche e industriali, ma anche un'interdipendenza fra loro, dovuta ad esempio alla sempre più cospicua mole di *big data* per addestrare l'IA che lo spazio renderà disponibili e che, verosimilmente, catalizzerà nuove scoperte tecniche e scientifiche.

In definitiva, queste crescenti complessità e interdipendenze sollevano importanti questioni geopolitiche in relazione alla competizione tra i grandi

2. Le infrastrutture critiche all'intersezione tra dispositivi cyber-fisici e Cyber Threat Intelligence, Quaderni di Cyber Intelligence #5, ICT Security Magazine, pp. 34-45, 2024, https://www.ictsecuritymagazine.com/pubblicazioni/quaderni-di-cyber-intelligence-5/.

attori statuali e non statuali, che sono i protagonisti della competizione per la conquista dello spazio e lo sviluppo delle tecnologie ubiquitarie.

SFIDE PORTATE AL LIVELLO DELLA SICUREZZA CIBERNETICA

Come visto in precedenza, l'intersezione tra sicurezza cibernetica e sicurezza spaziale è divenuta un terreno fertile per le minacce cibernetiche e un campo aperto alle future innovazioni apportate dalle tecnologie ubiquitarie.

Con la crescente commercializzazione e militarizzazione del settore spaziale, la sicurezza delle infrastrutture spaziali rappresenta una sfida cruciale per il futuro.

Le infrastrutture terrestri critiche – come le comunicazioni, il trasporto aereo, il commercio marittimo, i servizi finanziari e il monitoraggio meteorologico – dipendono pesantemente da asset basati nello spazio, come satelliti, stazioni terrestri e collegamenti di comunicazione a livello nazionale, regionale e internazionale. La compromissione di queste infrastrutture avrebbe un impatto drammatico sui servizi essenziali dei paesi e della vita quotidiana.

Le infrastrutture spaziali dipendono da tecnologie informatiche e delle comunicazioni (ICT), mentre la sicurezza del cyberspazio risulta connessa a quella delle infrastrutture spaziali che spesso ne costituiscono parte, più o meno strettamente integrata, come i sistemi per le telecomunicazioni, specie quelli a bassa latenza basati su costellazioni (es. Starlink). Con la crescita del settore spaziale, la sicurezza cibernetica di tale ambito deve necessariamente rimanere al passo con le principali sfide sin qui individuate.

Le infrastrutture spaziali sono vulnerabili alle tradizionali minacce cyber come l'*hacking*, l'intercettazione dei segnali e la manipolazione dei dati.

Alcune delle principali vulnerabilità sono qui di seguito individuate, a titolo esemplificativo, in maggiore dettaglio cfr. Dario Sgobbi *et alii* (2015)[3]:

1) **Vulnerabilità delle comunicazioni.** La minaccia più comune contro i canali di comunicazione (canali *uplink* e *downlink*, ovvero il segmento di collegamento) è quella del *jamming*, che compromette i sistemi GPS. I disturbatori GPS inviano segnali sulla stessa frequenza del dispositivo GPS, per annullare o distorcere i segnali satellitari GPS. I disturbatori GPS sono ampiamente accessibili e poco costosi da acquistare, il che li rende disponibili agli attori malevoli statuali e commerciali meno sofisticati. Verso il segmento di utenza risulta rilevante lo *spoofing*, attacco in cui un attore malevolo prevede di nascondere la propria identità fingendo di essere una fonte affidabile per ottenere accesso a informazioni riservate e dati sensibili, o per fornirne di fuorvianti; nel caso dei GNSS, come GPS e Galileo, uno "*spoofer*", ovvero un apparato avversario, genera un segnale simile

3. Space and Cyber Security, in Schrogl KU, Hays PL, Robinson J, Moura D, Giannopapa C (eds), Handbook of Space Security. Policies. Applications and Programs, vol. 1, ch. 9, pp. 157-185.
Earth Observation for Defense, in Schrogl KU, Hays PL, Robinson J, Moura D, Giannopapa C (eds), Handbook of Space Security. Policies. Applications and Programs, vol. 2, ch 31, pp. 527-554.

a quello GPS contenente però coordinate fittizie, "costringendo" così all'errore il ricevitore dell'utente, con l'obiettivo di fargli compiere un percorso differente da quello previsto.

2) **Vulnerabilità della catena di fornitura.** Un altro problema importante, per la sicurezza cyber dei sistemi spaziali, è la complessità della catena di fornitura e dell'ecosistema di fornitori dei sistemi finanziati dalle agenzie governative. Di solito, i componenti specializzati necessari per gli asset spaziali non sono tutti sviluppati da un unico produttore. Infatti, per contenere i costi, le organizzazioni spaziali spesso acquistano i componenti da cataloghi di fornitori approvati in tutto il mondo: quando un'organizzazione governativa spaziale acquista un componente da un fornitore, ad esempio, ha poco controllo sul codice scritto dallo sviluppatore del software di quel componente. Ciò avviene, ancor di più, nel caso del software *open source*. Questa mancanza di conoscenza, se non mitigata da forme di certificazione e controllo della filiera, introduce un rischio considerevole per la sicurezza cibernetica. Va tuttavia ammesso che – specie per l'Italia, che non ha più una propria industria ICT di base in termini di hardware e sistemi operativi – il rischio presente in ambito spaziale deve essere gestito e mitigato e non può essere eliminato. In realtà esistono anche vere e proprie lacune nella *supply chain*, che vengono risolte accettando una dipendenza dall'estero, in alcuni settori di alta tecnologia; a titolo di esempio, buona parte dei semiconduttori e degli ugelli degli stadi italiani dei lanciatori della famiglia Vega.

Quanto esposto vale per le infrastrutture spaziali disponibili oggi; come anticipato, in futuro si dovranno aggiungere al quadro le variabili derivanti dalle citate tecnologie ubiquitarie.

In questo senso risulta molto difficile fare delle previsioni, ma si possono proporre alcune considerazioni di carattere generale.

L'IA, ancora per diversi anni, sarà fruita tramite sistemi digitali tradizionali, benché l'elevato parallelismo tipico del calcolo quantistico sia considerato utile per tale tipo di tecnologia; ciò comporta la possibilità del consueto approccio alla cybersecurity ma nella consapevolezza che l'IA potrà essere un *tool* sia per chi si difende sia per chi attacca, alzando definitivamente "l'asticella" della competizione e la correlata complessità.

Considerazioni analoghe valgono per il calcolo quantistico che, quando disponibile, abiliterà nuove capacità e nuovi approcci nel settore grazie al significativo incremento di potenza computazionale da esso attesa.

Le tecnologie quantistiche riguardano anche le comunicazioni e la sensoristica. Il primo ambito potrà rendere intrinsecamente sicure le comunicazioni, sebbene oggi ciò sia possibile solo limitatamente allo scambio di informazioni crittografiche a bassa velocità (liste chiavi), con modalità complesse che ancora non hanno convinto i governi – per quanto noto – ad un'adozione sistematica di tale tecnologia; la sensoristica quantistica potrà invece rendere estremamente performanti i sensori impiegati nei sistemi spaziali, tenendo presente che la fruizione del dato misurato sarà effettuata con sistemi cyber attaccabili.

Appare chiaro che saranno necessari investimenti significativi, in termini sia finanziari sia di risorse umane, per gestire la complessità descritta, già notevole oggi e destinata ad aumentare.

SFIDE PORTATE AL LIVELLO DELLA SICUREZZA NAZIONALE E POSSIBILI RACCOMANDAZIONI DI POLICY ADVICE

Si può plausibilmente sostenere che i sistemi spaziali sono stati alla base delle strategie di deterrenza che fino ad oggi hanno contribuito a mantenere relativamente pacifiche le diverse sfere di influenza (Stati Uniti, Russia, Europa e Cina). Tutti i principali *player* internazionali, infatti, ritengono che la superiorità nello spazio sia essenziale per la loro politica di sicurezza nazionale.

Ciò vale evidentemente anche per l'Italia che, tuttavia, non può perseguire tale obiettivo se non su un piano di cooperazione internazionale.

La principale sfida risiede nella complessità tecnologica e negli elevati costi dell'industria spaziale; che difficilmente potranno diminuire, considerando quanto emergerà come conseguenza delle nuove tecnologie ubiquitarie (IA, QT, cybersecurity).

In questo senso, deve essere sviluppata un'adeguata strategia nazionale.

Gli ingenti investimenti sono, oggi, in gran parte a carico del settore pubblico.

Esso ben si giustifica solo se si ottengono concreti ritorni in termini:

1) di capacità tecnologica;
2) geopolitici;
3) di sostenibilità tecnico/economica, quale capacità di vendere prodotti e servizi spaziali recuperando almeno i costi ricorrenti;
4) di prestigio internazionale.

Le attività spaziali hanno, quindi, una valenza economica, tecnica, capacitiva, di prestigio e geopolitica; sono abilitate dall'autonomia o, meglio ancora, dall'indipendenza strategica.

In particolare:

- uno Stato si può considerare "autonomo" se dispone di tutti gli elementi, anche di produzione non nazionale, delle infrastrutture, ubicate dentro o fuori del territorio nazionale, necessarie ad effettuare una qualsivoglia attività spaziale, nonché della capacità di utilizzo operativo delle stesse. In altri termini, può agire in autonomia ma ha bisogno del consenso di altri Stati coi quali ha un forte rapporto di cooperazione internazionale;
- uno Stato si può invece considerare "indipendente" se dispone a livello nazionale di tutti gli elementi, incluse le componenti in subfornitura e la relativa filiera produttiva, delle infrastrutture necessarie ad effettuare una qualsivoglia attività spaziale e della capacità di utilizzo operativo delle stesse. In altri termini, può agire in piena autonomia senza il consenso di altri Stati.

In entrambi i casi, sono da considerare inclusi nella capacità di utilizzo operativo il quadro regolatorio e la presenza di almeno un *service provider*.

L'Italia non ha capacità spaziali "indipendenti", ma solo parzialmente "autonome" e in misura decisamente migliorabile.

In primo luogo, è giusto rilevare l'indisponibilità sia di infrastrutture di lancio sia di accesso allo spazio

sotto controllo nazionale. L'Italia ha oggi accesso allo spazio con lanci terrestri solo da territori stranieri e, in particolare, dalla base di Kourou, formalmente ESA ma, di fatto, francese. Può usare da lì, oltre agli Ariane, i vettori della famiglia Vega, di cui l'italiana Avio è *prime contractor* e sistemista; i lanciatori Vega, sino a poco tempo fa, erano commercializzati in esclusiva da Arianespace che, nel corso del 2024, verrà affiancata da Avio in quest'ambito. I margini di autonomia sono invero ristretti, ma si deve salutare positivamente il nuovo ruolo di Avio nella commercializzazione.

Inoltre, limitando l'analisi a questioni di natura squisitamente economica, si sottolineano:

a) specificità italiane negli assetti proprietari dell'industria, specie a livello di *prime*: Thales Alenia Space (francese per ⅔), Telespazio (francese per un terzo), OHB (completamente tedesca) e Avio Spa (posseduta al 28,50% da Leonardo), quest'ultima con cospicue quote sui liberi mercati. Oltre ad esse sono presenti nel comparto spazio Leonardo, Telespazio, SITAEL, INTECS e un cospicuo numero di PMI;

b) lacune nella *supply chain*, già citate ma potenzialmente aggravate dalla situazione internazionale in atto.

In questo contesto diventa essenziale, quindi, supportare e proteggere gli asset industriali nazionali, che ci si aspetta contribuiscano ai ritorni descritti e una sempre maggiore autonomia che abbia come traguardo, in linea teorica, l'indipendenza.

Resta poi da comprendere fino a che punto asset di proprietà straniera o palesemente dominati da una logica finanziaria possano anch'essi contribuire efficacemente al raggiungimento di tali obiettivi legati alla sicurezza nazionale.

Ciò comporta l'analizzare in modo dettagliato e permanente l'economia dello spazio, al fine di approfondire i *trend* in essere e, per quanto possibile, le logiche industriali, finanziarie, geopolitiche che li determinano. Solo così si potrà pensare di definire – e aggiornare di conseguenza – un'effettiva ed efficace strategia nazionale di settore.

Di particolare rilievo, inoltre, risulta approfondire e monitorare gli aspetti qualitativi e qualificanti dell'ingresso dei privati nel settore spazio, processo spesso descritto come "commercializzazione dello spazio". Si ritiene che esso sia la conseguenza della necessità di avvalersi – *in primis* negli USA ma, in prospettiva, anche in Europa e in Italia – della maggiore efficienza e flessibilità dell'industria privata, rimanendo saldo e dominante il ruolo degli Stati nel finanziare i programmi, nel creare il mercato di riferimento e nello stabilire le strategie. Da tenere presente che, come da più parti si riconosce, uno dei fattori di successo della *Space economy* privata negli USA, di cui Space X è un esempio lampante, è la forte integrazione verticale, in netto contrasto con il modello europeo oggi disponibile, sia in European space agency (ESA) sia in Commissione Europea (CE).

Rimangono inalterati, quindi, il paradigma dei ritorni sopra definito e la necessità che il comparto industriale collabori al conseguimento degli obiettivi strategici in base ai quali si giustifica l'intervento pubblico.

Qualora dovesse emergere un mercato in cui la domanda fosse di natura privata in maniera crescente (e, in prospettiva, addirittura dominante),

dovrà essere rivisto il già menzionato paradigma di ritorni e riconsiderato il ruolo dell'investitore pubblico.

Solo a titolo esemplificativo, potrebbe essere opportuna una verifica del rapporto fra i costi sostenuti in termini finanziari e i gradi di libertà delegati nella politica industriale.

In questo senso potrebbe essere utile re-indirizzare, a fini di autonomia nazionale, gli stessi investimenti in ESA, ad oggi caratterizzati da una significativa delega della politica industriale nazionale di settore, anche per quanto attiene al PNRR Spazio.

Investire in ESA, infatti, è giustificato solo se porta a ritorni in tecnologia avanzata e, quindi, in concreta capacità aerospaziale; ciò può avvenire soltanto se si investe in programmi e progetti (specie quelli opzionali) realmente innovativi, attenti al mercato e al conseguimento di capacità di rilievo strategico che portino a una maggiore autonomia e competitività del sistema Italia.

Un parametro importante sul quale fare un serio e concreto approfondimento è quello del cosiddetto "ritorno geografico" o "geo-ritorno", per comprendere "quanto" degli investimenti fatti dal Paese ritorni concretamente nel sistema economico-industriale italiano, in termini di tecnologia a elevata qualificazione.

Rimane il tema squisitamente econometrico, reso impegnativo dal fatto che non esistono statistiche messe a punto dall'Istituto nazionale di statistica (ISTAT) con specifico riferimento al settore spazio. Appare di immediata evidenza quanto sia strategico conoscere l'andamento nel tempo dei principali parametri economici e le loro correlazioni con le altre grandezze che possono influenzare il comparto e la politica economica e industriale.

In conclusione l'obiettivo da perseguire con convinzione, ai fini della crescente autonomia del comparto spazio nazionale, è quello della disponibilità costante di una sistematica e approfondita analisi economica ed econometrica, per valutare sia gli oggettivi, concreti ritorni (nei termini sopra definiti) per il Paese rispetto agli investimenti fatti nello spazio, sia eventuali modifiche della politica industriale, che recepiscano il maggior ruolo del settore privato; quanto descritto è essenziale per l'aggiornamento di una strategia nazionale per lo spazio.

In base al quadro prospettato l'indipendenza strategica non appare alla piena portata dell'Italia, ma dovrebbe costituire una sorta di bussola alla cui indicazione tendere asintoticamente nel tempo. Infatti, si reputa possibile migliorare le capacità nazionali conseguendo sempre maggiore autonomia operativa con l'obiettivo di ridurre al minimo le forme di dipendenza più limitanti; il tutto, come accennato, in un contesto di cooperazione internazionale.

L'Italia opera principalmente sia in Europa, in ambito ESA e CE, sia in cooperazione bilaterale con gli Stati Uniti. In tali contesti dovrà ritagliarsi gli spazi di manovra per crescere nel settore spaziale, secondo le auspicabili prospettive che si sono descritte.

Il problema principale è la mancanza di un'Unione europea politica che possa dare reali e concrete garanzie di sicurezza a tutti gli Stati membri, creando sinergie e cooperazioni che oggi non sarebbero accettabili per via del contenuto dei trattati europei. Il Trattato sull'Unione Europea (TUE) e il

Trattato sul funzionamento dell'Unione Europea (TFUE), infatti, demandano ai singoli Stati le questioni di difesa e sicurezza.

Rimane, allora, la cooperazione in ESA, irrinunciabile in quanto la CE non sembra in grado di gestire l'implementazione di programmi spaziali in autonomia ma solo di svolgere su di essi un'alta vigilanza, essenzialmente tramite la leva finanziaria del proprio piano di investimenti di ciascun framework settennale. In tale contesto, si palesano tutti i limiti dell'attuale UE e si corrono seri rischi di compressione dell'autonomia nazionale, senza le garanzie necessarie in termini capacitivi e di sicurezza.

La cooperazione bilaterale con gli USA non va, allo stato, abbandonata ed è potenzialmente molto fruttuosa, sia in termini geopolitici sia per prospettive capacitive e tecnologiche.

Altra questione di estrema rilevanza è l'importanza del mantenimento della superiorità in ambito spaziale, a cui già si è fatto cenno.

Il concetto appare chiaro e difficilmente contestabile, ma nasconde un potenziale rischio.

Costruire e mantenere una superiorità spaziale, infatti, comporta costi elevati e tempi lunghi; fornisce un vantaggio molto significativo ma è privo di rischi solo quando il conflitto è fortemente asimmetrico.

Va considerato infatti che, specie alle quote basse, le cosiddette *Low earth orbit* (LEO) fra i 200 e i 2.000 km, ove risiedono quasi tutti i satelliti governativi e militari, è possibile un credibile tentativo di interdizione della superiorità spaziale tramite:

1. dispositivi di *jamming* ad alta potenza, potenzialmente distruttivi dell'elettronica di bordo;
2. esplosioni nucleari fuori dell'atmosfera, pure potenzialmente distruttive dell'elettronica di bordo tramite il *Nuclear electro magnetic pulse* (NEMP).

Tali capacità non richiedono di essere una superpotenza tecnologica; basti pensare che la Corea del Nord le ha. Fra l'altro tale attacco non farebbe vittime umane dirette e sarebbe, quindi, non semplice bilanciare un'adeguata reazione.

La domanda da farsi diventa, quindi: chi ha investito per ottenere la superiorità spaziale e, in qualche modo, vi si è abituato, quanto sarà capace di rinunciarvi? Tale rinuncia avrà effetto solo sugli operatori o anche su altre parti del dispositivo di resilienza e sicurezza dello Stato privato (in tutto o in parte) della sua superiorità spaziale?

A mero titolo esemplificativo, si ricorda che i sistemi GNSS forniscono il riferimento di tempo e frequenza ad un numero ormai elevatissimo di sistemi. Se mancasse il riferimento in questione quali e quanti fra i sistemi che lo usano potrebbero continuare a funzionare?

In definitiva, il tema qui succintamente evidenziato deve essere necessariamente recepito in una coerente Strategia spaziale nazionale.

CONCLUSIONI

Lo spazio non solo sta diventando sempre più congestionato, conteso e competitivo, ma anche sempre più commerciale; a titolo esemplificativo basta osservare che Space X e Starlink, entrambi di proprietà di Elon Musk, concentrano nelle mani

di una sola persona capacità spaziali che, forse, nessuno Stato oggi possiede, con la possibile eccezione degli USA.

Il pericolo legato alla crescita delle attività spaziali – e alla proliferazione di attori in grado di operare nello spazio – è quello di creare una crescente competizione geopolitica tra le parti, che può portare a errori di valutazione ai fini della sicurezza nazionale, soprattutto per quanto riguarda le nuove tecnologie ubiquitarie.

È chiaro che la mitigazione delle minacce informatiche nello spazio richiede soluzioni sia tecnologiche che politiche. Sebbene molte delle soluzioni tecnologiche per i sistemi terrestri possano essere applicate alle infrastrutture spaziali, lo spazio crea alcune sfide uniche per la sicurezza nazionale. Inoltre, poiché l'ambiente delle minacce è dinamico, anche le soluzioni tecnologiche devono essere dinamiche e adattarsi alle nuove situazioni di minaccia.

Oltre ai meccanismi di sicurezza cibernetica tradizionali, quali il contrasto agli attacchi e i protocolli di sicurezza, sono necessarie nuove architetture e soluzioni di sicurezza che tengano conto dell'evoluzione dei sistemi digitali, nonché dell'impatto dell'intelligenza artificiale e delle *Quantum technologies*.

Pertanto, un approccio globale per una risposta e una mitigazione efficaci richiede una soluzione politica sistematica e unificata che possa guidare gli sforzi tecnologici per proteggere i beni e i servizi spaziali del proprio Paese.

La soluzione politica deve affrontare diverse dimensioni, poiché nuovi attori (statuali, non statuali e commerciali) e nuove tecnologie stanno espandendo e trasformando le attività spaziali. Tuttavia, al momento né la politica spaziale né la politica di sicurezza nazionale a livello di Paese Italia sembrano pronte ad affrontare le sfide create dall'intreccio tra spazio e cyberspazio; e ciò aumenta drasticamente i rischi per la sovranità nazionale.

In conclusione, la convergenza tra spazio e cyberspazio richiede una visione olistica e una risposta globale. Le idee prospettate in questo breve testo vanno poste alla base di una strategia di medio-lungo periodo che definisca priorità, risorse e obiettivi intermedi: e ciò è essenziale per garantire all'Italia un futuro sicuro nello spazio.

Achille Pierre Paliotta, *Ricercatore senior della Struttura Mercato del Lavoro dell'INAPP (ex ISFOL).*

Dario Alessandro Maria Sgobbi, *Consulente del Ministero delle Infrastrutture e Trasporti*

BIOGRAFIA

Achille Pierre Paliotta

Ricercatore senior della Struttura Mercato del Lavoro dell'INAPP (ex ISFOL). Laurea in Sociologia all'Università di Roma "La Sapienza", Master in Data Science (DS) all'Università di Roma "Tor Vergata" nel 2015 e Master in Cybersecurity (SIIS) all'Università di Roma "La Sapienza" nel 2021. Svolge studi e ricerche sull'innovazione tecnologica, sulla *cyber intelligence*, sulla cybersicurezza, sulle professioni, sull'incrocio tra domanda ed offerta di lavoro, sulla formazione continua, sull'invecchiamento attivo, sulla contrattazione collettiva e, in generale, su tematiche di sociologia economica. Sta attualmente svolgendo il I Dottorato nazionale in Cybersecurity presso IMT Lucca e IIT CNR.

BIOGRAFIA

Dario Alessandro Maria Sgobbi

Il Contrammiraglio (aus) Dario Alessandro Maria Sgobbi è un Ufficiale con oltre quarant'anni di attività; ha conseguito due lauree, ingegneria elettronica e scienze politiche, ed un master di secondo livello in sistemi spaziali. Ha servito a bordo delle Unità Navali, nei settori dell'Intelligence militare, della security e del C4I&Space, lavorando anche negli USA presso il Link22 Project Office e in Olanda all'Agenzia Spaziale Europea presso il Galileo Security Office. Attualmente è consulente del Ministero delle Infrastrutture e Trasporti.

White Paper

RANSOMWARE
Innovazione e redditività del cyber-crime

Download gratuito su www.ictsecuritymagazine.com

Il ruolo cruciale dell'Ingegneria della Sicurezza nello spazio: affrontare le minacce cyber nel nuovo contesto globale

INTRODUZIONE

Il panorama dell'ingegneria della sicurezza applicata ai sistemi spaziali sta attraversando una trasformazione profonda, con gli attacchi informatici che emergono come la minaccia più insidiosa e pericolosa.

A differenza delle minacce fisiche, che consentono un intervento immediato, i cyber attacchi sono spesso difficili da identificare e comprendere, rendendo la prevenzione e la mitigazione delle loro conseguenze estremamente complesse: in risposta a questo nuovo scenario l'ingegneria della sicurezza ha assunto un ruolo di primaria importanza, diventando un campo specializzato all'interno dell'ingegneria spaziale. Questo settore si concentra sugli aspetti critici della sicurezza nella progettazione e nello sviluppo dei sistemi spaziali, con particolare attenzione alla protezione contro le minacce cyber.

L'evoluzione del concetto di "guerra non lineare" ha introdotto un nuovo approccio metodologico alla strategia militare, in netto contrasto con le pratiche del passato. Questa definizione (coniata da Vladislav Surkov, consigliere personale di Vladimir Putin) fa riferimento a una complessa tecni-

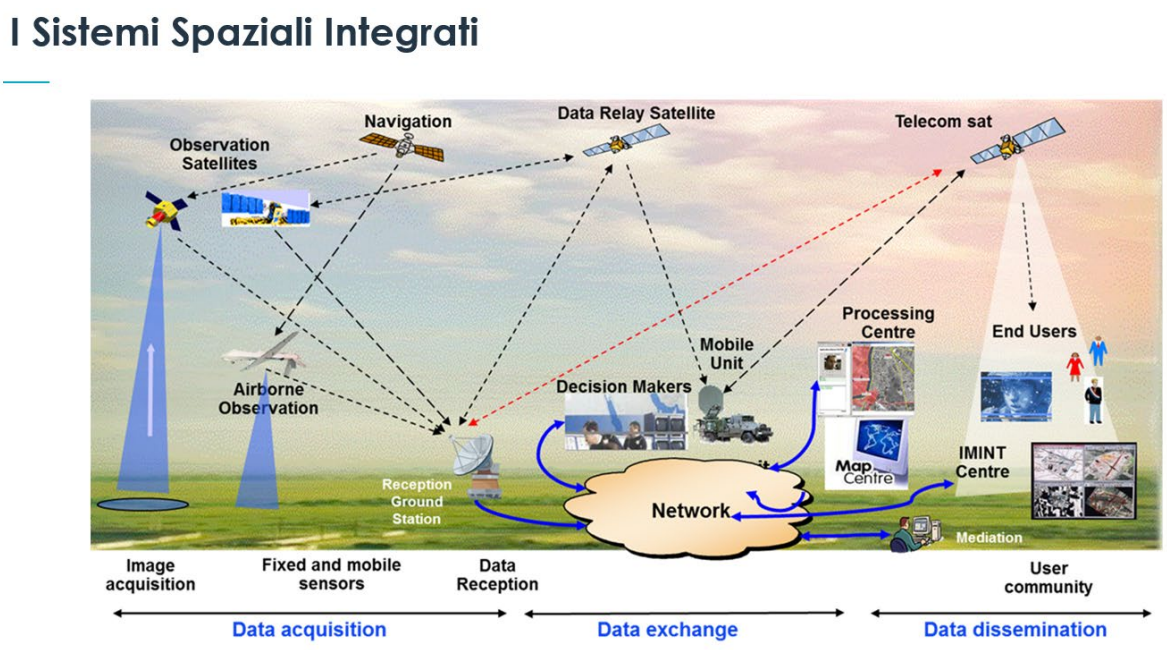


Fig 1 - I sistemi spaziali integrati nel teatro operativo

ca di manipolazione mediatica e finanziaria finalizzata a creare confusione e instabilità all'interno di un sistema, rendendolo vulnerabile e difficile da difendere/governare.

Due *driver* fondamentali guidano la sicurezza dei sistemi complessi: l'uso del sistema – soprattutto in contesti militari – e le politiche relative ai dati, che rivestono un ruolo cruciale nella protezione delle informazioni sensibili gestite dal sistema. Il contesto attuale è caratterizzato da sfide significative, con l'adozione di sistemi *dual-use* che rappresentano una tendenza emergente per massimizzare le sinergie finanziarie.

La cooperazione internazionale diventa sempre più essenziale per lo sviluppo e l'impiego di questi sistemi.

LA SICUREZZA DEI SISTEMI DI OSSERVAZIONE DELLA TERRA

I sistemi di osservazione della Terra rivestono un ruolo critico nella sicurezza, grazie alla loro capacità di fornire immagini ad alta risoluzione e di accesso globale. Tuttavia, questa stessa caratteristica li rende vulnerabili a diverse minacce: è pertanto necessario implementare misure di sicurezza per proteggere gli asset del sistema, garantendo la disponibilità, l'integrità e la confidenzialità dei dati.

La definizione di una politica di sicurezza efficace è fondamentale per affrontare le minacce cyber in modo proattivo. Questa politica dovrebbe comprendere l'identificazione degli asset da proteggere, l'analisi dei punti deboli del sistema e la valutazione delle contromisure necessarie. Tra le misure di sicurezza chiave si annoverano la certificazione Common Criteria, la protezione COMSEC e l'implementazione di sistemi crittografici.

GESTIONE DEGLI ASSET E MISURE DI SICUREZZA

Gli asset di un sistema spaziale possono includere

Fig. 2 - Esempi di Asset di un Sistema Spaziale

una vasta gamma di informazioni e dati sensibili che devono essere protetti per garantire la confidenzialità, l'integrità e la disponibilità. Tra questi rientrano i dati acquisiti dai sensori di bordo, i cataloghi di richieste, gli scenari operativi per la difesa, la protezione dei dati sui link terra/bordo, nonché i *database* e piani di missione duali.

In particolare:

Dati acquisiti dai sensori di bordo

Questi dati rappresentano informazioni critiche raccolte dai sensori dei satelliti, come immagini e dati scientifici. La loro protezione è essenziale per evitare l'accesso non autorizzato e garantire l'integrità delle informazioni trasmesse.

Cataloghi di richieste

I cataloghi di richieste contengono informazioni sulle esigenze degli utenti e le specifiche richieste per l'acquisizione di dati da parte dei satelliti. La loro protezione è necessaria per impedire l'accesso non autorizzato e assicurare che le richieste siano autentiche e non alterate.

Scenari operativi per la Difesa

Gli scenari operativi includono piani e strategie per l'utilizzo dei satelliti in operazioni di difesa. La protezione di questi scenari è cruciale per garantire la sicurezza nazionale e prevenire l'interferenza di attori ostili.

Protezione dei dati sui link terra/bordo

I link di comunicazione tra le stazioni a terra e i satelliti sono vulnerabili agli attacchi cyber. È fondamentale implementare misure di sicurezza, come la crittografia, per proteggere i dati trasmessi e prevenire l'intercettazione o la manomissione.

Database e piani di missione duali

I *database* contengono informazioni critiche per la gestione e il funzionamento dei satelliti, inclusi i piani di missione duali che prevedono l'uso dei satelliti sia per scopi civili che militari. La loro protezione è essenziale per garantire la continuità operativa e prevenire accessi non autorizzati.

Negli ultimi anni la *Cyber Defence* è diventata una priorità per molteplici settori, inclusi i sistemi spaziali. La crescente integrazione dei sistemi satellitari con le reti esterne ha esposto queste infrastrutture a nuove vulnerabilità, rendendo i cyber attacchi una delle minacce più pericolose. In questo contesto di guerra ibrida, caratterizzato da conflitti non lineari, è emersa l›urgenza di rivedere l›approccio metodologico nell›analisi del rischio per i sistemi spaziali, adottando soluzioni di sicurezza sempre più specifiche e avanzate.

Fino ai primi anni 2000, i sistemi satellitari erano considerati relativamente al sicuro rispetto alle minacce cyber, principalmente grazie alla loro segregazione fisica dalle reti esterne. Tuttavia, con l'incremento degli attacchi informatici e l'integrazione crescente dei sistemi spaziali con le reti terrestri, è diventato evidente che anche questi sistemi necessitano di robuste misure di sicurezza. L'emergere di sistemi duali ha ulteriormente complicato il panorama, richiedendo un'attenzione particolare alle problematiche di sicurezza specifiche per il segmento spaziale.

PECULIARITÀ DELLA SICUREZZA NEI SISTEMI SPAZIALI

La sicurezza dei sistemi spaziali presenta sfide uniche rispetto alle reti terrestri.

Le principali peculiarità sono:

- **Complessità della gestione delle chiavi**: negli scenari multi-operativi e multi-utenza, la gestione delle chiavi crittografiche diventa estremamente complessa.
- **Periodo di visibilità dei satelliti**: la finestra temporale per la comunicazione con i satelliti è limitata, il che complica ulteriormente la sicurezza delle trasmissioni.
- **Manutenzione impossibile**: l'hardware a bordo dei satelliti non può essere riparato una volta in orbita, richiedendo soluzioni di sicurezza che garantiscano la massima affidabilità.
- **Standard di cybersecurity non specifici**: gli standard come le Common Criteria sono progettati per i sistemi terrestri e non tengono conto delle specificità dei sistemi spaziali.

I sistemi spaziali moderni sono sempre più integrati, rendendo la sicurezza una questione complessa. La protezione deve considerare tutti i componenti del sistema, dai satelliti ai centri di controllo a terra. Le misure di sicurezza devono includere:

- **Valutazione dei sistemi dal punto di vista cyber** - inclusa la valutazione di satelliti e componenti a bordo, secondo standard come Common Criteria e FIPS.
- **Gestione dinamica delle chiavi** - l'adozione di sistemi di gestione delle chiavi dinamici e l'implementazione di algoritmi avanzati come quelli basati su sistemi dinamici caotici.
- **Protezione del software di bordo** - misure per garantire l'integrità del software e prevenire operazioni di *reverse engineering*.

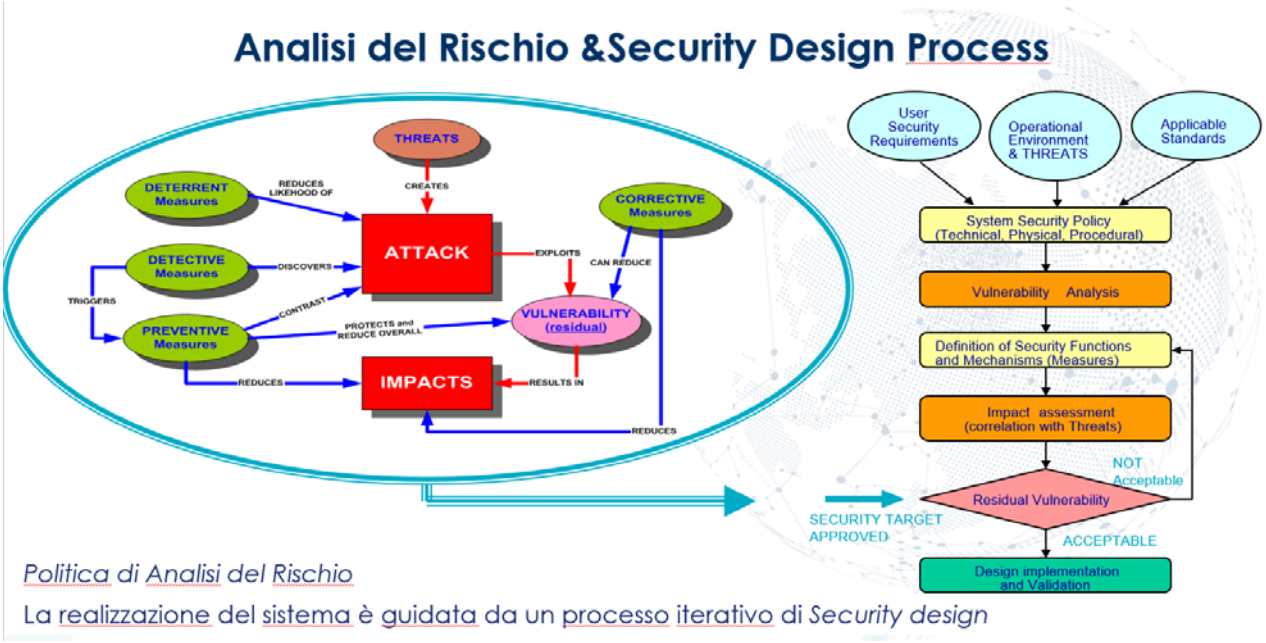


Fig 3 - Processo di Analisi del Rischio

- **Protezione elettromagnetica** - valutazioni TEMPEST per garantire la sicurezza elettromagnetica dei satelliti e dei sistemi cifranti.

ANALISI DEL RISCHIO

L'analisi del rischio è un processo essenziale per garantire la sicurezza e la resilienza di un sistema o un'organizzazione. È cruciale che questo processo inizi considerando una serie di input fondamentali, tra cui i requisiti del cliente, gli standard di riferimento e il contesto geopolitico: i requisiti del cliente forniscono una comprensione chiara delle aspettative e delle necessità specifiche del progetto, mentre gli standard di riferimento assicurano che l'analisi e le misure adottate siano conformi alle migliori pratiche e normative del settore. Il contesto geopolitico, inoltre, influenza significativamente il panorama delle minacce e delle vulnerabilità, variando in base a fattori come stabilità politica, legislazione locale e tensioni internazionali.

QUANTUM TECHNOLOGY APPLICATA AI SISTEMI SPAZIALI: LA RIVOLUZIONE DELLA QUANTUM KEY DISTRIBUTION

Negli ultimi anni le tecnologie quantistiche hanno iniziato a rivoluzionare vari settori, tra cui quello spaziale. Una delle applicazioni più promettenti è la *Quantum Key Distribution* (QKD), una tecnologia che permette di scambiare chiavi crittografiche in modo estremamente sicuro sfruttando le proprietà della meccanica quantistica. Questa innovazione risulta particolarmente efficace nei sistemi spaziali, dove la sicurezza delle comunicazioni è fondamentale.

La QKD si basa sui principi della meccanica quantistica per garantire la sicurezza delle chiavi crittografiche. Utilizzando fotoni *entangled* o singoli fotoni in stati quantistici, la QKD permette di rilevare qualsiasi tentativo di intercettazione; questo perché qualsiasi misurazione non autorizzata altera lo stato quantistico dei fotoni, rendendo immediatamente evidente la presenza di un attacco.

PECULIARITÀ DELLA QKD NEI SISTEMI SPAZIALI

- Distanza e Sicurezza: la QKD permette la trasmissione di chiavi crittografiche su grandi distanze senza compromettere la sicurezza. Nei sistemi spaziali questa caratteristica è cruciale, data la necessità di comunicare con satelliti che orbitano a centinaia di chilometri dalla Terra.
- Intercettazioni rilevabili: qualsiasi tentativo di intercettazione dei fotoni utilizzati per la QKD altera lo stato quantistico del segnale, permettendo di rilevare immediatamente una possibile intrusione. Questo garantisce un livello di sicurezza ineguagliabile rispetto ai metodi tradizionali.
- Protezione dai sistemi a computer quantistici: la QKD è intrinsecamente sicura contro gli attacchi futuri che potrebbero essere realizzati con i computer quantistici. Questi dispositivi, quando saranno pienamente operativi, avranno la capacità di rompere molte delle attuali tecniche di crittografia. La QKD, invece, rimane sicura grazie alle leggi fondamentali della fisica quantistica.

Oltre alla QKD, la sicurezza delle comunicazioni

nei sistemi spaziali deve considerare l'avvento dei computer quantistici. Gli algoritmi *post-quantum* sono progettati per resistere agli attacchi da parte di questi potenti computer: questi algoritmi si basano infatti su problemi matematici che si ritiene siano difficili da risolvere anche per i computer quantistici, come quelli legati alla teoria dei reticoli, ai codici di correzione degli errori e alle funzioni *hash* quantistiche.

Implementare algoritmi *post-quantum* nei sistemi spaziali, in combinazione con la QKD, garantisce un doppio livello di sicurezza. Da un lato, la QKD fornisce un metodo sicuro per la distribuzione delle chiavi; dall'altro, gli algoritmi *post-quantum* assicurano che i dati rimangano protetti anche se un avversario dovesse ottenere accesso a un computer quantistico.

La *Quantum Key Distribution* rappresenta una svolta significativa per la sicurezza delle comunicazioni nei sistemi spaziali. Le sue peculiarità, come la capacità di rilevare intercettazioni e la resistenza ai futuri attacchi quantistici, la rendono una tecnologia fondamentale per proteggere le informazioni sensibili trasmesse tra satelliti e stazioni terrestri. Integrando la QKD con algoritmi *post-quantum*, possiamo creare un'infrastruttura di comunicazione spaziale robusta e sicura, pronta ad affrontare le sfide del futuro tecnologico.

CONCLUSIONI

L'analisi condotta evidenzia l'importanza cruciale dell'Ingegneria della Sicurezza nei sistemi spaziali, sottolineando la necessità di una protezione integrata che copra tutti i componenti, dai satelliti ai centri di controllo a terra. Le misure di sicurezza devono essere progettate in modo tale da garantire la disponibilità, l'integrità e la confidenzialità dei dati, adottando un approccio che combini valutazioni cyber, gestione dinamica delle chiavi, protezione del software di bordo e valutazioni elettromagnetiche secondo standard come Common Criteria e FIPS.

L'analisi del rischio emerge come un processo essenziale, in grado di garantire la resilienza dei sistemi attraverso l'identificazione delle minacce, la valutazione delle vulnerabilità e l'implementazione di misure di mitigazione. Questo processo deve essere continuo e adattarsi ai cambiamenti del contesto geopolitico e alle evoluzioni tecnologiche, al fine di mantenere un elevato livello di sicurezza nel tempo.

In conclusione, la protezione dei dati e dei sistemi spaziali richiede un'attenzione costante e un approccio multidisciplinare, che integri competenze tecniche, normative e di gestione del rischio.

Solo attraverso una strategia di sicurezza ben strutturata e proattiva è possibile affrontare efficacemente le sfide poste dai cyber attacchi e garantire la sicurezza delle infrastrutture spaziali in un contesto globale sempre più interconnesso e vulnerabile.

Daniele Frasca, *Security Advisor, Thales Alenia Space Italia*

BIOGRAFIA

Daniele Frasca

Daniele Frasca, Ingegnere elettronico, attualmente ricopre il ruolo di Security Advisor dell'Amministratore Delegato di Thales Alenia Space Italia; è inoltre Responsabile del Dipartimento di Cyber Security Engineering.

Con oltre venti anni di esperienza nell'ingegneria della sicurezza e nella cybersecurity applicata ai Sistemi spaziali, ha lavorato su importanti programmi come COSMO-SkyMed, SICRAL, Copernicus e MUSIS.

Ha pubblicato numerosi lavori nel campo della sicurezza e della cybersecurity per i sistemi spaziali.

White Paper

INDUSTRIAL CYBERSECURITY

Download gratuito su www.ictsecuritymagazine.com

La governance di sicurezza del Programma spaziale europeo

IL QUADRO LEGALE E IL PROGRAMMA SPAZIALE EUROPEO

Il Trattato di Lisbona[1] stabiliva che l'Unione potesse perseguire una politica spaziale europea, promuovendo iniziative comuni, sostenendo la ricerca e lo sviluppo tecnologico e coordinando gli sforzi necessari per l'esplorazione e l'utilizzo dello spazio. Queste iniziative – recita il Trattato – possono assumere la forma di un Programma spaziale europeo: pertanto le iniziative del Parlamento europeo e del Consiglio, come il Programma spaziale stesso o lo *Space working party,* possono essere ricondotte al Trattato.

Nel 2021 il Regolamento (UE) 2021/696, che abrogava i precedenti, istituiva il programma spaziale dell'Unione europea e sanciva la nascita dell'Agenzia dell'Unione europea per il programma spaziale (EUSPA). In aggiunta ai componenti Galileo e PRS, EGNOS, Copernicus, SSA/SST e GOVSATCOM, ricompresi nel Regolamento (UE) 2021/696, possiamo considerare anche il Programma dell'Unione per una connettività sicura (IRIS^2) introdotto dal Regolamento (UE) 2023/588.

Di fondamentale importanza è altresì la decisione (PESC) 2021/698, che definisce i meccanismi e il ruolo Consiglio dell'Unione europea e dell'Alto Rappresentante per prevenire una minaccia alla sicurezza dell'Unione o di uno o più dei suoi Stati membri, o per attenuare le conseguenze di un danno grave agli interessi essenziali dell'Unione o di uno o più dei suoi Stati membri, derivante dal dispiegamento, dal funzionamento o dall'uso dei sistemi istituiti e dei servizi forniti nell'ambito delle componenti del programma spaziale dell'Unione, oppure in caso di minaccia al funzionamento di uno di tali sistemi o alla fornitura dei servizi.

ALCUNI PRINCIPI

Al fine di comprendere le dinamiche e la *governance* degli aspetti di sicurezza, occorre considerare due principi fondamentali.

1. Il primo è quello sancito dall'articolo 4 (2) del Trattato sull'Unione europea[2], secondo il quale **la sicurezza nazionale resta competenza esclusiva di ciascuno Stato membro**. Da qui discende una notevole capacità degli Stati membri di direzionare (cd. *steering*), a livello degli organi comunitari, i vari dossier con impatti sulla sicurezza, compresi quelli relativi al settore spaziale.
2. Il secondo aspetto è legato alla giurisdizione delle regole di sicurezza: a ogni istituzione europea, come alle agenzie da essi coordinate, si applicano le regole di quella istituzione. Nonostante le regole di *information assurance*, COMSEC e *crypto* discendano tutte, per som-

1. Il Trattato di Lisbona modifica il Trattato sull'Unione Europea e il Trattato che istituisce la Comunità Economica Europea (2007/C 306/01), articolo 127(bis)

2. Trattato sull'Unione europea (TUE) (Maastricht, 7 febbraio 1992) modificato dal Trattato di Lisbona

mi capi, da quelle del **Consiglio[3], alla Commissione, al Parlamento e al Servizio Europeo di Azione Esterna (EEAS) si applicano le proprie regole di sicurezza**. Nel Programma spaziale il medesimo principio si applica anche all'Agenzia Spaziale Europea (ESA) e all'Agenzia per i Programmi Spaziali Europei (EUSPA). Non esistono, conseguentemente, un *corpus* unico di regole di sicurezza e un'unica Autorità di Sicurezza a livello del Programma spaziale, bensì regole diverse, anche se omogenee.

UNA GOVERNANCE MULTILIVELLO

Il Regolamento spaziale ha ribadito due principi, ovvero (1) quello secondo cui bisogna **tenere conto dell'esperienza acquisita dagli Stati membri nel settore della sicurezza** e ispirarsi alle loro migliori pratiche; e (2) l'applicabilità delle regole di sicurezza del Consiglio e della Commissione, che prevedono, tra le altre cose, una **separazione tra le funzioni operative e di accreditamento.**

La Commissione Europea (DG DEFIS), quale *programme manager*, ha la responsabilità generale dell'attuazione del programma anche nel settore della sicurezza, fatte salve le prerogative degli Stati membri in materia di sicurezza nazionale.

Con il supporto di EUSPA, garantisce:

a) la protezione dell'infrastruttura (sia spaziale sia di terra) e la fornitura di servizi, in particolare contro gli attacchi fisici e informatici, incluse le interferenze con i flussi di dati;

b) il controllo e la gestione dei trasferimenti di tecnologia;

c) lo sviluppo e la conservazione all'interno dell'Unione delle competenze e delle conoscenze acquisite;

d) la protezione delle informazioni sensibili non classificate e delle informazioni classificate.

Sulla base dell'analisi del rischio e delle minacce per ciascun componente, la Commissione definisce i requisiti di sicurezza di quel componente[4] e l'identificazione della struttura per il monitoraggio della sicurezza. Per questi aspetti la Commissione è assistita, *ratione materiae*, dal comitato di programma in configurazione di sicurezza; i lavori sono svolti tramite gruppi di lavoro composti dagli esperti degli Stati membri.

EUSPA, oltre a contribuire alla sicurezza del Programma e a supportare la Commissione nella definizione degli aspetti di sicurezza, è responsabile per la sicurezza operativa dei componenti per i quali è responsabile della gestione (*component manager*), come ad esempio Galileo.

Il comitato di accreditamento di sicurezza (SAB, *Security Accreditation Board*), istituito presso EUSPA, è responsabile di tutte le attività necessarie a ottenere e mantenere l'accreditamento di tutti i componenti del Programma, incluse eventuali interconnessioni con altri sistemi o sottosistemi.

---

3. Decisione del Consiglio del 23 settembre 2013 sulle norme di sicurezza per proteggere le informazioni classificate UE (2013/488/UE)

4. I requisiti generali di sicurezza sono adottati quali atti di esecuzione (implementing acts), dopo l'approvazione degli Stati membri nel comitato del programma in configurazione di sicurezza

Il SAB adotta, in modo strettamente indipendente, le decisioni di accreditamento riferite al lancio di satelliti; le autorizzazioni necessarie a operare sistemi, sottosistemi o servizi e al dispiegamento di nuove configurazioni (*system releases*), incluso il segnale nello spazio; e l'autorizzazione a gestire le stazioni terrestri. Infine, per quel che concerne il *Public Regulated Service* (PRS), adotta decisioni relative all'autorizzazioni delle entità industriali.

Con un esempio pratico, all'atto dell'avvio di un nuovo componente del Programma che implementa caratteristiche di sicurezza, sarà la Commissione a definire – con il supporto degli esperti degli Stati membri nonché attraverso il Comitato di programma in configurazione sicurezza e i propri gruppi di lavoro – i *general security requirements* e gli altri requisiti di sicurezza (e.g. aspetti COMSEC, di sicurezza industriale) e a monitorarne l'implementazione da parte di EUSPA ed ESA. Essi, a loro volta, implementeranno i requisiti nell'ambito delle loro precipue competenze (e.g. EUSPA quale *service manager*, ESA quale *system design authority*) e li declineranno ulteriormente in requisiti di livello inferiore, applicandoli altresì ai contratti o *grant* classificati che EUSPA ed ESA gestiscono quali stazioni appaltanti.

Il SAB – che, ricordiamo, è composto anch'esso dagli esperti degli Stati membri, la Commissione e il Servizio Europeo di Azione Esterna – verifica, tramite l'accreditamento di sicurezza, la corretta implementazione dei requisiti (*compliance*) prima di autorizzare (tramite ATO, *authorization to operate*) o meno le operazioni del componente stesso, di sottosistemi, network, apparati.

La sicurezza del Programma spaziale dell'Unione è, quindi, garantita tramite una *governance* multilivello nella quale le decisioni finali sono prese in maniera collettiva e adottate in un contesto di responsabilità condivisa per la sicurezza dell'Unione e degli Stati membri.

L'AUTONOMIA STRATEGICA DELLA UE

Con il Regolamento 2021/696, la UE ha deciso di dotarsi di uno strumento specifico per preservare la sicurezza, l'integrità e la resilienza dei sistemi operativi dell'Unione. L'Articolo 24 si pone, infatti, l'obiettivo di essere un ulteriore scudo a salvaguardia della tecnologia e delle catene di fornitura (*supply chain*) fondamentali europee, al fine di garantirne l'autonomia strategica e preservare, al contempo, un'economia aperta.

I medesimi principi sono applicati anche al Programma IRIS[5].

L'Articolo 24, che viene implementato nelle condizioni di ammissibilità e di partecipazione (*participating conditions*) delle entità che partecipano agli appalti, alle sovvenzioni o ai premi (*procurement* e *grant*), prevede che:

a. il soggetto giuridico ammissibile è stabilito in uno Stato membro e le sue strutture di gestione esecutiva sono stabilite nello stesso Stato membro;

b. il soggetto giuridico ammissibile si impegna a svolgere tutte le attività pertinenti in uno o più Stati membri;

5. Articolo 22 del Regolamento (UE) 2023/588

c. il soggetto giuridico ammissibile non è soggetto al controllo di un paese terzo o di un soggetto di paese terzo.

Il meccanismo prevede, quindi, un "controllo all'ingresso" al fine di assicurarsi che i soggetti giuridici non siano sotto il controllo di attori terzi, ovvero che non vi sia la possibilità per questi ultimi di esercitare, direttamente o indirettamente, un'influenza determinante attraverso uno o più soggetti giuridici intermedi.

Come monitorano gli Stati membri l'implementazione dell'Articolo 24? Attraverso il Comitato di programma in configurazione sicurezza: le autorità competenti degli Stati membri forniscono pareri sulla definizione delle condizioni di partecipazione e, soprattutto, verificano se i soggetti giuridici in parola abbiano attuato misure sufficienti ad assicurare la protezione delle Informazioni Classificate Europee (EUCI) nonché ad assicurare l'integrità, la sicurezza e la resilienza delle componenti del programma, del loro funzionamento e dei loro servizi.

Sebbene formalmente indipendente dal Programma spaziale, è opportuno menzionare un altro strumento che contribuisce a rafforzare la competitività dell'Unione, dotando gli Stati membri e la Commissione di un mezzo per affrontare in modo globale i rischi per la sicurezza (e per l'ordine pubblico).

Il **Regolamento (UE) 2019/452**[6], ispirato tra gli altri al D. legge n. 21 del 2012[7] italiano che istituisce il *golden power*, definisce **un quadro per il controllo degli investimenti esteri diretti nell'Unione**. Tale Regolamento rappresenta, quindi, un ulteriore strumento per verificare, in cooperazione con gli Stati membri, se nell'ambito del Programma spaziale è in programma – o è stato realizzato – un investimento estero e intervenire di conseguenza.

IL CONTROLLO DELL'EXPORT DELLA TECNOLOGIA AD USO DUALE

Pur ribadendo la natura civile del Programma spaziale, il Regolamento 2021/696 sottolinea quanto, storicamente, le attività spaziali siano legate alla sicurezza; e quanto i componenti, gli apparati, i sistemi, i dati e le applicazioni abbiano una natura duale.

Il regime di controllo delle esportazioni e trasferimenti ad uso duale[8] prevede che gli Stati membri possano subordinare l'autorizzazione o il transito di determinati apparati, sistemi, software, applicazioni all'autorizzazione delle competenti autorità nazionali. Il materiale aerospaziale, il software

6. Regolamento (UE) 2019/452 del Parlamento Europeo e del Consiglio del 19 marzo 2019, che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione

7. Decreto legge 15 marzo 2012, n. 21 "Norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni"

8. Regolamento (UE) 2021/821 del Parlamento Europeo e del Consiglio del 20 maggio 2021, che istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso

crittografico e gli algoritmi, ad esempio, sono ricompresi nella normativa europea per il controllo dell'export.

LA STRATEGIA EUROPEA PER LA SICUREZZA E LA DIFESA

Il Programma spaziale, come la *governance* di sicurezza con esso stabilita, non rappresenta un monolite granitico o immutabile nel corso del suo periodo di validità[9].

Nel 2023, con la **Strategia Europea per la Sicurezza e la Difesa**[10], sono state infatti avviate iniziative per difendere gli interessi strategici della UE, rafforzarne la postura strategica e la capacità deterrente verso le minacce nello – e provenienti dallo – spazio.

Tra queste iniziative la Commissione Europea ha avviato, con il supporto di EUSPA, l'**ISAC (*Information Sharing and Analysis Centre*)**, un centro di fusione di informazioni circa le minacce, vulnerabilità, *trend* e migliori pratiche relativi alla sicurezza e alla cybersicurezza, al fine di aumentare le capacità di resilienza dell'industria spaziale. Il Centro è rivolto all'industria europea, incluso il settore New Space, a università e centri di ricerca, nonché ad agenzie spaziali, ESA e CERT (*Computer Emergency Response Teams*) nazionali.

Per quanto concerne gli aspetti di cybersicurezza, è da sottolineare altresì il rinnovato interesse a incrementare lo scambio informativo. Ciò vede, quale perno principale, i centri operativi di sicurezza (**SOC, *Security Operation Centre***) dei componenti del Programma. In particolare, sarà aumentata la cooperazione con il CERT-EU (il *Computer Security Incident Response Team* delle istituzioni della UE) e con ENISA (Agenzia dell'Unione europea per la cibersicurezza).

È altresì verosimile ritenere che anche il **C-SOC (*Cyber-Security Operations Centre*)**[11] di ESA verrà incluso, con modalità da definire, in questo **sistema di sistemi**.

Infine, nel panorama dei futuri sviluppi tecnologici, meritano un cenno le comunicazioni e la sicurezza quantistiche.

Al progetto **SAGA (*Security And cryptoGrAphic mission*)**[12], che prevede la creazione di una serie di satelliti quantici gestiti da ESA e un network di stazioni terrestri gestite dalla Commissione Europea (DG CONNECT), si è affiancata l'iniziativa UE **EuroQCI**[13]. Lo scopo del progetto è sviluppare un

9. Il Regolamento copre il quadro finanziario pluriennale (MFF, Multiannual Financial Framework) 2021-2027

10. OIN(2023) 9 final, Joint communication to the European Parliament and the Council "European Union Space Strategy for Security and Defence"

11. Il C-SOC fornisce ad ESA capacità di monitoraggio ed implementazione preventiva e reattiva delle misure di cybersicurezza riferite agli assetti spaziali gestiti da ESA

12. https://www.esa.int/ESA_Multimedia/Images/2019/04/SAGA_for_quantum_key_distribution

13. https://digital-strategy.ec.europa.eu/it/policies/european-quantum-communication-infrastructure-euroqci

segmento terrestre – basato su reti di comunicazione in fibra ottica che collegano siti strategici a livello nazionale – e un segmento spaziale, basato su satelliti quantistici: EuroQCI sarà parte integrante di IRIS.

La rivoluzione quantistica, che pure presenta una serie di sfide non banali (e.g. per l'accreditamento di sicurezza), è un elemento che permetterà un significativo salto di qualità, aumentando il livello di resilienza dei nostri sistemi spaziali e la capacità di affrontare minacce di livello strategico.

Antonio Piccirillo, *Programme Officer presso la Commissione Europea, Direzione Generale Defense Industry and Space (DG DEFIS)*

BIOGRAFIA

Antonio Piccirillo

Attualmente Programme Officer nella Direzione Generale Industria della difesa e spazio (DG DEFIS) della Commissione Europea, da Ufficiale dell'Esercito Italiano è stato impiegato in Italia e in vari teatri operativi, in ruoli di comando nel settore delle telecomunicazioni e dell'information security. Si è occupato di gestione delle crisi presso l'Ufficio del Consigliere Militare della Presidenza del Consiglio dei Ministri ed è stato parte dello staff dell'Autorità Nazionale Responsabile per il Galileo PRS. Dal 2019 è nel team che si occupa della definizione e gestione degli aspetti di sicurezza del Programma Spaziale dell'Unione.

White Paper

LA DIGITAL FORENSICS NEL PROCESSO PENALE

Download gratuito su www.ictsecuritymagazine.com

Aspetti di Cyber-Space Security e interessi dei Threat Actor

INTRODUZIONE

Oggi l'Italia, molto più di quanto spesso si riconosca, svolge un ruolo fondamentale nelle missioni e nelle attività spaziali a livello mondiale, vantando il secondo maggior numero di veicoli in orbita tra le nazioni europee. Inoltre, contribuisce in modo essenziale alle missioni dell'Agenzia Spaziale Europea (ESA) e della NASA; in termini di lanciatori spaziali svolge un ruolo sostanziale, contribuendo all'accesso autonomo europeo allo spazio.

Da un punto di vista economico, l'Italia è il secondo Paese in Europa per investimenti nel settore. Il panorama industriale è composto da più di 200 aziende (in maggioranza PMI) e genera ricavi complessivi per oltre 2 miliardi di euro.

Questa *leadership* globale sull'industria spaziale è il risultato di decenni di intenso e ponderato sviluppo dell'ecosistema spaziale italiano e delle sue relazioni con il resto del mondo.

La maturità nell'industria spaziale e l'attività economica del Paese indicano che l'Italia sta entrando in una nuova era della sua storia spaziale.

In un contesto globale in continua evoluzione, tale ruolo richiede un solido assetto istituzionale, basato su una visione coerente, una *governance* efficiente e un alto livello di consapevolezza; ma anche un costante aggiornamento e potenziamento del *know-how* e delle capacità attraverso piani e investimenti adeguati.

Nel campo dell'EO (*Earth Observation*), il nostro

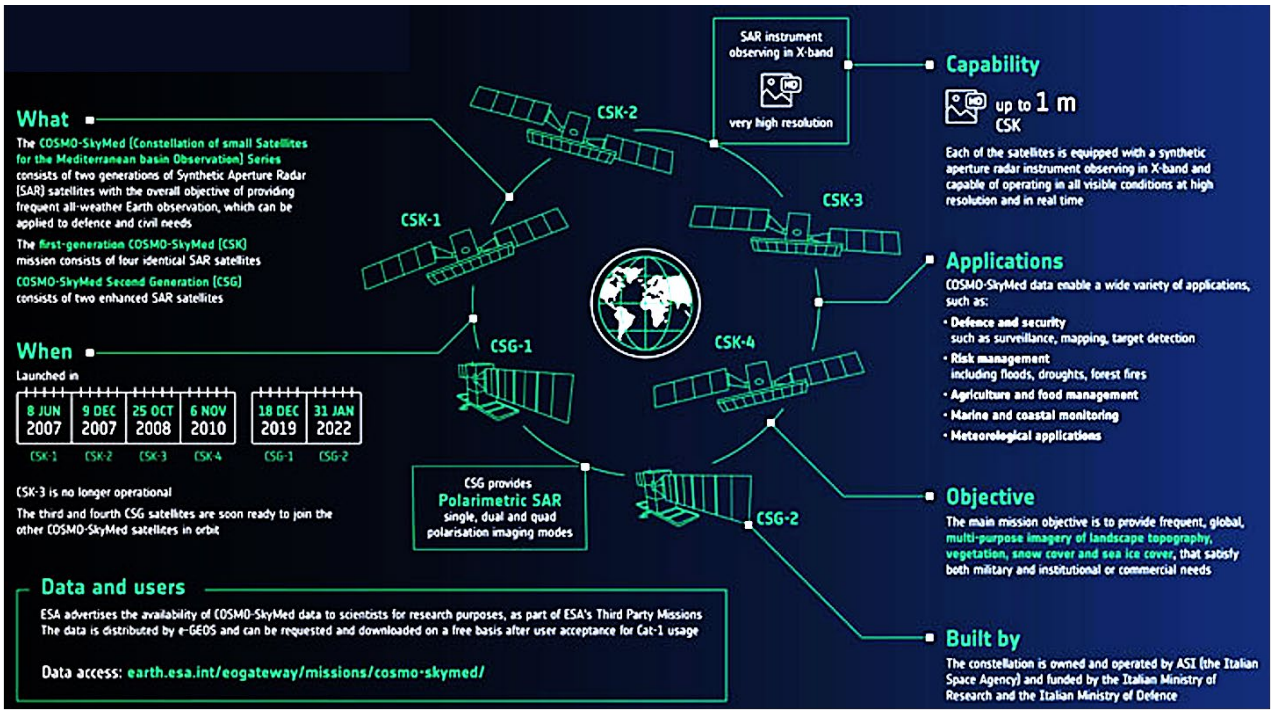


Fig. 1 – Missioni della COSMO-SkyMed

Paese ha una competenza specifica tale da poter dare un grande contributo agli sforzi europei. Roma è stata pioniera di un approccio *dual-use* con il lancio della costellazione di satelliti SAR (*Synthetic Aperture Radar*) COSMO-SkyMed (*Constellation of small Satellites for the Mediterranean basin Observation*), composta da quattro asset di prima generazione e due di seconda, mentre è già prevista una terza generazione.

Grazie al programma congiunto tra il Ministero della Difesa e l'ASI, il primo satellite COSMO è stato lanciato nel 2007, mentre il sesto asset è stato lanciato a bordo di un razzo SpaceX Falcon 9 nel gennaio 2022. Si ricorda che COSMO-SkyMed fornisce servizi critici per la geo-intelligenza, le operazioni di sicurezza e difesa, la navigazione marittima, la gestione di emergenze e disastri e altre attività. In quanto tale, COSMO-SkyMed è un ottimo esempio di come gli asset a duplice uso ottimizzino le risorse e prevedano un'infrastruttura piuttosto unica.

Sempre più frequentemente i satelliti sono oggetti di attacchi, nonostante i trattati e i regimi esistenti vietino l'armamento dello spazio. Un primo semplice esempio è l'impiego di tecniche di guerra elettronica (EW) per disturbare o interrompere le loro funzioni critiche senza creare detriti.

Allo stesso modo, a causa della loro funzione di connettività, i mezzi spaziali sono vulnerabili ai continui attacchi informatici, e l'offesa gode di diversi vantaggi strutturali rispetto alla difesa.

Le agenzie di *intelligence* statunitensi avvertono dell'aumento degli attacchi informatici contro le compagnie spaziali da parte di servizi di intelligence stranieri: l'FBI, il National Counterintelligence and Security Center (NCSC) e l'Air Force Office of Special Investigations (AFOSI) affermano che *"Foreign intelligence entities (FIEs) recognize the importance of the commercial space industry to the US economy and national security, including the growing dependence of critical infrastructure on space-based assets… They see US space-related innovation and assets as potential threats as well as valuable opportunities to acquire vital technologies and expertise. FIEs use cyberattacks, strategic investment (including joint ventures and acquisitions), the targeting of key supply chain nodes, and other techniques to gain access to the US space industry".*

Nell'aprile del 2023, l'influente *Cyberspace Solarium Commission* ha dichiarato alla Casa Bianca che avrebbe dovuto nominare formalmente lo spazio come settore delle infrastrutture critiche e adottare misure per proteggere i satelliti e altri sistemi spaziali dagli attacchi informatici.

Inoltre, la stessa Commissione ha affermato che la minaccia proveniente da Russia e Cina sta crescendo e che entrambi i paesi *"hanno messo i sistemi spaziali americani e dei partner nel loro mirino, come dimostrato dai test sulle capacità anti-satellite (ASAT)".*

Le preoccupazioni per il settore sono aumentate dopo l'attacco della Russia alla compagnia satellitare Viasat, all'inizio dell'invasione dell'Ucraina da parte di Mosca, nel tentativo di interrompere le comunicazioni.

TIPOLOGIE DI ARMI CONTROSPAZIALI

Il CSIS ha lavorato per definire una tassonomia delle armi "controspaziali" sulla base dei loro effetti, per le modalità di dispiegamento, per la loro

rilevabilità, per la loro capacità di essere attribuite a una fonte e per il livello di tecnologia e di risorse necessarie per il loro sviluppo e la loro messa in campo.

Le armi controspaziali sono distinte in quattro grandi gruppi di capacità.

1. **Kinetic Physical Weapons**: le armi cinetiche fisiche contro lo spazio cercano di colpire direttamente o di far esplodere una testata vicino a un satellite o a una stazione terrestre. Le tre forme principali di attacco fisico cinetico sono le armi antisatellite (ASAT) a gittata diretta, le armi ASAT co-orbitali e gli attacchi alle stazioni terrestri. Le armi ASAT a caduta diretta vengono lanciate dalla Terra su una traiettoria suborbitale per colpire un satellite in orbita, mentre le armi ASAT co-orbitali vengono prima messe in orbita e poi successivamente manovrate verso, o vicino, al loro bersaglio in orbita. Queste manovre sono comunemente note come operazioni di *rendezvous* e prossimità (RPO). Gli attacchi alle stazioni di terra sono mirati ai siti terrestri responsabili del comando e del controllo dei satelliti o del trasferimento dei dati delle missioni satellitari agli utenti. Un attacco alle stazioni di terra ha il vantaggio di colpire molti satelliti di una costellazione (che comunicano con la stazione di terra) piuttosto che richiedere armi multiple per colpire i singoli satelliti.

   Gli attacchi fisici cinetici tendono a causare danni irreversibili ai sistemi colpiti e dimostrano una forte dimostrazione di forza, che sarebbe probabilmente attribuibile e visibile pubblicamente. Un attacco fisico cinetico riuscito nello spazio produrrà detriti orbitali, che possono colpire indiscriminatamente altri satelliti in orbite simili. Questi tipi di attacchi sono tra le uniche azioni di contrasto allo spazio che possono comportare la perdita diretta di vite umane se mirati a stazioni di terra con equipaggio o a satelliti in orbite in cui sono presenti esseri umani, come la Stazione Spaziale Internazionale (ISS) in orbita terrestre bassa (LEO). Ad oggi, nessun Paese ha condotto un attacco fisico cinetico contro il satellite di un altro Paese, ma quattro Paesi – Stati Uniti, Russia, Cina e India – hanno testato con successo armi ASAT a gittata diretta contro i propri satelliti. Anche l'Unione Sovietica ha testato armi ASAT cinetiche co-orbitali già negli anni Sessanta.

2. **Non-kinetic Physical Weapons:** hanno effetti fisici sui satelliti o sui sistemi terrestri senza entrare in contatto fisico con essi. I laser possono essere utilizzati per abbagliare temporaneamente o accecare permanentemente i sensori dei satelliti o per provocare il surriscaldamento dei componenti. Le armi a microonde ad alta potenza (HPM) possono disturbare l'elettronica di un satellite o causare danni permanenti ai circuiti elettrici e ai processori di un satellite. Un ordigno nucleare detonato nello spazio può creare un ambiente ad alta radiazione e un impulso elettromagnetico (EMP) con effetti indiscriminati sui satelliti nelle orbite interessate. Gli attacchi non cinetici operano alla velocità della luce e, in alcuni casi, possono essere meno visibili a osservatori terzi e più difficili da attribuire. I satelliti possono essere bersagliati con laser e armi HPM da siti terrestri

o navali, da piattaforme aeree o da altri satelliti. Un sistema di laser per satelliti richiede un'elevata qualità del fascio, un'ottica adattiva (se utilizzato attraverso l'atmosfera) e un controllo avanzato del puntamento per orientare con precisione il fascio laser: una tecnologia costosa e che richiede un elevato grado di sofisticazione. Un laser può essere efficace contro un sensore su un satellite solo se si trova all'interno del campo visivo del sensore, rendendo possibile l'attribuzione dell'attacco alla sua origine geografica approssimativa. Un'arma HPM può essere usata per disturbare l'elettronica di un satellite, corrompere i dati memorizzati, causare il riavvio dei processori e, a livelli di potenza più elevati, causare danni permanenti ai circuiti elettrici e ai processori. Gli attacchi HPM possono essere più difficili da attribuire perché l'attacco può provenire da diverse angolazioni, anche da altri satelliti in orbita. Sia per le armi laser che per quelle HPM, l'attaccante può avere una capacità limitata di sapere se l'attacco ha avuto successo perché non è probabile che produca indicatori visibili. L'uso di un'arma nucleare nello spazio avrebbe effetti indiscriminati e su larga scala che sarebbero attribuibili e visibili al pubblico. Una detonazione nucleare nello spazio colpirebbe immediatamente i satelliti nel raggio d'azione dell'EMP e creerebbe un ambiente ad alte radiazioni che accelererebbe il degrado dei componenti dei satelliti a lungo termine per i satelliti non schermati nel regime orbitale interessato. La detonazione di armi nucleari nello spazio è vietata dal Trattato per la messa al bando parziale degli esperimenti nucleari del 1963, che conta più di 100 firmatari, tra i quali però non figurano né la Cina né la Corea del Nord.

3. **Electronic Weapons**: hanno come obiettivo lo spettro elettromagnetico attraverso il quale i sistemi spaziali trasmettono e ricevono dati. I dispositivi di disturbo interferiscono con le comunicazioni verso o dai satelliti generando rumore nella stessa banda di radiofrequenza (RF). Un disturbatore di *uplink* interferisce con il segnale che va dalla Terra a un satellite, come l'*uplink* di comando e controllo; i disturbatori di *downlink* mirano al segnale proveniente da un satellite che si propaga fino agli utenti sulla Terra. Lo *spoofing* è una forma di attacco elettronico in cui l›aggressore inganna il ricevitore facendogli credere che un segnale falso, prodotto dall›aggressore, sia il vero segnale che sta cercando di ricevere. Uno *spoofer* può essere utilizzato per iniettare false informazioni in un flusso di dati o, *in extremis*, per impartire falsi comandi a un satellite per interromperne le operazioni. I terminali utente dotati di antenne omnidirezionali, come molti ricevitori GPS e telefoni satellitari, hanno un campo visivo più ampio e quindi sono suscettibili di *jamming* e *spoofing* del *downlink* da una gamma più ampia di angolazioni a terra. Le forme di attacco elettronico possono essere difficili da rilevare o distinguere dalle interferenze accidentali, rendendo più difficile l'attribuzione e la consapevolezza. Sia il *jamming* che lo *spoofing* sono forme di attacco reversibili, perché le comunicazioni possono tornare normali una volta rimosso il segnale di disturbo.

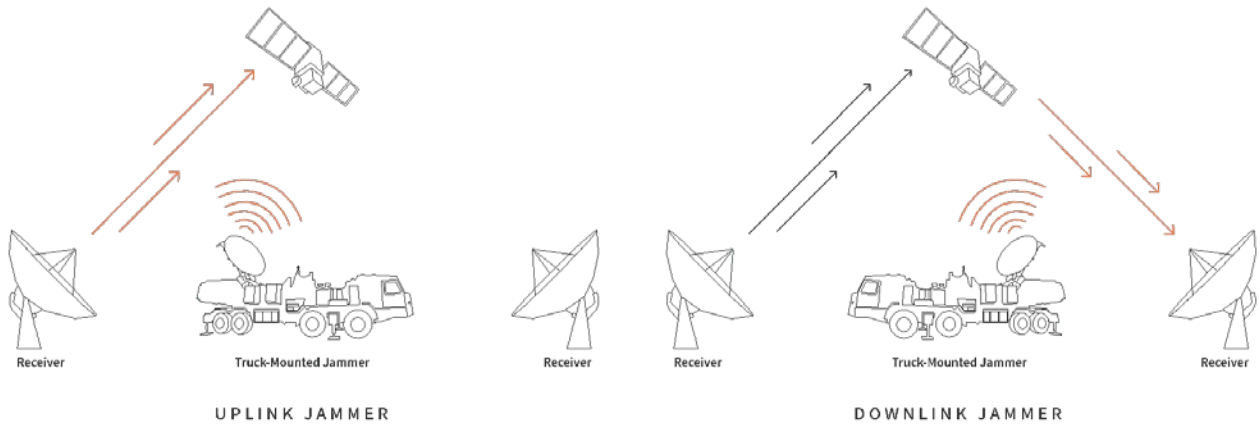


Fig. 2 – rappresentazioni di attacchi basate su jamming

Grazie a un tipo di *spoofing* chiamato *"meaconing"*, anche il segnale GPS militare P(Y) crittografato può essere spoofato. Il *meaconing* non richiede la decifrazione della crittografia, perché si limita a ritrasmettere una copia ritardata del segnale originale senza decifrarlo o alterare i dati. La tecnologia necessaria per disturbare e alterare molti tipi di segnali satellitari è disponibile in commercio e poco costosa, il che ne rende relativamente facile la proliferazione tra gli attori statali e non statali.

Questa categoria include *jamming* e *spoofing* del sistema globale di navigazione satellitare (GNSS) e comunicazioni satellitari (SATCOM). Lo *spoofing* è una forma di attacco elettronico in cui un aggressore inganna il ricevente facendogli credere che un falso il segnale prodotto dall›attaccante è il segnale reale che sta cercando di ricevere. Può influenzare i segnali GNSS dal Sistema Globale di posizionamento (GPS), Galileo, BeiDou e i sistemi GLONASS, oltre ai segnali satellitari non criptati.

4. **Cyber Weapons**: l'ultima categoria riguarda le operazioni informatiche e comprende qualsiasi attività offensiva nel cyberspazio che abbia come obiettivo sistemi spaziali, comprese le infrastrutture terrestri, terminali satellitari, porti spaziali e veicoli spaziali. Le operazioni informatiche possono distruggere o disattivare un sistema specifico; ma possono anche essere utilizzate per interrompere temporaneamente le comunicazioni o per svolgere attività di spionaggio, compreso l'accesso a informazioni tecniche proprietarie o sensibili su una rete bersaglio. La stessa complessità rende difficile riuscire a comprendere e classificare con precisione la maggior parte dei comportamenti ostili dei satelliti russi e cinesi. In generale, è difficile categorizzare in modo netto queste capacità.

Mentre le forme di attacco elettronico tentano di interferire con la trasmissione dei segnali RF, gli attacchi cyber prendono di mira i dati stessi e i sistemi che utilizzano, trasmettono e controllano il flusso di dati. Gli attacchi informatici ai satelliti possono

essere utilizzati per monitorare i modelli di traffico dati, intercettare o inserire dati o comandi falsi e/o corrotti in un sistema. Questi attacchi possono colpire le stazioni di terra, le apparecchiature degli utenti finali o i satelliti stessi. Sebbene gli attacchi informatici richiedano un alto grado di comprensione dei sistemi presi di mira, non richiedono necessariamente risorse significative per essere condotti.

La barriera all'ingresso è relativamente bassa e gli attacchi informatici possono essere appaltati a gruppi privati o a singoli individui: anche se uno Stato o un attore non statale non dispone di capacità informatiche interne, può comunque rappresentare una minaccia informatica.

Un attacco informatico ai sistemi spaziali può comportare la perdita di dati o servizi forniti da un satellite, con effetti sistemici diffusi se usato contro un sistema come il GPS. I cyberattacchi possono avere effetti permanenti se, ad esempio, un avversario prende il controllo di un satellite attraverso il suo sistema di comando e controllo. Un aggressore potrebbe interrompere tutte le comunicazioni e danneggiare in modo permanente il satellite, impartendo comandi che gli fanno consumare propellente o danneggiare l'elettronica e i sensori.

L'attribuzione accurata e tempestiva di un attacco informatico può essere difficile perché gli aggressori possono utilizzare una serie di metodi per nascondere la propria identità, come ad esempio l'utilizzo di server dirottati quando viene lanciato un attacco.

Una prima distinzione tra le possibili tipologie di attacchi cyber è riportata nella tabella 1.

Gli utenti e i settori aerospaziale, della difesa e delle telecomunicazioni fanno sempre più affidamento sulle infrastrutture spaziali per le comunicazioni e la connettività in tutto il mondo.

Il settore privato ha ampliato la propria quota di mercato nell'industria satellitare per le comunicazioni e i trasferimenti di dati; e numerosi Paesi hanno progettato programmi per sviluppare rapidamente i propri programmi spaziali scientifici e

Types of Attack	*Data Interccept or Monitoring*	*Data Corruption*	*Seizure of Control*
Attribution	*Limited or uncertain attribution*	*Limited or uncertain attribution*	*Limited or uncertain attribution*
Reversibility	*Reversible*	*Reversible*	*Irreversible or reversible, depending on mode of attack*
Awareness	*May or may not be known to the public*	*Satellite operator will be aware; may or may not be known to the public*	*Satellite operator will be aware; may or may not be known to the public*
Attacker Damage Assessment	*Near real-time confirmation of success*	*Near real-time confirmation of success*	*Near real-time confirmation of success*
Collateral Damage	*None*	*None*	*Could leave target satellite disabled and uncontrollable*

Tab. 1 - Tipologie di Attacchi Cyber

militari nei prossimi anni, ampliando la superficie di attacco potenziale per gli attori malintenzionati.

Gli enti governativi hanno identificato questo settore come una potenziale minaccia emergente e hanno avviato iniziative per affrontare la sicurezza informatica nello spazio.

Mandiant, prevedendo che l'attività di minaccia informatica nello spazio aumenterà nel lungo periodo, man mano che le imprese e i programmi governativi raggiungeranno le stelle, ha identificato tre rischi principali per il settore aerospaziale e i fornitori di servizi satellitari:

- *Data Theft Operations*: le minacce sponsorizzate dallo Stato prendono di mira le imprese aerospaziali e le agenzie governative per ottenere un accesso persistente, nonché il furto di credenziali e di dati per supportare i programmi spaziali della nazione, evitando cicli di ricerca costosi e dispendiosi in termini di tempo. Analogamente, gli attori dello spionaggio informatico possono sfruttare l'accesso ai sistemi di comunicazione satellitare per intercettare canali di comunicazione mirati.
- *Disruptive and Destructive Attacks*: gli attori delle minacce possono sfruttare questa dipendenza dalle infrastrutture spaziali per condurre operazioni di disturbo mirate alle infrastrutture satellitari per bloccare o manipolare le comunicazioni o i trasferimenti di dati. Inoltre, gli attori malintenzionati possono intercettare i dati e utilizzarli per i propri scopi, o corromperli in modo da renderli inutilizzabili per il destinatario previsto.
- *Space Junk*: con l'aumento del numero di dispositivi nell'orbita bassa terrestre, aumenta il rischio di collisioni tra gli oggetti che possono generare detriti più piccoli con nuove traiettorie, creare ulteriori rischi di collisioni e spingere all'impostazione di nuove traiettorie di volo per evitare i detriti. Inoltre, gli attori dello spionaggio possono utilizzare le informazioni destinate alla gestione del traffico spaziale per tracciare i dispositivi per future operazioni di disturbo o sfruttare le collisioni tra satelliti per operazioni informative.

PRINCIPALI THREAT ACTOR CHE HANNO ATTACCATO L'INDUSTRIA SPAZIALE

Gli analisti di Mandiant hanno osservato che i *threat actor* di tipo *State-Sponsored* cinesi, russi, nordcoreani e iraniani prendono di mira le imprese e le organizzazioni aerospaziali, al pari delle aziende delle Telco che supportano le infrastrutture spaziali, probabilmente come tecnica di *intelligence* finalizzata alla raccolta di informazioni per operazioni future.

La compromissione di queste organizzazioni può consentire ai *threat actor* di raccogliere informazioni sensibili a sostegno dei propri programmi aerospaziali militari e civili nazionali senza dover sostenere i cicli di ricerca e sviluppo, costosi e dispendiosi in termini di tempo.

La figura seguente mostra i principali gruppi *State-Sponsored* che hanno realizzato (o si presume abbiano realizzato) attacchi aventi oggetto agenzie spaziali nel periodo 2020-2022:

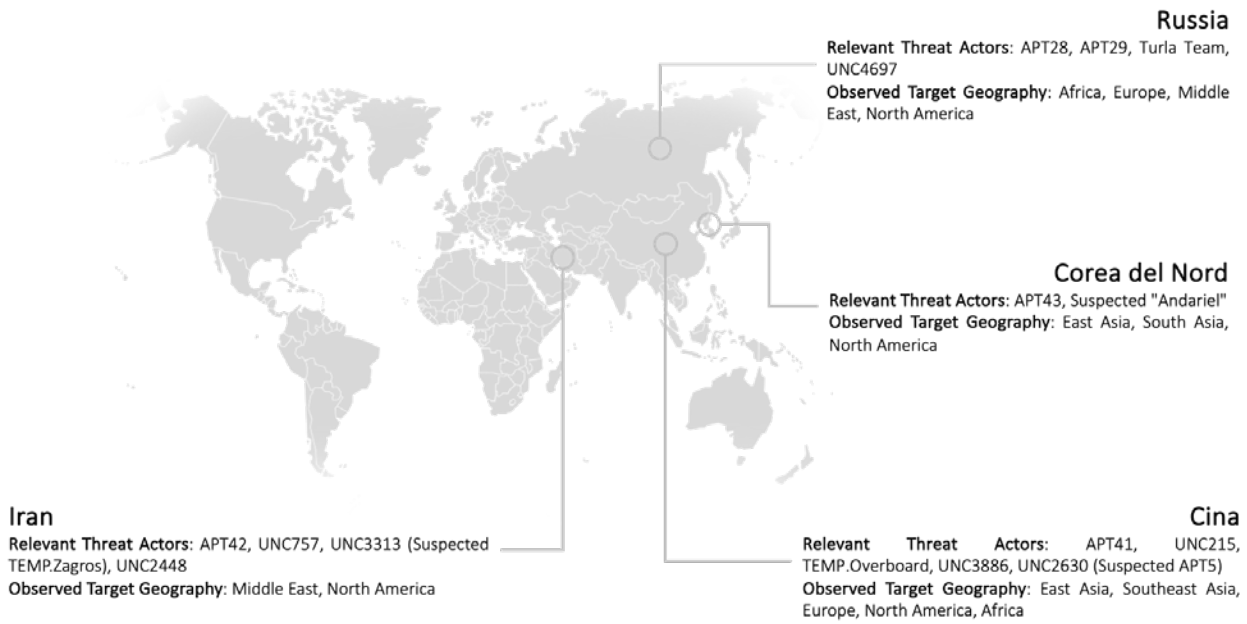


Fig. 3 – Mappa degli attaccanti State-Sponsored

Di seguito sono riportate le principali campagne rilevate dagli Stati:

- **Cina**: le operazioni di cyberspionaggio cinesi osservate che hanno preso di mira agenzie spaziali, aziende aerospaziali e di telecomunicazioni satellitari hanno probabilmente molteplici obiettivi, tra cui il sostegno allo sviluppo di programmi aerospaziali civili e militari, la raccolta di informazioni a lungo termine e il monitoraggio di sviluppi più tattici, ad esempio legati al conflitto in Ucraina. Tra le campagne di cyberspionaggio cinesi più significative degli ultimi anni contro le organizzazioni del settore aerospaziale, della difesa e delle telecomunicazioni si rilevano quella di APT41 dell'inizio del 2020, che ha sfruttato Citrix NetScaler/ADC (CVE-2019-19781); la campagna UNC2630 dell'inizio del 2021, che ha sfruttato uno *zero-day* in Pulse Secure VPN (CVE-2021-22893) comportando il furto di proprietà intellettuale a doppio uso e l'attività di UNC3886. Si rileva anche la campagna iniziata nel 2020 di TEMP.Overboard, che ha ripetutamente preso di mira un'azienda di telecomunicazioni satellitari dell'Asia orientale con e-mail di *spear-phishing* che hanno portato a distribuire *malware* FRONTSHELL, TSCOOKIE e FLAGPOLE; infine, un'operazione di spionaggio informatico cinese che utilizzava varianti aggiornate di SOFTSLING per colpire un produttore russo di armi e un'azienda che produce prodotti per comunicazioni sicure. Questa attività è probabilmente iniziata poco prima dell'invasione russa dell'Ucraina. Riteniamo che questa operazione faccia parte di una campagna più ampia della Cina che prende di mira la Russia prima e dopo l'invasione dell'Ucraina.

- **Russia**: le operazioni di cyberspionaggio russo rivolte a enti pubblici e privati nei settori delle telecomunicazioni, dell'aerospazio e della di-

fesa hanno probabilmente molteplici obiettivi, tra cui la raccolta di informazioni a lungo termine e il potenziale utilizzo di sistemi di telecomunicazione satellitare per mascherare il traffico malevolo. Operazioni più recenti, in particolare la compromissione del provider di Internet via satellite Viasat nel febbraio 2022, potrebbero anche rappresentare operazioni tattiche legate all'attuale conflitto in Ucraina, nonché potenziali ricognizioni per future campagne di spionaggio tradizionale e operazioni di disturbo.

Nel marzo 2023, Microsoft ha divulgato e rilasciato una *patch* per la vulnerabilità *zero-day* CVE-2023-23397 di Outlook che consente la raccolta di credenziali New Technology Lan Manager (NTLM). Gli analisti di Mandiant valutano che la vulnerabilità sia stata sfruttata dal *threat actor* UNC4697 almeno dall'aprile 2022, per prendere di mira entità in Europa occidentale e Asia centrale in ambito diplomatico, aerospaziale e della difesa, energetico e logistico. La Cybersecurity and Infrastructure Systems Agency (CISA) degli Stati Uniti ha indicato alla fine del 2022 che APT28 era responsabile della compromissione di una rete satellitare statunitense e di individui coinvolti nei settori delle infrastrutture critiche statunitensi. Mandiant ha denunciato pubblicamente la scoperta di una compromissione della catena di fornitura attuata distribuendo *malware* SUNBURST in una campagna ora attribuita ad APT29. L'operazione ha compromesso il software di gestione della rete di SolarWinds, Orion, compromettendo circa 18.000 reti in tutto il mondo, tra cui numerose agenzie governative europee e statunitensi nonché innumerevoli aziende private, comprese entità aerospaziali e di difesa, in tutto il mondo. Nel dicembre 2020 sono stati identificati i domini di Command & Control (C&C) del Turla Team, che si risolvono in indirizzi IP associati a fornitori di servizi Internet (ISP) che forniscono servizi basati su satellite. Anche se non possiamo confermare la motivazione dietro questa attività, è possibile che il Turla Team abbia dirottato le connessioni internet satellitari di *downlink* per oscurare la posizione della sua infrastruttura C&C

- **Iran**: le attività *State-Sponsored* iraniane colpiscono le agenzie spaziali, le organizzazioni aerospaziali e di telecomunicazioni satellitari, probabilmente per raccogliere informazioni a sostegno dello sviluppo del programma spaziale interno dell'Iran. A tale motivazione può essere legata la campagna tracciata da Proofpoint nel dicembre 2022 (ma iniziata nel 2020). A metà del 2021, sono stati pubblicati documenti file classificati presumibilmente interni al Corpo delle Guardie della Rivoluzione Islamica iraniana (IRGC) che dettagliavano la ricognizione su infrastrutture critiche civili, compresi i *water ballast systems* e i dispositivi di comunicazione satellitare marittima.

  Una versione personalizzata della *web shell* TANKSHELL è stata scoperta nel corso di un *Incident Response* da Mandiant presso un ente di servizi pubblici del Medio Oriente e un fornitore di telecomunicazioni satellitari nel giugno 2020. Sebbene l'attribuzione di questa attività sia incerta, le TTP impiegate di questo attacco e la similitudine a altre campagne suggeriscono un'associazione a gruppi iraniani.

  Nel settembre 2020 il Department of Justice

americano ha emesso un *indictment* contro tre gruppi iraniani per spionaggio informatico che, secondo quanto riferito, operavano per conto dell'IRGC per rubare proprietà intellettuale relativa alla tecnologia aerospaziale e satellitare. Alcune delle operazioni e degli indicatori descritti sembrano condividere alcune caratteristiche con le operazioni Mandiant precedentemente attribuite ad APT33.

- **Corea del Nord**: nel 2022, la Corea del Nord ha accelerato i suoi sforzi per sviluppare le sue capacità nucleari e i suoi missili balistici, nonostante gli sforzi delle potenze regionali per ostacolarne i progressi. Questa priorità nazionale probabilmente guiderà la *cyber threat activity* contro enti che lavorano nel settore governativo, militare e tecnologico, nonché nell'ambito accademico e dei *think tank* che possiedono competenze in materia di difesa e sicurezza.

  Gli analisti di Mandiant hanno rilevato attività di *social engineering* svolta dal gruppo nordcoreano APT43, che si fingeva composto da giornalisti ed esperti per interagire direttamente con obiettivi, sollecitare opinioni e valutare le reazioni a ipotetici eventi. Infine, è stata rilevata una sospetta campagna nordcoreana che coinvolgeva operatori, generalmente noti come "Andariel", dell'ingegneria aerospaziale e dell'industria manifatturiera negli Stati Uniti e in India. In tale campagna è stata impiegata una versione aggiornata del *malware* QUINSTATUS distribuita tramite un'e-mail di *spear-phishing* che sembrava provenire da uno scienziato di un'organizzazione di ricerca e sviluppo della difesa con sede in India.

Oltre che dai gruppi *State-Sponsored,* minacce al settore delle telecomunicazioni e delle trasmissioni satellitari sono state identificate da parte di *hacktivist* quali, ad esempio, XakNet Team, Infoccentr e CyberArmyofRussia_Reborn (probabilmente coordinati dal gruppo APT28).

Altri gruppi *hacktivist* che hanno operato contro questi settori sono NB65 e Kristina. Il gruppo NB65 ha preso di mira l'operatore di gestione documentale "Tensor", l'agenzia spaziale Roscosmos, la VGTRK, All-Russia State Television and Radio Broadcasting Co. di proprietà dello Stato russo, la banca russa JSC Bank PSCB e la società di pagamenti e servizi finanziari Qiwi, sempre di proprietà russa.

Il gruppo Kristina ha condiviso i dati della Corporazione Spaziale di Stato russa Roscosmos sul forum clandestino RAID nel febbraio 2022. In particolare l'attore ha condiviso informazioni degli utenti, comprese le credenziali e anche i dati relativi a istruzione, investimenti e tasse.

Infine, nell'*adversary landscape* rivolto contro i settori di interesse, sono in attività anche *threat actor* legati all'*eCrime*.

Gli analisti di Mandiant hanno identificato molteplici attività del gruppo FIN11 che hanno interessato entità aerospaziali nel periodo 2019-2022. In precedenza, questo gruppo ha rappresentato un rischio da moderato ad alto per gli ambienti *Operational Technology* (OT), a causa del suo *targeting* opportunistico contro le risorse OT e delle operazioni di *ransomware* dirompenti. Le famiglie di *malware* associate a FIN11 (e ai *threat-cluster* associati a questo gruppo, come CLOP, MBRKILLER e RAGNARLOCKER) possiedono capacità dirompenti/distruttive e capacità orientate all'OT, che aumentano la capacità dell'attore di incidere sulla disponibilità

delle risorse OT.

Nel giugno 2020, in un post di DopplePaymer, si affermava che avevano compromesso Digital Management, un fornitore di servizi per agenzie governative statunitensi, come la NASA e la Defense Information Systems Agency (DISA). Mentre nel marzo 2023, in un post di LockBit 3.0 sul loro Data Leak Site (DLS), si affermava che erano stati esfiltrati dati da Maximum Industries, inclusi file relativi a schemi di progettazione di SpaceX.

ATTACCO ALL'INFRASTRUTTURA VIASAT

Data la risonanza e l'importanza che ha avuto l'attacco russo contro l'infrastruttura dell'azienda di comunicazioni satellitari Viasat, si ritiene opportuno farne un – seppur breve – approfondimento tecnico.

L'invasione russa dell'Ucraina ha comportato numerose operazioni informatiche che hanno messo alla prova le ipotesi collettive sul ruolo svolto dal dominio cyber nella guerra moderna. L'attacco all'infrastruttura Viasat è stato pubblicamente reso noto per la prima volta a causa dei problemi con i router **Viasat KA-SAT.**

L'interruzione del funzionamento di questi router ha interrotto 5.800 turbine eoliche Enercon in Germania. Queste non sono state rese inutilizzabili dall'attacco, ma il "monitoraggio e controllo remoto delle turbine eoliche" è diventato non disponibile a causa di problemi con le comunicazioni satellitari.

Oltre che alle turbine eoliche, l'attacco alla rete Viasat ha prodotto disagi a migliaia di organizzazioni in tutta Europa.

Solo nella giornata di mercoledì 30 marzo 2022 Viasat ha rilasciato una prima dichiarazione in cui affermava che l'attacco è avvenuto in due fasi: in primo luogo un attacco DOS proveniente da *"several SurfBeam2 and SurfBeam2+ modems"* e *"[…other on-prem equipment…] physically located within Ukraine"* che ha temporaneamente messo offline i modem KA-SAT e, infine, la progressiva scomparsa dei modem dal servizio Viasat.

Viasat riferisce che gli aggressori hanno sfruttato un'*appliance* VPN configurata in modo errato, hanno ottenuto l'accesso al segmento di gestione della fiducia della rete KA-SAT e si sono spostati lateralmente; quindi hanno utilizzato il loro accesso per *"eseguire comandi di gestione legittimi e mirati su un gran numero di modem residenziali contemporaneamente".*

Viasat aggiunge poi che *"questi comandi distruttivi hanno sovrascritto i dati chiave nella memoria flash dei modem, rendendo i modem incapaci di accedere alla rete, ma non permanentemente inutilizzabili".*

Nell'agosto del 2023 Mark Colaluca, vicepresidente e responsabile della sicurezza informatica di Viasat, ha parlato insieme a Kristina Walter, capo della sicurezza informatica della base industriale della difesa (DIB) presso la NSA. In questa occasione, Colaluca ha affermato che la rete KA-SAT di Viasat serve più di 100.000 clienti situati in tutta Europa e nel Medio Oriente. Viasat offre sia connettività a banda larga che satellitare: ma l'attacco, attribuito ad hacker russi, ha preso di mira i clienti della banda larga. Colaluca ha rivelato che gli aggressori hanno realizzato due attacchi separati per interrompere le operazioni dell'azienda. *"In alcuni*

casi, era molto sofisticato e avevano una profonda comprensione di come funzionava la nostra rete", mentre *"In altri casi, hanno tratto grande vantaggio dagli strumenti e dalle capacità disponibili per eseguire l'attacco senza dover fare molto da soli. Una delle lezioni più importanti apprese è che la parte dell'attacco che non richiedeva grandi sofisticazioni – con un po' più di igiene e qualche accorgimento extra – probabilmente avrebbe potuto essere mitigata".*

Il 23 febbraio gli hacker hanno attaccato un centro direzionale a Torino, in Italia, prendendo di mira un'installazione VPN che forniva l'accesso alla rete ad amministratori e operatori.

Alle 17:00 (ora locale) l'analisi ha mostrato come avessero tentato invano di accedere alla VPN più volte, prima di riuscirci. Gli hacker si sono fatti strada verso i server di gestione che davano loro un ampio accesso alle informazioni, verso i modem dell'azienda che erano online e altro ancora.

Dopo alcune ore, gli attaccanti hanno avuto accesso a un altro server che forniva aggiornamenti software ai modem, e ciò ha consentito loro di diffondere il *malware wiper* identificato pubblicamente dai ricercatori l'anno scorso. L'attacco ha portato offline dai 40.000 ai 45.000 modem, migliaia dei quali non hanno mai ripreso il funzionamento.

Sulla base delle condizioni tecniche necessarie perché l'attacco possa essere realizzato, si ipotizza che il *threat actor* abbia utilizzato il meccanismo di gestione KA-SAT in un attacco alla *supply chain* per caricare un *wiper* progettato per modem e router.

Un *wiper* per questo tipo di dispositivo sovrascri-

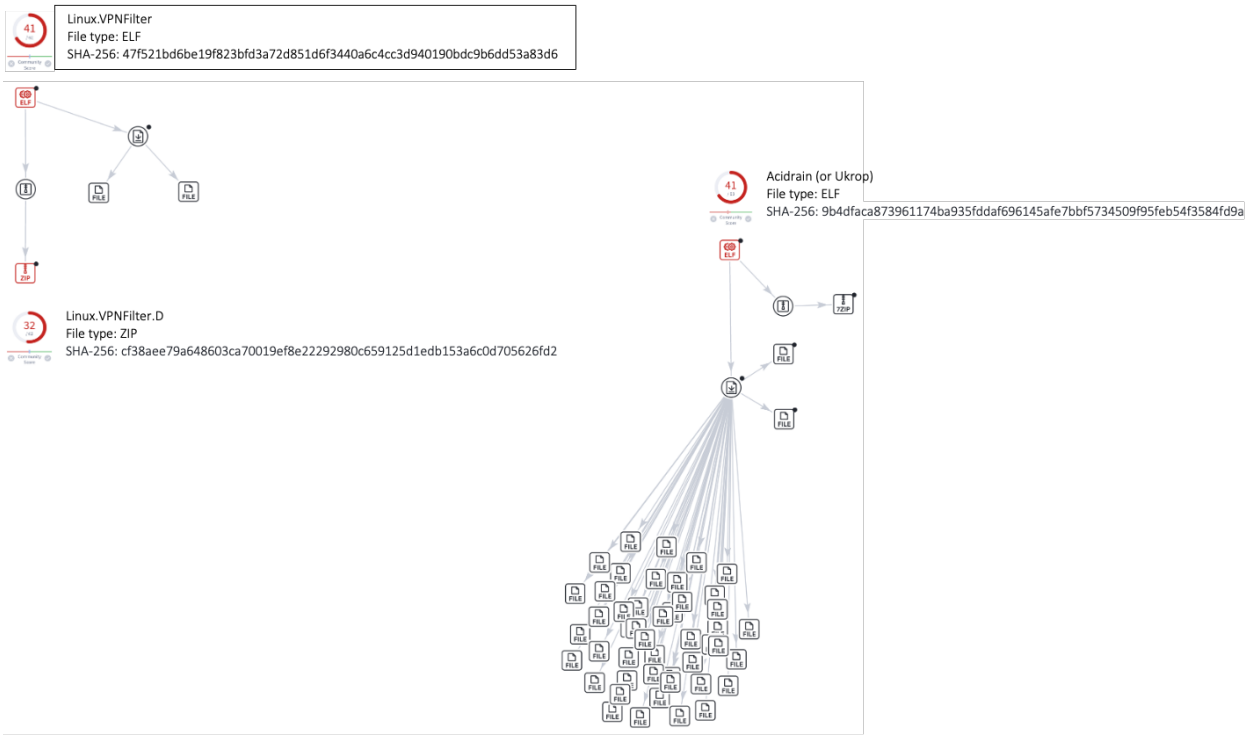


Fig. 4 – Rappresentazioni di VPNFilter e Acidrain

ve i dati chiave nella memoria flash del modem, rendendolo inutilizzabile e forzandone il *reflash* o la sostituzione. Al *wiper* in questione è stato dato il nome di AcidRain.

La funzionalità di AcidRain è relativamente semplice e richiede un tentativo di forza bruta che evidenzia o la mancanza di familiarità degli aggressori con i dettagli del *firmware* di destinazione, o la volontà di lasciare che lo strumento rimanesse generico e riutilizzabile. Il file binario esegue una cancellazione approfondita del *file system* e di vari file noti del dispositivo di archiviazione. Se il codice viene eseguito come *root*, AcidRain esegue una sovrascrittura ricorsiva iniziale ed elimina i file non standard nel *file system*.

Il caso individuato in precedenza è VPNFilter, un *malware* modulare rivolto ai router SOHO e ai dispositivi di archiviazione QNAP. VPNFilter includeva un'impressionante gamma di funzionalità sotto forma di *plugin* multi-fase distribuiti selettivamente sui dispositivi infetti.

La funzionalità spazia dal furto di credenziali al monitoraggio dei protocolli Modbus SCADA. Tra i suoi numerosi *plugin*, includeva anche la funzionalità per cancellare e bloccare i dispositivi, nonché per attaccare un bersaglio DDoS. Il motivo per cui viene chiamato in causa VPNFilter è l'interessante sovrapposizione di codice tra uno specifico *plugin* VPNFilter e AcidRain.

Nonostante Viasat abbia dichiarato che non vi è stato alcun attacco alla *supply chain* o utilizzo di codice dannoso sui router interessati, resta valida l'ipotesi che gli aggressori abbiano implementato AcidRain (e forse altri file binari e *script*) su questi dispositivi per condurre le loro operazioni. Sebbene AcidRain a VPNFilter (o al più ampio *cluster* di minacce di Sandworm) non si possano collegare in modo definitivo, si valuta – con confidenza media – che esistano delle somiglianze tra loro e nelle loro componenti.

INTRODUZIONE ALLA SPARTA MATRIX

Nella cybersecurity le matrici sono diventate un approccio standard del settore per fornire una base di conoscenza dei comportamenti degli avversari, fungendo anche da tassonomia per le azioni degli avversari durante tutto il ciclo di vita dell'attacco.

La *Aerospace Corporation* ha creato la matrice *Space Attack Research and Tactic Analysis* (o SPARTA) per identificare, classificare e condividere le principali tattiche, tecniche e procedure cyber (TTP) impiegate dai *threat actor* nel condurre attacchi finalizzati alla compromissione dei veicoli spaziali.

Basandosi sulla definizione fornita nell'**SPD-5**[1], lo Space System è definito come *"a combination of systems, to include ground systems, sensor networks, and one or more space vehicles, that pro-*

1. La Space Policy Directive 5 (o SPD5) stabilisce i principi chiave della sicurezza informatica per guidare e servire da base per l'approccio statunitense alla protezione informatica dei sistemi spaziali. Fornisce inoltre indicazioni sulla protezione dei beni spaziali e delle infrastrutture di supporto dalle minacce informatiche in evoluzione e attenua il potenziale di creazione di detriti spaziali dannosi derivanti da attività informatiche dolose

vides a space-based service."

Sulla base di questa definizione, gli elementi fondamentali che compongono lo Space System sono rappresentabili come segue:

Nella figura precedente le linee blu indicano le normali comunicazioni e accessi, mentre le linee rosse indicano le comunicazioni avviate dell'avversario.

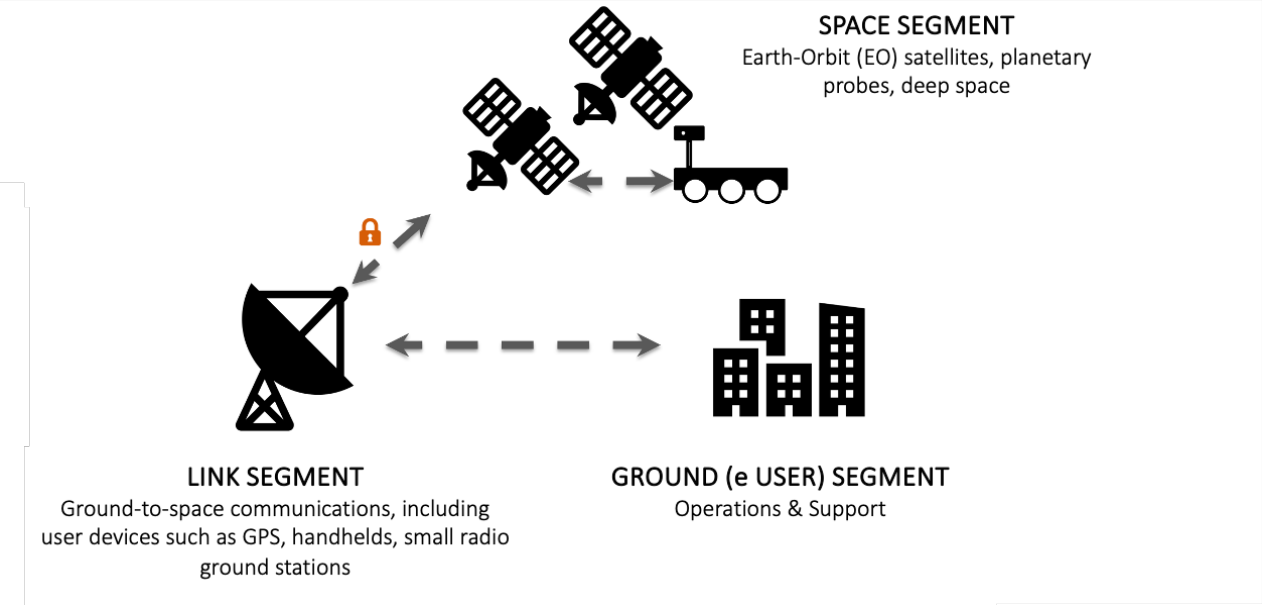


Fig. 5 – Principali elementi dello Space System

Gli elementi e le loro comunicazioni sono gli ambiti della *Space-Security*.

La figura seguente sintetizza graficamente i principali attacchi attinenti alla *Space-Security*:

Il modello di sicurezza che si prova a seguire nello Space System è il *Defense-in-Depth*, che prende in considerazione sia il *Ground* e *User segment*, come pure il *link* e lo *Space segment*. Storica-

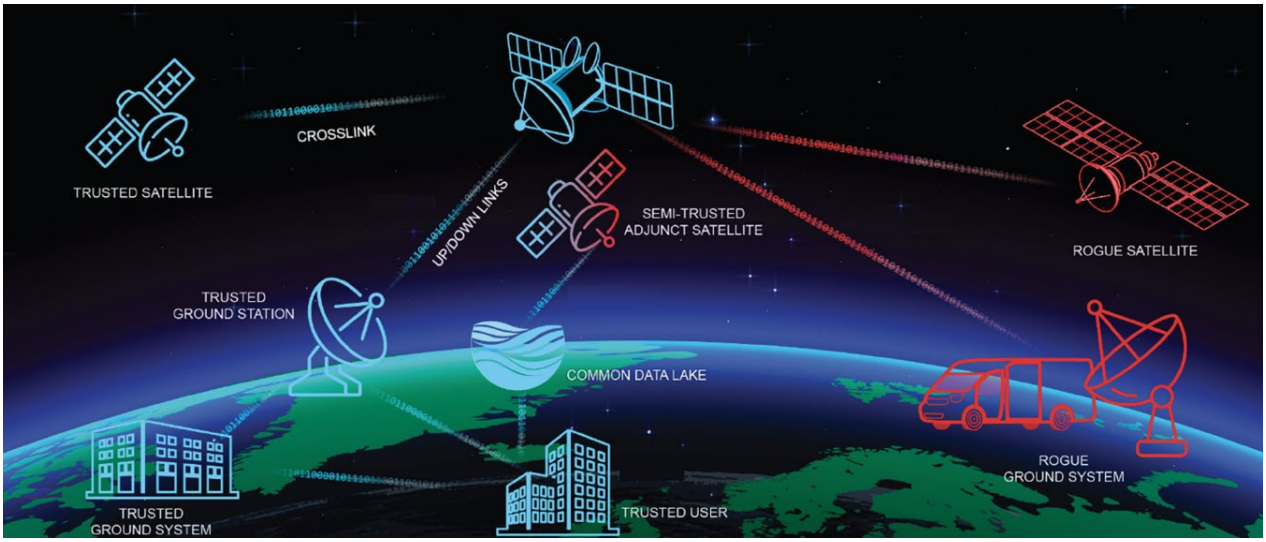


Fig. XX - Panoramica dei vettori di Cyber Threat Vectors per Space Systems

mente è stata data molta attenzione ai primi due, mentre la sicurezza del segmento spaziale (vale a dire, delle navicelle spaziali) e delle comunicazioni da e verso questi dispositivi è sicuramente rimasta indietro.

La figura 6 illustra una rappresentazione "a strati" in cui applicare le difese sul *Ground* e sullo *Space segment*. Lo strato esterno è la *Prevention*, che consiste nella *governance*, nella protezione della *supply chain* e nel *risk management.*

Gli strati interni rappresentano il luogo in cui risiedono i dati della missione e il software di volo, con protezioni come crittografia e *Software Assurance* per ridurre i rischi.

- *SBC e IDS/IPS*: a bordo sono disponibili poche (o nessuna) funzionalità focalizzata sulla sicurezza, monitoraggio, registrazione e avvisi;
- *Crypto*: alcuni sistemi dispongono di *"safe modes"* per i guasti crittografici che possono mettere i veicoli spaziali in una posizione di *vulnerabile state* (ovvero, modalità bypass crittografico);
- *Ground*: non sono mature le funzionalità per il monitoraggio della compromissione del sistema di terra da parte di utenti malintenzionati;
- *Prevention*: la gestione dei rischi nella *supply chain* continua a rappresentare una sfida e le

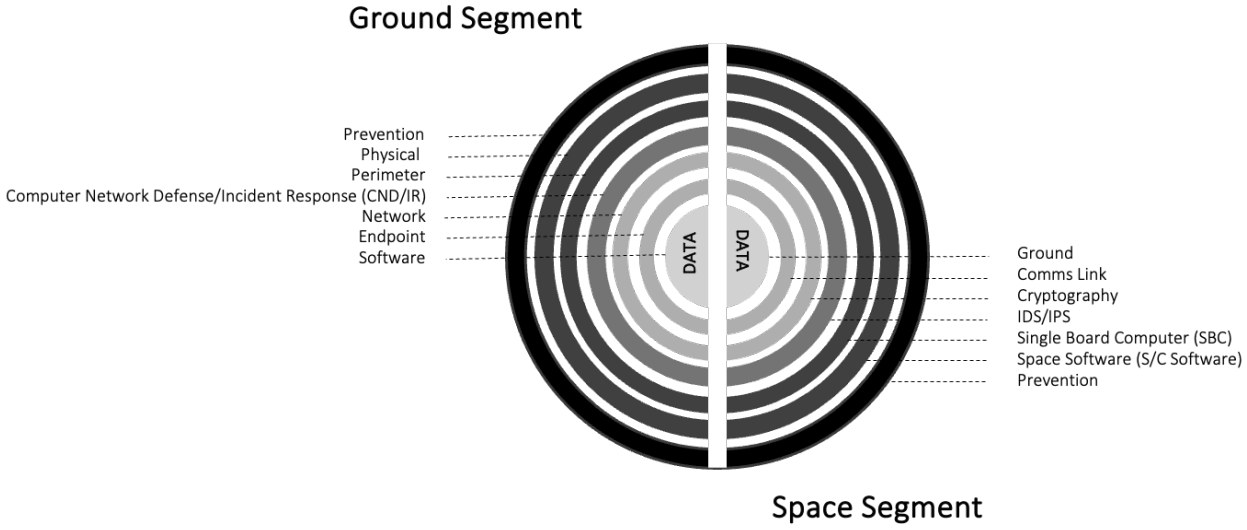


Fig. 6 – Panoramica del Defense-in-the-Depth Overview per Space Systems

Gli elementi dello *Space segment* che devono essere messi in sicurezza sono i seguenti.

- *S/C Software*: i principi di *Software Assurance* rappresentano una sfida con i sistemi software esistenti e hanno molte meno probabilità di essere applicati al software dei veicoli spaziali;

policy e procedure *satellite-focused cybersecurity* non sono sufficienti. Anche le minacce interne vengono raramente prese in considerazione o – al massimo – si applicano spesso controlli di sicurezza inadeguati.

Mentre le minacce al *Ground* e *Link segment* sono

descritte dalle matrici MITRE ATT&CK Enterprise e OT/ICS per fini di *defence* e *threat intelligence*, le minacce dello *Space segment* sono descritte nella matrice SPARTA. Al pari delle matrici MITRE ATT&CK, anche la matrice SPARTA descrive le minacce in termini di:

- *Tactics*: rappresentano il "perché" di una tecnica o sotto-tecnica SPARTA. Una tattica rappresenta l'obiettivo dei *threat actor* e la motivazione per cui impiega una o più tecniche;
- *Techniques*: rappresentano il "come" un *threat actor* raggiunge un obiettivo tattico eseguendo una specifica azione (o una sequenza di azioni);
- *Sub-techniques*: rappresentano una variazione – o un'istanza più specifica – del comportamento del *threat actor* impiegato per raggiungere un obiettivo. Le sotto-tecniche descrivono tipicamente il comportamento a un livello inferiore rispetto a una tecnica e sono considerate figlie della tecnica madre.
- *Procedures*: rappresentano una specifica implementazione utilizzata dal *threat actor* delle tecniche e sotto-tecniche. Le procedure sono le descrizioni passo-passo di come il *threat actor* intende procedere per raggiungere il proprio scopo.

Le TTP contenute nella matrice SPARTA descrivono come un attaccante può realizzare attacchi contro veicoli spaziali: ma complessivamente occorre prendere in considerazione anche le modalità di attacco descritte nelle matrici Enterprise e OT/ICS del MITRE, attraverso le quali gestire le TTP che un attaccante può eseguire sui segmenti di terra.

L'ultima versione della matrice SPARTA è la v1.6, rilasciata nel febbraio del 2024, che considera le seguenti tattiche:

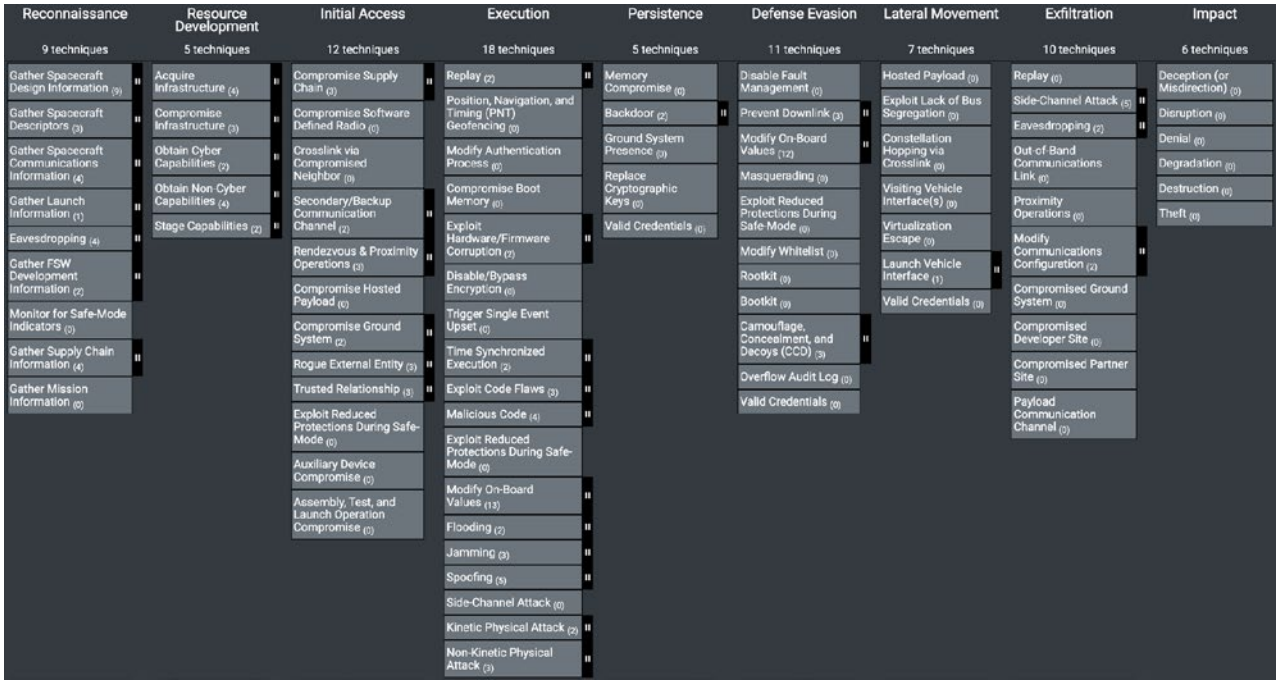


Fig. 7 - Space Attack Research & Tactic Analysis (SPARTA)

ID	*Tactics*	*Description*
ST0001	*Reconnaissance*	Threat actor raccoglie informazioni da utilizzare per pianificare operazioni future
ST0002	*Resource Development*	Threat actor stabilisce le risorse da utilizzare per supportare le operazioni
ST0003	*Initial Access*	Threat actor cerca di ottenere il punto di presenza/esecuzione dei comandi sulla navicella spaziale
ST0004	*Execution*	Threat actor tenta di eseguire codice malevolo sulla navicella spaziale
ST0005	*Persistence*	Threat actor cerca di mantenere il proprio accesso per comandare/eseguire codice sul veicolo spaziale.
ST0006	*Defense Evasion*	Threat cerca di evitare di essere rilevato
ST0007	*Lateral Movement*	Threat actor prova a spostarsi sui sottosistemi della navicella spaziale
ST0008	*Exfiltration*	Threat actor prova a rubare informazioni
ST0009	*Impact*	Threat actor tenta di manipolare, interrompere o distruggere i sistemi spaziali e/o i dati

Tab. 2 – Le tattiche della tabella SPARTA

ID	*Tactics*	Descrizione delle *Tactics*	*Techniques*
ST0001	*Reconnaissance*	Threat actor raccoglie informazioni da utilizzare per pianificare operazioni future	*Gather Spacecraft Design Information* *Gather Spacecraft Descriptors* *Gather Spacecraft Communications Information* *Gather Launch Information* *Eavesdropping* *Gather FSW Development Information* *Monitor for Safe-Mode Indicators* *Gather Supply Chain Information* *Gather Mission Information*
ST0002	*Resource Development*	Threat actor stabilisce le risorse da utilizzare per supportare le operazioni	*Acquire Infrastructure* *Compromise Infrastructure* *Obtain Cyber Capabilities* *Obtain Non-Cyber Capabilities* *Stage Capabilities*

ST0003	*Initial Access*	Threat actor cerca di ottenere il punto di presenza/esecuzione dei comandi sulla navicella spaziale	*Compromise Supply Chain* *Compromise Software Defined Radio* *Crosslink via Compromised Neighbor* *Secondary/Backup Communication Channel* *Rendezvous & Proximity Operations* *Compromise Hosted Payload* *Compromise Ground System* *Rogue External Entity* *Trusted Relationship* *Exploit Reduced Protections During Safe-Mode* *Auxiliary Device Compromise* *Assembly, Test, and Launch Operation Compromise*
ST0004	*Execution*	Threat actor tenta di eseguire codice malevolo sulla navicella spaziale	*Replay* *Position, Navigation, and Timing (PNT) Geofencing* *Modify Authentication Process* *Compromise Boot Memory* *Exploit Hardware/Firmware Corruption* *Disable/Bypass Encryption* *Trigger Single Event Upset* *Time Synchronized Execution* *Exploit Code Flaws* *Malicious Code* *Exploit Reduced Protections During Safe-Mode* *Modify On-Board Values* *Flooding* *Jamming* *Spoofing* *Side-Channel Attack* *Kinetic Physical Attack* *Non-Kinetic Physical Attack*

ST0005	*Persistence*	Threat actor cerca di mantenere il proprio accesso per comandare/ eseguire codice sul veicolo spaziale.	*Memory Compromise* *Backdoor* *Ground System Presence* *Replace Cryptographic Keys* *Valid Credentials*
ST0006	*Defense Evasion*	Threat cerca di evitare di essere rilevato	*Disable Fault Management* *Prevent Downlink* *Modify On-Board Values* *Masquerading* *Exploit Reduced Protections During Safe-Mode* *Modify Whitelist* *Rootkit* *Bootkit* *Camouflage, Concealment, and Decoys (CCD)* *Overflow Audit Log* *Valid Credentials*
ST0007	*Lateral Move-ment*	Threat actor prova a spostarsi sui sottosistemi della navicella spaziale	*Hosted Payload* *Exploit Lack of Bus Segregation* *Constellation Hopping via Crosslink* *Visiting Vehicle Interface(s)* *Virtualization Escape* *Launch Vehicle Interface* *Valid Credentials*
ST0008	Exfiltration	Threat actor prova a rubare infor-mazioni	Replay Side-Channel Attack Eavesdropping Out-of-Band Communications Link Proximity Operations Modify Communications Configuration Compromised Ground System Compromised Developer Site Compromised Partner Site Payload Communication Channel

ST0009	Impact	Threat actor tenta di manipolare, interrompere o distruggere i sistemi spaziali e/o i dati	Deception (or Misdirection) Disruption Denial Degradation Destruction Theft

Tab. 3 – Le tecniche della tabella SPARTA

Francesco Schifilliti, *Consulente in Cyber Security & Threat Intelligence*

RIFERIMENTI

https://spacenews.com/from-galileo-to-the-lunar-gateway-mapping-italys-growing-space-industry

https://www.iai.it/sites/default/files/iai2201.pdf

“AcidRain | A Modem Wiper Rains Down on Europe” di Juan Andres Guerrero-Saade e Max van Amerongen (https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe)

“Satellite outage knocks out thousands of Enercon’s wind turbines” (https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28)

“KA-SAT Network cyber attack overview” (https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview)

https://www.proofpoint.com/us/blog/threat-insight/ta453-refuses-be-bound-expectations

Mandiant - Inter(not so)stellar: Cyber Threats to Space

“Defending Spacecraft in the Cyber Domain” (https://csps.aerospace.org/sites/default/files/2021-08/Bailey_Defending-Spacecraft_11052019.pdf)

https://video.aiaa.org/title/641d6fd5-f5f5-4230-b116-4f6a4e9a3c3a

https://medium.com/the-aerospace-corporation/protecting-space-systems-from-cyber-attack-3db773aff368

https://www.cisa.gov/resources-tools/resources/space-policy-directive-5

Cybersecurity Protections for Spacecraft: A Threat Based Approach (April 29, 202) (https://aerospace.org/sites/default/files/2022-07/DistroA-TOR-2021-01333-Cybersecurity Protections for Spacecraft--A Threat Based Approach.pdf)

https://sparta.aerospace.org

“Using SPARTA to conduct Space Vehicle Cyber Assessments” (https://sparta.aerospace.org/resources/OTR202400438_SPARTA_for_SV_Assessments.pdf)

“Protecting Space Systems from Cyber Attack” (https://medium.com/the-aerospace-corporation/protecting-space-systems-from-cyber-attack-3db773aff368)

“Hacking an On-Orbit Satellite: An Analysis of the CYSAT 2023 Demo” (https://medium.com/the-aerospace-corporation/hacking-an-on-orbit-satellite-an-analysis-of-the-cysat-2023-demo-ae241e5b8ee5)

“SPARTA v1.6 — What’s New?” (https://medium.com/the-aerospace-corporation/version-1-6-update-1-nasas-space-security-best-practice-guide-mapping-ca91d3951979)

“Hackers to show they can take over a European Space Agency satellite” (https://therecord.media/space-cybersecurity-satellite-hacked-esa-thales)

"The Countries With The Most Satellites In Space" (https://www.forbes.com/sites/katharinabuchholz/2023/04/26/the-countries-with-the-most-satellites-in-space-infographic/?sh=2aa543a2ce27)

"China's plan for anti-satellite cyber weapon found in leaked CIA documents" (https://techmonitor.ai/technology/cybersecurity/chinese-anti-satellite-cyber-weapon)

"China building cyberweapons to hijack enemy satellites, says US leak" (https://arstechnica.com/information-technology/2023/04/china-building-cyberweapons-to-hijack-enemy-satellites-says-us-leak/?comments-page=1)

"Pentagon: Chinese Military Units Training With ASAT missiles China, Russia militarizing space to challenge U.S." (https://www.ff.org/pentagon-chinese-military-units-training-with-asat-missiles-china-russia-militarizing-space-to-challenge-u-s/)

"Italian Space Budget, 2005-2021" (https://www.thespacereport.org/resources/spanish-space-budget-2009-2021)

"ITALY SPACE INDUSTRY" (https://www.trade.gov/market-intelligence/italy-space-industry)

"Foundations of Supply Chain Management for Space Application", Galluzzi&All (https://ntrs.nasa.gov/api/citations/20170011140/downloads/20170011140.pdf)

"FBI, Air Force warn of cyberattacks on space industry by 'foreign intelligence operations'" (https://therecord.media/fbi-warns-of-space-cyberattacks)

"This new satellite enters orbit with one mission: To get abused by hackers" (https://therecord.media/new-satellite-enters-orbit-to-get-hacked)

"Hackers to show they can take over a European Space Agency satellite" (https://therecord.media/space-cybersecurity-satellite-hacked-esa-thales)

https://www.starlinkmap.org

"SPACE THREAT ASSESSMENT 2023", APRIL 2023

"SPACE THREAT ASSESSMENT 2024", APRIL 2024

BIOGRAFIA

Francesco Schifilliti

Esperto in sicurezza delle informazioni, digital forensic e cyber threat intelligence per grandi aziende. È stato il Practice Manager di Forensic Technology & Discovery Services (FTDS) in Fraud Investigation & Dispute Services (EY). Ricercatore nel campo di Malware e Memory Analysis, Structured Analytic Procedures (SAT), OSINT, Intelligence Investigation Techniques, Incident Responding Techniques e Cyber Threat Intelligence. Laureato in Informatica presso l'Università degli Studi di Catania, è docente in corsi e master in digital forensics e malware forensics.

Quaderno di Cyber Intelligence #2

CYBER CRIME

White paper gratuito su www.ictsecuritymagazine.com

Il rilevamento del GPS spoofing nei droni

Il controllo di un UAV (*Unmanned Aerial Vehicle*[1], cioè velivolo senza pilota umano a bordo) rappresenta una sfida tecnologica apparentemente gestibile e alla portata di un pubblico sempre più esteso; se non fosse soggetto ad attacchi di *GPS spoofing*, che hanno il potere di alterare la percezione dell'UAV in merito al posizionamento corrente.

Si capisce che l'effetto di tale pratica può essere spiacevole, fino a divenire devastante nei casi di velivoli ad uso militare. In questo articolo ci occuperemo di alcune possibilità di rilevare lo *spoofing*, in maniera che si possano prendere misure di contrasto, almeno per evitare effetti drastici conseguenti a queste tipologie di attacchi.

UAV E DRONI

I termini "UAV" e "droni" oggi sono usati praticamente come sinonimi[2].

In realtà, mentre "UAV" è usato soprattutto in ambienti militari, "drone" viene utilizzato nell'ambito di applicazioni civili come la fotografia, l'esplorazione, l'agricoltura, la manutenzione di opere stradali e ferroviarie o le attività ricreative; e si tratta, in genere, di velivoli a pilotaggio remoto.

Il termine più tecnico ("UAV") descrive invece l'assenza di un pilota umano a bordo. Si usano, in effetti, vari acronimi: *Unmanned Aircraft System* (UAS) sta ad indicare un intero sistema, composto non solo dal velivolo ma anche da una stazione di controllo e da un collegamento per la comunicazione tra questa e il velivolo. La statunitense FAA (Federal Aviation Administration, agenzia federale del Dipartimento dei Trasporti, che si occupa dell'aviazione civile) ha introdotto il termine UA per indicare un aeromobile senza pilota. Le regole della FAA richiedono che in un UAS ci sia un pilota in comando remoto (RPIC), o un osservatore visivo, che sia in grado di vedere il velivolo in ogni momento mentre l'aereo è in volo. Spesso si usa la sigla "RPAV" (*Remotely Piloted Aerial Vehicle*), in italiano SAPR (Sistema Aeromobile a Pilotaggio Remoto[3] [4], ambito regolato dall'ENAC[5] ma divenuto obsoleto dopo l'emissione del regolamento UAS-IT[6]). A rendere più confuso lo scenario ci sono i termini UAVS e RPAS, ove la lettera S descrive il sistema, come già detto per gli UAS.

1. https://www.britannica.com/technology/unmanned-aerial-vehicle

2. https://www.linkedin.com/pulse/what-difference-between-uav-drone-sisi-yui-cuhcc

3. https://www.overfly.me/operatore-sapr-significato

4. https://www.enac.gov.it/sites/default/files/allegati/2020-Lug/Regolamento_APR_Ed_3_Emend_1.pdf

5. https://www.enac.gov.it/

6. https://www.enac.gov.it/sites/default/files/allegati/2021-Gen/Regolamento_UAS-IT080121.pdf

Precisiamo che gli UAV possono essere a guida completamente autonoma (se fanno uso di sensori e di una logica autonoma) o semi-autonoma (il velivolo funziona utilizzando sensori, un sistema di controllo a terra e una programmazione software specifica). Merita una menzione a parte la sottocategoria FPV (*First-Person View*) in cui il pilota remoto vede ciò che è visibile dal drone[7]. Naturalmente è un caso speciale di UAS.

È ancora dubbio se un velivolo a pilotaggio remoto possa essere chiamato UAV o meno: in letteratura ci sono indicazioni contrastanti al riguardo[8] [9]. Esistono numerose altre sigle[10] ma non si tratta di una questione rilevante ai fini della presente analisi. La letteratura sul tema è piuttosto ricca[11].

NAVIGAZIONE SATELLITARE

Da parecchi anni è disponibile la navigazione satellitare, che supporta la localizzazione nel tempo e nello spazio di molti operatori; negli ultimi anni, grazie alla diffusione di smartphone e tablet, è utilizzata anche dal grande pubblico.

Tecnicamente si tratta di satelliti orbitanti che forniscono informazioni per il geoposizionamento; se la copertura è globale si parla di GNSS (*Global Navigation Satellite Systems*), mentre se è regionale si usa RNSS (*Regional Navigation Satellite Systems*).

Drone usato per l'ispezione di uno scomodo viadotto autostradale. Generated with AI.

I sistemi globali sono attualmente quattro: GPS (statunitense), GLONASS (russo), BDS (cinese) e Galileo (europeo). Il funzionamento del GNSS si basa su alcuni principi fisici che qui non discutere-

7. https://www.dji-store.it/qual-e-la-differenza-tra-droni-uas-uav-e-sapr/

8. https://en.wikipedia.org/wiki/Unmanned_aerial_vehicle

9. https://it.wikipedia.org/wiki/Aeromobile_a_pilotaggio_remoto

10. https://www.911foto.it/news/sapr.htm

11. Oltre alle altre fonti già indicate (e limitandoci a quelle online), si segnalano: https://www.rand.org/topics/unmanned-aerial-vehicles.html, https://www.sciencedirect.com/topics/agricultural-and-biological-sciences/unmanned-aerial-vehicle, https://www.ai4business.it/robotica/uav-cose-e-come-funziona-un-velivolo-senza-pilota/, https://www.sciencedirect.com/topics/engineering/unmanned-aerial-vehicle, https://airandspace.si.edu/exhibitions/military-unmanned-aerial-vehicles-uav.

mo[12], limitandoci a osservare come il più diffuso sia sicuramente il GPS. In tutti i casi è prevista la messa a punto di un dispositivo di ricezione che riceve segnali dai satelliti per determinare la posizione. Da qui, due conseguenze pratiche: non c'è ricezione di segnale satellitare in un ambiente *indoor*[13]; la diffusa convinzione per cui un ricevitore è anche in grado di comunicare la posizione è errata, occorrendo, oltre al ricevitore, un trasmettitore.

Di seguito faremo riferimento al GPS, il più noto fra i GNSS; tuttavia, quanto discusso vale, in linea di principio, per tutti gli altri sistemi di navigazione satellitare.

LO SPOOFING E I SUOI EFFETTI

Il termine *spoofing* è usato in numerosi scenari differenti: tutti hanno in comune l'idea di un attaccante che falsifica l'identità per ottenere un vantaggio illegittimo. Può avvenire nell'email, nelle comunicazioni a pacchetto, nella telefonia, ecc.

L'attacco è pienamente applicabile ai sistemi di navigazione satellitare, attraverso determinate azioni che interferiscono con i (deboli) segnali emessi dai satelliti, facendo pervenire ai ricevitori satellitari informazioni errate. Con il termine *GPS spoofing*[14,15] ci riferiamo alle azioni mirate a perturbare/avvelenare la ricezione di ricevitori satellitari, con lo scopo di far loro determinare una posizione errata.

Illustrazione suggestiva del GPS spoofing. Generated with AI

Questo può avere varie conseguenze, che possono arrivare ad essere critiche.

Si capisce facilmente che nel caso FPV gli effetti di un tale attacco potranno essere arginati, poiché contrastati dalla visione del pilota remoto che, in molti casi, avrà altri elementi visuali per determi-

12. https://en.wikipedia.org/wiki/Satellite_navigation, https://en.wikipedia.org/wiki/GNSS_augmentation

13. Se si richiede il geoposizionamento a un dispositivo dotato di ricevitore GNSS situato in un ambiente indoor, questo, non ricevendo segnale satellitare, si limiterà a fornire la posizione della torre a cui il dispositivo è connesso; nel caso migliore, rilevando la presenza di almeno tre torri, potrà effettuare la triangolazione.

14. https://www.repubblica.it/tecnologia/2023/10/18/news/che_cose_il_gps_spoofing_e_perche_e_potenzialmente_letale-417950578/

15. https://www.doctorspy.it/che-cose-il-gps-spoofing-come-manipolare-un-segnale-gps/

nare la posizione del velivolo; per cui una discrepanza fra il posizionamento GPS e quello ottenuto usando altri elementi, per esempio visuali, può facilmente condurre a un rilevamento positivo e conclamato.

Nel caso di applicazioni civili il *GPS spoofing* potrà avere effetti da trascurabili a gravi, fino a comportare il fallimento della missione del drone; il che potrà essere magari trascurabile nelle applicazioni ludiche, ma ben più grave quando si usa un drone per attività di ricognizione, manutenzione infrastrutture, recupero/consegna, ecc.

Peggiori le conseguenze nel caso militare, in cui si immagina facilmente un drone *kamikaze* colpire un bersaglio errato, addirittura amico.

In sintesi, se facilmente possiamo immaginare scenari ove il *GPS spoofing* avrebbe conseguenze nulle o trascurabili, altrettanto facilmente immaginiamo differenti scenari ove le conseguenze potrebbero essere letali.

Alcuni droni sono costruiti con speciali integrazioni hardware che prevengono molti tipi di attacchi di *GPS spoofing*: tali integrazioni sono, però, piuttosto costose e di conseguenza vengono ritenute giustificate in poche applicazioni.[16]

Sono disponibili varie guide per combattere il GPS spoofing[17,18,19,20,21], che tuttavia molto spesso soffrono il limite di non offrire una visione metodologica. Se è chiaro che il *GPS spoofing* è indesiderabile, si capisce che un punto di partenza critico è la capacità di rilevare uno *spoofing*, per poi tentare di attuare delle contromisure.

ALCUNE TECNICHE DI RILEVAMENTO

In questa sezione saranno prese in esame alcune tecniche che prevedono ipotesi non sempre soddisfatte, ma che possono essere anche impiegate simultaneamente.

Continuità della posizione

Assumiamo in questo caso che l'eventuale *spoofing* non avvenga presso la stazione di decollo del drone; il che appare anche abbastanza ragionevole perché la stazione, conoscendo la sua posizione, si accorgerebbe immediatamente di uno *spoofing* in atto, semplicemente confrontando la sua posizione (nota) con quella rilevata.

Se il drone rileva le proprie successive posizioni, queste dovranno allora variare descrivendo l'andamento di una funzione continua del tempo, perché il dispositivo non può registrare una

16. https://www.modis.com/it-it/insights/articoli/gps-spoofing-machine-learning-per-migliorare-la-sicurezza-dei-moderni-sistemi-per-droni/

17. https://powerdmarc.com/it/what-is-gps-spoofing/

18. https://www.okta.com/identity-101/gps-spoofing/

19. https://www.scientificamerican.com/article/gps-is-easy-to-hack-and-the-u-s-has-no-backup/

20. https://www.septentrio.com/en/learn-more/insights/what-spoofing-and-how-ensure-gps-security

21. https://www.iplocation.net/10-tips-for-preventing-gps-spoofing-attacks

discontinuità spaziale. Piuttosto, una discontinuità dovrebbe corrispondere all'ingresso in un'area soggetta a *spoofing*.

Il metodo si basa dunque sul confronto sistematico delle posizioni rilevate, con la prima posizione assunta come corretta. Inoltre, la tecnica potrebbe venir rafforzata dalla verifica che ogni mini-spostamento rilevato abbia ampiezza compatibile con tempi di rilevazione e velocità, applicando equazioni elementari della cinematica.

Denominiamo "falso positivo" l'errata rilevazione di uno *spoofing* non presente; un "falso negativo" è, invece, la rilevazione dell'assenza di *spoofing* quando questo è in realtà presente.

Possibilità di falsi negativi[22]: bassa; di falsi positivi: trascurabile.

Osservazione

Prendiamo atto della ampia disponibilità di mappe fotografiche, satellitari e non, che descrivono l'intero pianeta[23].

L'idea consiste nel dotare il drone di una fotocamera (magari che funzioni anche ad infrarossi) che effettui foto del paesaggio circostante e le confronti con le mappe disponibili, effettuando una verifica della posizione. Se le coordinate ottenute dal *pattern matching* sono compatibili con quelle rilevate dal GPS si ha conferma della posizione; in caso contrario, di uno *spoofing* in atto.

Il *matching* potrebbe essere a) verificato a bordo o b) elaborato nella *ground station*. Nel caso a) si pone il problema della necessità di potenza computazionale (per il *pattern matching*) a bordo e della banda necessaria (per caricare gli scenari fotografici di riferimento), il che incrementa i costi e va a svantaggio dell'autonomia.

Nel caso b) rimarrebbe la necessità di banda (per la continua trasmissione delle immagini ottenute).

Possibilità di falsi negativi: bassa; di falsi positivi: bassa.

Confronto con triangolazione GSM

Molti droni sono già resi disponibili con scheda per il collegamento GSM, se non UMTS. Quello che appare facile, anche se non sempre possibile, è rilevare la distanza dalla cella cui la scheda è agganciata.

Idealmente il drone si trova su una circonferenza il cui raggio è pari alla distanza rilevata e il centro è costituito dalla cella, che si trova in una posizione nota: il geoposizionamento GPS deve essere compatibile con l'appartenenza a tale circonferenza[24]. Se la scheda percepisce due torri, sebbene con potenze differenti, allora si possono intersecare le due circonferenze, determinando due sole zone per la compatibilità con le coordinate GPS. Nel caso di tre (o più; magari si considerano le tre più potenti) celle, si può completare la trian-

22. Assumiamo il corretto funzionamento del drone.

23. Ad es., https://earth.google.com/

24. In realtà non è una circonferenza ma una semi-sfera.

golazione e determinare una posizione esatta da confrontare con quella GPS.

Quindi, con l'aumentare delle celle percepite aumenta l'accuratezza. In generale il problema sarà la ridotta disponibilità di celle.

Nel caso di tre o più celle, la possibilità di falsi negativi o positivi è trascurabile; con il diminuire delle celle, aumenta la possibilità dei falsi negativi.

Analisi statistica

La tecnica in questo caso è applicabile quando il drone percorre una traiettoria abituale, per la quale esiste dunque una memoria storica dei posizionamenti. Si assume anche che un eventuale *spoofing* non sia persistente.

Il drone si limita a trasmettere le successive geolocalizzazioni GPS, che definiscono una successione da confrontare con i valori tipici delle successioni precedenti. Se i valori riscontrati non si discostano in maniera percettibile da quelli precedentemente riscontrati, deduciamo l'assenza di *spoofing*; altrimenti, rilevando una variazione anomala, si denuncia uno *spoofing* in atto.

Due elementi sono rilevanti. Il primo è dato dalla quantificazione statistica che misura la conformità o l'anomalia: questa deve essere il risultato di un'attenta valutazione condotta da un matematico. Il secondo è la scrupolosa annotazione di ogni evento anomalo che, per la stessa missione, determina una traiettoria parzialmente o totalmente differente.

Possibilità di falsi negativi: trascurabile; di falsi positivi: bassa.

Stormi

Qui si ipotizza il volo contemporaneo di più droni, sufficientemente distanziati per non essere considerati vittime dello stesso *spoofing* ma non così lontani da non poter comunicare tra loro.

Denominiamo l'insieme di droni "stormo coeso." Questa situazione è analoga a quanto descritto nella sezione 4.3, ove al posto delle celle telefoniche vanno considerati droni dello stesso stormo coeso. Ciascun drone trasmette le proprie coordinate GPS; in qualunque insieme di tre droni ciascuno trasmetterà agli altri due le proprie coordinate GPS.

Ogni drone potrà costruire due triangoli: il primo usando la propria posizione GPS e le apparenti coordinate di origine delle trasmissioni degli altri due (triangolo di comunicazione) e il secondo usando solo coordinate GPS (triangolo GPS).

Se i due triangoli sono abbastanza simili fra loro, si deduce l'assenza di *spoofing*; altrimenti se ne determina la presenza. Ogni drone può effettuare tale verifica triangolando con i più vicini.

Lo stormo coeso è un'ipotesi piuttosto restrittiva, ma la possibilità di falsi positivi e negativi sono basse.

Angolazione Sole/Luna

In questa ultima tecnica si assume che un drone sia equipaggiato con sensori in grado di rilevare la posizione del Sole o della Luna, determinando in particolare l'angolo fra il piano di volo e la congiungente fra astro e drone stesso. Tale posizione deve essere compatibile con quella calcolata

conoscendo le coordinate GPS e il tempo esatto. L'ipotesi che sia possibile rilevare Sole o Luna non è sempre soddisfatta, per cui l'applicabilità della tecnica è ridotta. Inoltre, il calcolo dell'angolo menzionato deve essere fatto da un astrofisico competente che fortunatamente può applicare una metodologia generale.

Falsi positivi e negativi possono essere considerati medi.

RIASSUMENDO

Difendersi dal *GPS spoofing* – come dallo spoofing rivolto a qualsiasi sistema GNSS o RNSS – richiede o un esborso importante o una serie di metodologie che, se sapientemente impiegate, possono condurre al risultato.

Qui ne abbiamo proposte sei: le metodologie possono coesistere, ma alcune di esse richiedono ipotesi importanti. Abbiamo pensato di proporre una tabella riepilogativa in cui si evidenziano le caratteristiche di applicabilità, difficoltà, costo, falsi positivi e negativi.

Per applicabilità e difficoltà usiamo la scala ordinale ("nessuna, facile, media, difficile"); per il costo e i falsi positivi/negativi, i valori "trascurabile, basso, medio, alto".

La questione merita ben altri approfondimenti e, in aggiunta, la rassegna di tecniche sovraesposta è incompleta; il presente articolo intende rappresentare, tuttavia, una prima utile riflessione sull'argomento.

Fabrizio d'Amore, *Docente presso l'Università degli Studi di Roma "La Sapienza", membro del Cyber Intelligence and Information Security Center*

Metodologia	*Applicabilità*	*Difficoltà*	*Costo*	*Falsi positivi*	*Falsi negativi*
4.1 Continuità della posizione	facile	nessuna	basso	trascurabili	bassi
4.2 Osservazione	media	media	trascurabile	bassi	bassi
4.3 Confronto con triangolazione GSM	media	facile	trascurabile	trascurabili	trascurabili
4.4 Analisi statistica	media	media	trascurabile	bassi	trascurabili
4.5 Stormi	difficile	facile	trascurabile	bassi	bassi
4.6 Angolazione Sole/Luna	difficile	difficile	medio	medi	medi

BIOGRAFIA

Fabrizio d'Amore

Romano, docente di Cybersecurity alla Sapienza Università di Roma. Ha trascorso periodi di studio e ricerca all'estero (Zurigo, Buenos Aires, Berkeley, UMIACS a College Park Maryland). Insegna inoltre corsi di crittografia, sicurezza delle informazioni, sicurezza applicativa e steganografia presso alcuni master ed altre iniziative di alta formazione. Direttore del master di 2° livello in Sicurezza delle informazioni e informazione strategica, in collaborazione con il DIS. Svolge attività di verificatore e di consulente tecnico di parte. Referente scientifico di contratti di ricerca applicata, studio e analisi fra università ed enti istituzionali e privati. Dal 2015 la sua attività di ricerca si concentra sul campo della steganografia/watermarking, sicurezza del software (antiplagio), cybersecurity del volo aero civile e delle infrastrutture, modelli di autenticazione, protezione dei dati & privacy e OSINT.

Supply Chain Security: Il caso di Avio S.p.A.

I RISCHI ATTUALI PER LE AZIENDE: IMPATTI SU CLIENTI E FORNITORI

Il numero degli attacchi informatici contro le imprese che hanno origine nella vulnerabilità dei propri clienti e fornitori coinvolti nella s*upply chain* risulta sempre più in aumento.

La partecipazione di ogni azienda al sistema espone ogni membro della s*upply chain* a fattori di rischio informatico che sono intrinseci nei concetti di *network* e di *collaboration*. La compromissione di un anello della catena può innescare un effetto domino che andrà a impattare su tutti gli attori: ed è per questo che la sicurezza di una azienda è pari alla sicurezza dell'anello più debole della propria s*upply chain*.

Oggi, di conseguenza, è necessario avere idonee garanzie anche circa gli standard presenti presso le terze parti.

Le violazioni di dati o gli attacchi che si verificano a qualsiasi livello della catena hanno conseguenze devastanti; e anche un incidente di sicurezza localizzato presso un singolo fornitore può impattare su tutti i membri della s*upply chain* di cui fa parte.

Gli attaccanti sfruttano con successo le falle nella s*upply chain* in quanto, molto spesso, risulta più semplice attaccare un *target* connesso all'obiettivo finale che l'obiettivo stesso.

È, infatti, estremamente comune lo scenario in cui un *target enterprise* interessante per i cybercriminali si avvalga di fornitori di eccellenza nell'ambito di un *business* in cui, tuttavia, non sono presenti programmi di *cybersecurity* maturi.

Sono principalmente tre i motivi per cui le terze parti delle s*upply chain* spesso non sono protette da soluzioni di *cybersecurity* sufficientemente solide e mature.

1. Mancanza di budget: le piccole realtà di eccellenza italiane spesso non hanno fondi per gestire la propria infrastruttura informatica, ma forniscono realtà *enterprise* con componenti fondamentali per il processo di *business* di queste ultime;
2. mancanza di consapevolezza;
3. risorse interne non specializzate nei temi legati alla *cybersecurity*.

Le vulnerabilità originate dalla *supply chain* sono molteplici:

in alcuni casi i fornitori vengono dotati di credenziali per accedere a reti, dati e applicazioni del business e, quindi, hanno la possibilità di diffondere *malware* o commettere infiltrazioni.

- Le credenziali di un fornitore potrebbero essere state sottratte e riutilizzate da un *hacker*.
- Altre possibilità: un fornitore di *software* (ad esempio) potrebbe aver subito un attacco *cyber*, il codice da lui prodotto potrebbe contenere quindi un *malware* che sarebbe quindi distribuito a tutti i clienti.

La Figura n. 1 illustra la struttura tipica di un *data breach* che coinvolge la *supply chain.*

Con riferimento alla *liability* aziendale e alle responsabilità delle terze parti, esistono già requisiti di *compliance* per aspetti come la *vendor due diligence*[1], il *risk management della supply chain* o i requisiti dei contratti di acquisto.

Da qui l'importanza di un programma specifico di *compliance* integrata per la *supply chain cybersecurity*, che possa consentire di includere i principali rischi associati alla fornitura di prodotti e servizi.

LA COMPLIANCE CYBER NELLA SUPPLY CHAIN E IL CASO DI AVIO S.P.A.

Il concetto di *supply chain* ha integrato il concetto stesso di catena di distribuzione, anche attraverso l'introduzione di prodotti informatici e automatizzati. L'iper-specializzazione e la digitalizzazione dei sistemi di *supply chain* rende ogni realtà aziendale sempre più legata alla galassia dei propri fornitori, generando una crescente vulnerabilità informatica in termini di *outsourcing* e digitalizzazione.

I fronti su cui può svilupparsi una minaccia cibernetica per il mondo dell'approvvigionamento sono essenzialmente due: da un lato lo scambio dati tra fornitori e clienti aziendali, dall'altro l'eventualità che proprio la catena logistica sia minacciata da *malware*.

Nel primo caso – quello dello scambio informativo fra fornitori e aziende – il rischio è chiaro: sono infatti da considerare "fornitori critici" coloro che

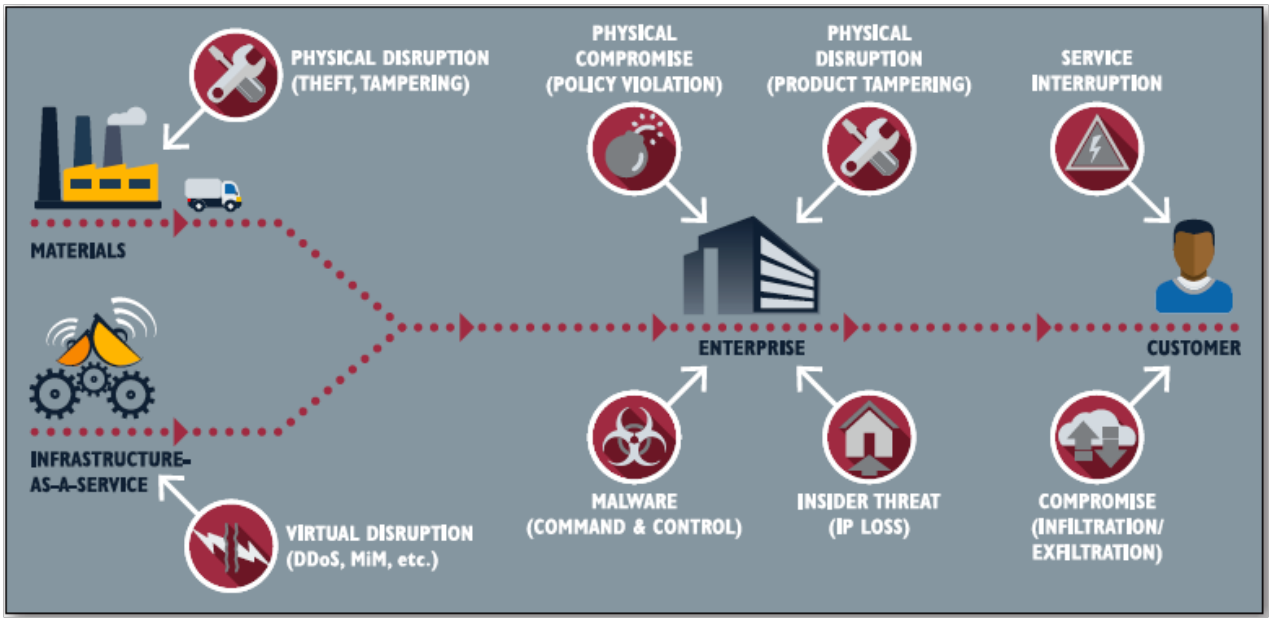


Figura n. 1.

1. Si intende quel processo di indagine promossa proprio dal titolare o dall'amministratore di un'impresa sull'impresa stessa, spesso svolta ai fini della futura cessione dell'attività.

forniscono infrastrutture server[2], sistemi di virtualizzazione[3], ERP[4] *as a service*, *software* TMS[5] e WMS in *cloud*[6], partner senza i quali un'azienda avrebbe serie difficoltà a garantire la propria continuità operativa. Poniamo il caso che un'intrusione informatica comprometta i *web server* del nostro erogatore di servizi WMS (*Warehouse management system*): controllare in tempo reale i movimenti del magazzino potrebbe divenire assai difficoltoso ed è questo un rischio che un'industria come AVIO S.p.A. non può certo ignorare. In questa circostanza, andrebbero allora individuate le catene di approvvigionamento delle tecnologie condivise, così da certificare la trasparenza di tutta la filiera, dai dispositivi *hardware* agli applicativi *software*.

Ma come può un'azienda cercare di arginare o, quanto meno, di mitigare un tale attacco *cyber*, partendo sempre dal presupposto che non può essere mai considerato il "rischio zero"?

Al riguardo, può essere uno spunto importante l'esperienza di Avio S.p.A.; azienda che, data la sua natura industriale e strategica, ha necessariamente dovuto rispondere in modo veloce e programmatico al quesito qui riportato, prevedendo azioni di mitigazioni del rischio *cyber relativo* alla propria *supply chain*, al momento di selezionare un possibile fornitore.

Per assicurarsi una buona protezione, Avio S.p.A. ha definito linee guida e controlli integrandoli con i processi aziendali esistenti. A queste azioni poi si sono affiancate delle *best practice* nella gestione dei fornitori per quanto riguarda gli obblighi contrattuali, tra le quali la richiesta di notifica delle violazioni con una precisa *timeline* e dei parametri condivisi. Inoltre, l'azienda cerca sempre di richiedere al proprio fornitore l'integrità del prodotto; ma soprattutto cerca di fare in modo che tutti gli obblighi e le *best practice* siano messe in atto, a loro volta, anche dai fornitori nei confronti dei loro sub-fornitori.

---

2. L'infrastruttura IT è costituita da hardware, software e rete, ovvero i componenti necessari a far funzionare e gestire gli ambienti IT enterprise. Può essere distribuita all'interno di un sistema di cloud computing o nella struttura stessa di un'organizzazione.

3. La virtualizzazione è un processo che consente alle aziende di eseguire più macchine virtuali su una singola macchina fisica: permette quindi di eseguire simultaneamente più sistemi operativi sullo stesso apparato informativo, migliorando l'affidabilità del sistema e riducendo i costi relativi all'hardware.

4. L'ERP (Enterprise Resource Planning) è un tipo di sistema software che aiuta le organizzazioni ad automatizzare e gestire i processi aziendali principali per ottenere le prestazioni ottimali.

5. Un sistema di gestione dei trasporti (TMS) è una piattaforma logistica che utilizza la tecnologia per aiutare le aziende a pianificare, eseguire e ottimizzare il movimento fisico dei prodotti, sia in entrata che in uscita, assicurandosi che la spedizione sia conforme e che la documentazione adeguata sia disponibile.

6. WMS Cloud estende le supply chain per uniformare la gestione dell'inventario e i servizi di evasione degli ordini ai metodi di acquisto moderni, offrendo visibilità in tempo reale sull'intero magazzino tramite smartphone e browser: l'unico requisito è disporre dell'accesso ad Internet.

Avio S.p.A., infatti, ha preliminarmente implementato tutte le misure sopra indicate, oltre ad averle anche integrate successivamente con le misure previste dal DPCM 81/2021 (Allegato B) aventi ad oggetto la gestione dei fornitori; le ha poi trasferite anche nelle proprie procedure aziendali, in modo tale da permettere a tutti i suoi dipendenti, attuali e futuri, di attuare queste *best practice* nel migliore dei modi.

Questa è una pratica molto utilizzata attualmente: si tratta, infatti, di inserire clausole di *cyber compliance* anche all'interno dei contratti di appalto, nelle condizioni generali di fornitura, nelle procedure aziendali, come appunto indicato anche per Avio S.p.A.

Si tratta di applicare principi organizzativi e gestionali tali da consolidare e perimetrare le azioni di sicurezza, che costituiscono la principale leva strategica per l'accelerazione e la crescita economica di un'intera impresa. Non si parla di strumenti informatici avanzati, ma di buona gestione d'impresa: *cyber security* e *supply chain* devono iniziare a essere considerati come espressione della medesima disciplina – cioè la gestione del rischio – e, per farlo, devono essere applicati i principi propri della gestione del rischio aziendale.

In primo luogo, occorre riconoscere come una minaccia alla catena di approvvigionamento minacci la tenuta dell'impresa stessa; da ciò discende che è fondamentale la collaborazione aperta e trasparente con i propri fornitori critici, nell'ottica di una più armoniosa coordinazione delle politiche di risposta a un evento critico. In secondo luogo, è necessario fortificare lo scheletro aziendale con una "squadra di risposta" che possa facilitare il percorso di *incident response* e che coinvolga, pertanto, non solo il dipartimento informatico aziendale ma anche la direzione generale, l'ufficio legale, il DPO incaricato, il responsabile di un eventuale sistema di qualità e del sistema di controllo della qualità del prodotto finale.

Tornando al nostro esempio pratico, relativo alle *best practice* applicate da Avio S.p.A., oltre a quanto sopra, nel momento in cui l'azienda ha l'esigenza di acquistare un bene o un servizio la Direzione *Procurement* attiva una procedura interna che prevede, in una fase iniziale – ossia prima di individuare l'effettivo fornitore – l'analisi di alcuni aspetti strettamente legati a un'eventuale vulnerabilità informatica in termini di *outsourcing*.

La scelta del fornitore di Avio S.p.A., prima di focalizzarsi su analisi tecniche e specifiche delle capacità di sicurezza informatica del soggetto individuato, parte nel selezionare determinati possibili fornitori che, *ab origine,* presentino determinate caratteristiche:

- fornitori di Paesi UE o NATO, in quanto hanno più probabilità di essere conformi a determinati standard di sicurezza;
- fornitori con certificazioni di cybersecurity rilevanti;
- fornitori con pregressa esperienza nel settore aerospaziale in cui Avio S.p.A. è uno dei leader mondiali.

Conclusa la verifica di questi aspetti più generici, la Direzione *Procurement* avvia una nuova analisi valutativa con lo scopo di verificare la valorizzazione qualitativa del "fornitore" e del "prodotto" offer-

to, il quale deve avere un peso sempre maggiore rispetto al fattore prezzo.

Al termine di questo preliminare processo di selezione, è così individuata la "rosa" dei possibili fornitori di Avio S.p.A., che, come già indicato in precedenza, dovranno poi soddisfare tecnicamente quei requisiti di sicurezza indicati nelle proprie condizioni generali di contratto, nonché nelle proprie *policies* e procedure aziendali, inerenti alla loro infrastruttura informatica.

Tuttavia, quanto descritto in precedenza non è sufficiente a garantire la propria azienda da eventuali attacchi informatici; pertanto, diviene necessario progettare allo stesso tempo l'armatura difensiva aziendale per i casi di interruzioni di fornitura che andrebbero ad impattare sulla *business continuity*[7] e definire processi di *disaster recovery*[8] come, ovviamente, realizzato anche da Avio S.p.A.

Infatti, è proprio in un'ottica di *business continuity* che è necessario agire: e, per assicurarla, è necessario che le aziende si dotino di sistemi di *business continuity management*.

Lo scopo ultimo per ogni azienda è assicurarsi la continua erogazione dei propri servizi e la certezza di poter svolgere le proprie attività anche in caso di incidenti o problemi. A tal fine le aziende redigono un *business continuity plan,* uno degli strumenti più efficaci per assicurare la resilienza cyber: si tratta di un "manuale d'uso" delle eventuali minacce in cui l'azienda può incorrere e delle relative soluzioni che questa può adottare.

Non vi è dubbio che fornirsi di un esaustivo *business continuity plan* sia fondamentale per la prevenzione dei rischi e per la valutazione degli interventi nei casi di concretizzazione degli eventi avversi, all'interno del quale si dovranno prevedere anche attività di *disaster recovery.*

Un altro fronte a cui è necessario prestare attenzione da parte delle aziende – e che rientra appieno nel monitoraggio della sicurezza della propria *supply chain* – è legato all'incursione malevola all'interno delle piattaforme informatiche aziendali della catena di fornitura. Si tratta di attacchi informatici alle catene di approvvigionamento tramite minacce dette *Advanced Persistent Threat*[9] o APT (i *malware* rappresentano la componente più nota e spesso utilizzata per questa tipologia di attacchi), che rappresentano circa il 92% degli incidenti di sicurezza informatica tra le piccole e medie imprese nel mondo.

---

7. Processo atto a individuare le potenziali minacce alle quali è esposta una data organizzazione e a definire i processi necessari per assicurare la resilienza della struttura a seguito del verificarsi delle condizioni avverse, per porre al sicuro l'operatività, la capacità produttiva, gli interessi e l'immagine dell'azienda.

8. Il disaster recovery, parte integrante di un business continuity plan, specifica le funzioni da mettere al sicuro e le misure da adottare per raggiungere questo obiettivo.

9. Le Advanced Persistent Threats rappresentano una minaccia avanzata e persistente, ovvero un attacco informatico complesso e selettivo che, mediante un accesso non autorizzato ai sistemi di informazione e comunicazione, è in grado di accedere a dati riservati o causare danni a un'azienda, un'industria o un'organizzazione.

L'effetto "a cascata" provocato da questi attacchi dipende dalla sicurezza di ogni singolo tassello della *supply chain* e dimostra come la minima debolezza di un partecipante alla catena possa creare problematiche ingenti e irreversibili, non solo a tutti gli appartenenti alla catena ma anche a chi, pur non ne facendone parte, può risentire gli effetti dell'incidente: ad esempio consumatori, Stati, etc.

Dunque è necessario che, a tutela della sicurezza della *supply chain,* le aziende definiscano i fornitori più critici, ovvero quelli che potrebbero comportare le conseguenze più problematiche in caso di *data breach*/malfunzionamento dei loro sistemi informatici; e che individuino al loro interno il "*Vendor Owner*", persona dell'organizzazione responsabile della gestione e *reporting* di tutti gli aspetti, comprese eventuali problematiche legali, *audit*, revisione di procedure e documentazione fornita dal *Vendor*.

Ultimo elemento – forse il più rilevante – è, infine, quello della programmazione: ossia cercare di immaginare un'interruzione di servizio o un attacco informatico alla propria catena distributiva e, quindi, pianificare le modalità tramite le quali riaccendere i motori dell'impresa e far ripartire la produzione.

La migliore strategia, in questo caso, risiede proprio nella preparazione, nella valutazione dei rischi e nella mitigazione degli stessi attraverso una serie di strumenti non soltanto tecnologici, quanto soprattutto culturali.

Anche il *World Economic Forum* si esprime in materia e propone **tre principi fondamentali** che possono contribuire alla mitigazione della sfida della sicurezza della *supply chain*.

1. Integrare sicurezza e *privacy* nel processo di approvvigionamento e nel ciclo di vita: avere una politica di gestione dei rischi delle terze parti garantirà che sicurezza e *privacy* siano sempre prese in considerazione con misure mature, coerenti ed efficaci.

2. Adottare un approccio basato sul rischio delle valutazioni di terze parti: tale approccio sarà in grado di aiutare il processo decisionale di accettazione o rifiuto delle terze parti e mitigare, di conseguenza, le minacce che le terze parti potrebbero porre a tutto l'ecosistema della *supply chain*.

3. Implementare *policy* sul codice sorgente e *policy* sullo sviluppo, che deve essere sicuro *by design*: ciò mira a ridurre al minimo i rischi relativi al ciclo di vita del *software*, che deve prendere in considerazione anche l'impatto sui clienti in caso di possibile incidente. Tale approccio aiuterà a proteggere tutto l'ecosistema digitale della *supply chain*, contribuendo al tempo stesso a rafforzare la fiducia.

Le **raccomandazioni per il cliente** includono:

1. identificare e mantenere una documentazione aggiornata di fornitori e *provider* di servizi;

2. definire criteri di rischio per i differenti fornitori e servizi, identificando le criticità e i possibili "*point of failure*";

3. avere un piano di monitoraggio dei rischi a cui si è esposti per il fatto di essere parte di una *supply chain*;

4. gestire i fornitori durante tutto il ciclo di vita di prodotti e servizi, pianificando le procedure per le fasi di "*end of life*";
5. classificare gli asset e le informazioni che vengono condivise con i fornitori, identificando delle procedure di accesso alle stesse e di gestione del modo in cui vengono trattate.

Le **raccomandazioni per il fornitore** includono:

1. assicurarsi che l'infrastruttura utilizzata per le fasi di sviluppo, creazione, gestione e consegna del prodotto segua le *best practices* per la *cybersecurity*;
2. implementare un processo di sviluppo, manutenzione e supporto del prodotto coerenti con i processi di sviluppo del prodotto comunemente accettati;
3. monitorare le vulnerabilità di sicurezza segnalate da fonti interne ed esterne, che includano i componenti di terze parti utilizzati;
4. mantenere un inventario delle risorse che includa informazioni rilevanti per le *patch*.

Alla luce di quanto emerso, occorre quindi facilitare un processo di armonizzazione tra le indicazioni, le norme e le *best practice* fornite per il problema analizzato. L'approccio finalizzato alla messa in sicurezza della catena di approvvigionamento è quello del *risk management*, non quello tecnologico: lo strumento è di indole informatica ma la soluzione va ricercata nelle procedure e nei processi, mentre la chiave di lettura è la continua e costante integrazione e attuazione del *risk management* alla *supply chain*.

Giorgio Martellino, *Avvocato e Giurista d'impresa*

BIOGRAFIA

Giorgio Martellino

Avvocato e Giurista d'impresa, dal 2016 è General Counsel, Compliance Officer e Risk Manager nonché membro dell'Odv 231 di Avio (società quotata alla Borsa di Milano segmento STAR).

In oltre vent'anni di esperienza maturata sia in contesti esteri (Abbott) che presso multinazionali italiane (Natuzzi) anche quotate (Cementir Holding), ha diretto gli affari legali e societari occupandosi anche di sistemi di Corporate Governance e di Compliance aziendale.

Già General Counsel & Compliance Officer di Acquedotto Pugliese, nonché docente e relatore su tematiche concernenti la compliance, la responsabilità amministrativa delle società/enti ex. D. lgs. 231/2001 e la prevenzione della corruzione, è Presidente AITRA (Associazione Italiana Trasparenza e Anticorruzione) e Vice Presidente AIGI (Associazione Italiana Giuristi di Impresa).

FORUM ICT SECURITY

23-24 OTTOBRE 2024

AUDITORIUM DELLA TECNICA, ROMA

Iscriviti alla newsletter di ICT Security Magazine
per conoscere l'agenda e partecipare alla
22ª Edizione del Forum ICT Security