Venti di guerra nello Spazio

di Marco Lisi

Negli ultimi anni si è più volte discusso, anche sulle pagine di questa Rivista, della dipendenza della nostra società dai sistemi spaziali e degli attacchi, più o meno evidenti, operati contro di essi in varie forme. Particolarmente preoccupanti, per chi si occupa di geomatica, erano i vari e spesso ripetuti episodi di "jamming" e "spoofing" nei confronti dei segnali GNSS, soprattutto GPS, in varie aree del mondo, quali Medio Oriente, stretto di Hormuz, mar della Cina, Corea. Non meno gravi, anche se forse meno noti, i tentativi di attacchi cibernetici contro sistemi satellitari per l'osservazione della Terra e le comunicazioni.

Nelle ultime settimane quelli che sembravano tuttavia rischi episodici e molto localizzati, lontani comunque dal cuore dell'Europa, sono tragicamente balzati agli onori della cronaca.
La guerra in Ucraina ha dimostrato tutta l'importanza e la vulnerabilità delle infrastrutture spaziali e l'urgente necessità di provvedere alla loro difesa in un quadro più ampio, che include ovviamente tutte le infrastrutture critiche europee.
Molto gravi sono anche state le conseguenze indirette della guerra, quali la decisione della Russia di interrompere la cooperazione in programmi spaziali con le nazioni occidentali, includendo la International Space Station (ISS) ed i lanci di satelliti europei con lanciatori russi.
La sospensione dei lanci Soyuz dalla base di lancio europea in Guiana francese, con il ritorno in patria degli ingegneri e tecnici russi che supportavano tali lanci, potrebbe avere serie conseguenze sul programma spaziale europeo, ad esempio ritardando il lancio dei due satelliti Galileo, originariamente previsto a fine 2022.
La conclusione evidente è che i sistemi spaziali, essendo altamente integrati nelle infrastrutture critiche della nostra società, devono essere garantiti e protetti da attacchi intenzionali e non, in termini di riservatezza, disponibilità, integrità, continuità e qualità del servizio.
Altrettanto evidente è che la convergenza tra difesa e spazio deve essere affrontata con senso di realismo.
La percezione comunemente condivisa è che lo Spazio rischia di diventare lo scenario di una guerra futura, se non lo è già diventato (fig. 1).

Sicurezza spaziale e autonomia strategica dell'UE

Una buona comprensione dell'attuale piano dell'Unione Europea per raggiungere l'autonomia strategica nello spazio può essere derivata considerando i quattro pilastri del programma spaziale europeo, perseguito dalla Commissione Europea attraverso la sua "European Union Space Program Agency" (EUSPA) (fig. 2):

• Galileo, sistema di posizionamento globale, navigazione e riferimento temporale. Questo sistema, oltre a costituire una spina dorsale globale per tutte le infrastrutture critiche, fornisce anche servizi

governativi e legati alla sicurezza, come il servizio di ricerca e salvataggio (SAR) e il servizio pubblico regolamentato (PRS), un segnale crittografato resistente a jamming e spoofing.
A livello regionale europeo, Galileo è integrato da EGNOS (European Geostationary Navigation Overlay Service), un sistema di potenziamento basato su satellite (SBAS) utilizzato per migliorare le prestazioni di Galileo e GPS;
• Copernicus, "sistema di sistemi" integrato di osservazione della Terra, che svolgerà un ruolo importante nel monitoraggio ambientale (cambiamenti climatici, inquinamento), nella gestione delle emergenze (calamità naturali come terremoti, incendi, inondazioni, ecc.), e nella sorveglianza di frontiera/costiera. Copernicus è costituito da un insieme complesso di sistemi che raccolgono dati da più fonti: satelliti per l'osservazione della Terra e sensori "in situ", come stazioni a terra e sensori aerei e marittimi.
• GOVSATCOM, sistema europeo di telecomunicazioni satellitari per uso governativo, che fa parte della più ambiziosa "Secure Connectivity Initiative". GOVSATCOM fornirà capacità di comunicazione garantite, sicure ed economiche a missioni, operazioni e infrastrutture critiche per la sicurezza, adottando tecnologie quantistiche per la crittografia. Il sistema GOVSATCOM presterà inoltre un'attenzione particolare alla fornitura di connettività alla sempre più strategica regione artica;
• Space Situational Awareness (SSA), un sistema per la sorveglianza degli oggetti in orbita, monitorando anche l'uso pacifico dello "Spazio Esterno", come previsto dai trattati internazionali (ONU).

Fig. 1 - Interferenze contro i segnali GPS rilevate dal satellite Hackeye 360 in Ucraina

È evidente l'obiettivo strategico perseguito dall'UE nello sviluppo del suo programma spaziale e la conseguente necessità di rafforzare la sicurezza e la resilienza delle sue risorse spaziali e terrestri contro gli attacchi informatici e fisici.

Infrastrutture spaziali: vulnerabilità e minacce

La sicurezza satellitare è stata erroneamente limitata in passato alla crittografia e alle tecnologie anti-jamming. In realtà i satelliti fanno parte di sistemi ibridi, che incorporano sia componenti spaziali che terrestri; i loro segmenti di terra sono quindi esposti allo stesso tipo di trattamenti (virus, worm, cavalli di Troia, attacchi Denial-Of-Service, vulnerabilità sfruttate, ecc.) tipici dei sistemi informativi terrestri.
Le vulnerabilità dei sistemi spaziali possono essere sfruttate concentrando gli attacchi su uno qualsiasi dei tre segmenti che compongono la capacità spaziale (fig. 3):

• Segmento spaziale: il satellite o la costellazione di satelliti, inclusi i carichi utili;
• Segmento di terra: include tutte le strutture hardware e software che consentono di controllare e gestire con successo gli asset spaziali, dal lancio alla dismissione. Elementi tipici di un segmento di terra sono i centri di controllo (centro di controllo della missione e centri operativi dedicati) e le reti delle stazioni di terra; il
• Segmento utenti: utenti aziendali e individuali, comprese le loro apparecchiature e

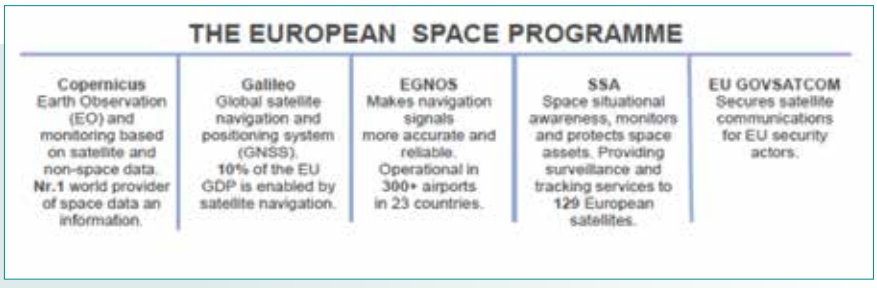

Fig. 2 - Il programma spaziale dell'Unione Europea.

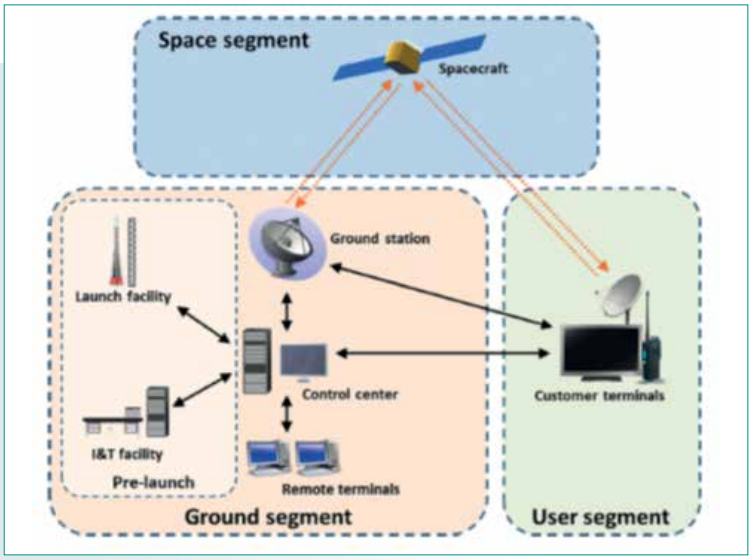

Fig. 3 - Segmenti spazio, terra e utente di un sistema satellitare.

applicazioni software.
Inoltre, i sistemi spaziali, come i satelliti ei loro segmenti di controllo, adottano tipicamente tecnologie sofisticate considerando gli stringenti requisiti riguardanti le comunicazioni, la protezione dalle radiazioni e la potenza di calcolo richiesta a bordo.
La crescente preoccupazione dei governi e delle compagnie spaziali per il rischio di attacchi cibernetici alle loro infrastrutture terrestri ed in orbita è nota e ben supportata da prove concrete. Ma altre minacce incombono sullo Spazio e sul suo uso pacifico, come mostrato nelle Tabelle 1 e 2.
Oltre agli attacchi informatici, principalmente diretti contro le infrastrutture del segmento di terra (centri di controllo, stazioni di terra, basi di lancio), sono oggi possibili numerose minacce fisiche, che vanno dalle "Armi antisatellite a energia cinetica" ("Kinetic Energy Anti-Satellite Weapons") alle "Armi ad energia diretta" ("Direct-Energy Weapons") ed ai disturbi a radiofrequenza ("RF jamming").
Un'arma cinetica anti-satellite può essere un missile lanciato da terra nello spazio fino a quando non intercetta un satellite già in orbita e lo distrugge per impatto, oppure un satellite "killer" che viene messo in orbita e rimane lì in attesa di essere utilizzato, modificando la sua orbita.
In entrambi i casi, un attacco ad "energia cinetica", basato sull'impatto fisico con un satellite "bersaglio" e la sua distruzione, è seguito anche dall'inevitabile conseguenza della produzione di "detriti", che continuano a rimanere in orbita, aumentando la già preoccupante quantità di detriti spaziali intorno alla Terra.
Le armi ad energia sono solitamente dirette contro asset in orbita e possono essere realizzate come laser ad alta energia o come fasci di radiofrequenza generati a terra, in grado di "accecare" i satelliti e danneggiarne le apparecchiature elettroniche. Impulsi molto dannosi di energia a radiofrequenza possono essere generati anche dall'esplosione di

Type of threat	Vulnerable satellite system components
Ground-based:	
Natural occurrences (including earthquakes and floods; adverse temperature environments)	Ground stations; TT&C and data links
Power outages	
Space-based:	
Space environment (solar, cosmic radiation; temperature variations)	Satellites; TT&C and data links
Space objects (including debris)	
Interference-oriented:	
Solar activity; atmospheric and solar disturbances	Satellites; TT&C and data links
Unintentional human interference (caused by terrestrial and space-based wireless systems)	

Source: DOD and GAO analysis.

Tab. 1 - Minacce non intenzionali ai sistemi satellitari.

Type of threat	Vulnerable satellite system components
Ground-based:	
Physical destruction	Ground stations; communications networks
Sabotage	All systems
Space-based (anti-satellite):	
Interceptors (space mines and space-to-space missiles)	Satellites
Directed-energy weapons (laser energy, electromagnetic pulse)	Satellites; TT&C and data links
Interference and content-oriented:	
Cyber attacks (malicious software, denial of service, spoofing, data interception, and so forth)	All systems and communications networks
Jamming	All systems

Source: GAO analysis.

Tab. 2 - Minacce intenzionali ai sistemi satellitari.

piccole bombe nucleari nella ionosfera ("Electro-Magnetic Pulse", EMP).
Per i sistemi globali di navigazione satellitare (GNSS), come il Galileo europeo, oltre alle minacce citate, bisogna ricordare gli specifici attacchi nei confronti degli utenti, nella forma di "jamming" (disturbo del segnale) e "spoofing" (generazione di un segnale falsificato).
Per tutte le minacce alla sicurezza discusse finora, possono essere messe in atto adeguate strategie di mitigazione e contromisure specifiche, come sintetizzato nella Tabella 3.
Per quanto riguarda i sistemi GNSS, la contromisura adottata nelle applicazioni militari e governative è quella di crittografare i codici dei segnali, rendendo impossibile la loro falsificazione. In ambito civile è da segnalare l'iniziativa della Commissione Europea che ha introdotto nel sistema Galileo l'autenticazione del segnale civile, la cosiddetta "Open Service Authentication" (OS-NMA).
Un'ultima menzione merita una vulnerabilità molto spesso sottovalutata: la filiera.
La complessità della filiera necessaria per realizzare i sistemi spaziali, infatti, li rende appetibili anche per gli hacker (fig. 4).
La maggior parte dei sistemi satellitari richiede molti produttori/fornitori con varie specializzazioni per svilupparne tutti i componenti, che sono poi assemblati da un integratore di sistema. Questi fornitori offrono numerose opportunità ad un utente malintenzionato di accedere alla linea di produzione satellitare, iniettando software dannoso ("malware": virus, "trojans") o introducendo hardware malevolo ("trojan hardware"). Per queste catene di approvvigionamento e organizzazione della produzione altamente complesse, si dovrebbe presumere l'applicazione di protocolli di sicurezza rigorosi, ma questo è raramente vero, specialmente nelle industrie commerciali.
Nonostante le numerose potenziali minacce descritte, per molti anni gli standard di sicurezza degli asset spaziali, soprattutto commerciali, non sono stati regolamentati da alcun ente istituzionale.
Fino a poco tempo non c'erano agenzie nazionali o internazionali che limitassero l'uso dei satelliti e monitorassero il loro effettivo utilizzo, a parte l'ONU ("United Nations Office for Outer Space Activities", UNOOSA), con il mandato specifico di preservare lo Spazio dagli usi militari, e l'"International Telecommunications Union" (ITU), che coordina principalmente le orbite dei satelliti e l'utilizzo dello spettro delle radiofrequenze al fine di evitare interferenze.
La mancanza di normative di sicurezza implica che i satelliti non abbiano standard di sicurezza informatica comuni e potrebbero essere utilizzati per attacchi informatici impunemente ed anonimamente, a meno che le società commerciali e le agenzie governative non prendano provvedimenti per proteggere questi sistemi. Questa situazione sta diventando ancora più grave a causa della proliferazione di satelliti molto piccoli (da 1 a 20 chili) a basso costo che utilizzano la tecnologia COTS (commer-

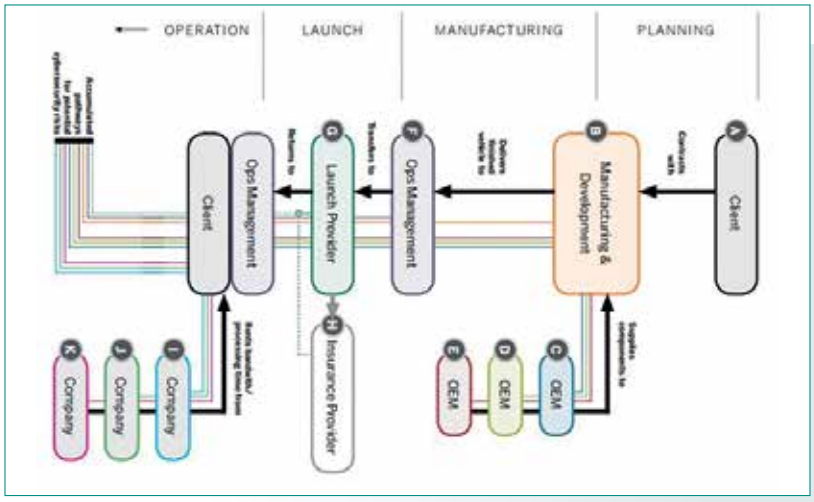

Fig. 4 - Potenziali accessi di attacchi cibernetici nel ciclo di vita di un satellite.

Satellite system components	Security techniques available	Type of threat addressed
TT&C and data links	Encryption	Cyber attacks
	High-power radio frequency (RF) uplink	Jamming
	Spread spectrum	Jamming
	Unique digital interface	Cyber attacks, jamming
Satellites	Hardening	Space environment, interceptors, directed-energy weapons
	Redundancy	Sabotage, space objects, interceptors, directed-energy weapons
Ground stations	Physical and logical security controls	Physical destruction, sabotage, cyber attacks, jamming, power outages
	Hardening	Natural occurrences, physical destruction, cyber attacks, jamming
	Redundancy	Natural occurrences, physical destruction, sabotage, power outages

Source: GAO analysis.

Tab. 3 - Tecniche di mitigazione delle minacce ai sistemi spaziali.

Fig. 5 - Il centro di eccellenza dell'ESA per i servizi di sicurezza (ESEC) a Redu, in Belgio.

cial-off-the-shelf). Questi micro o pico-satelliti, i cosiddetti "CubeSats", possono essere sviluppati e messi in orbita a costi molto abbordabili (poche centinaia di migliaia di euro) e sono quindi molto appetibili per piccoli imprenditori, istituti di ricerca e accademie. Il lato negativo della medaglia è che i controlli di sicurezza e gli standard per questa classe di satelliti sono praticamente inesistenti. Il rischio allora è che possano essere hackerati da attori malintenzionati, per essere usati come armi contro asset spaziali più grandi e vitali.
Limitandoci allo scenario europeo, le uniche due iniziative europee in materia di sicurezza spaziale a livello istituzionale provengono dalla "European Space Agency" (ESA) e dalla "European Union Space Programme Agency" (EUSPA).
L'ESA sta creando un nuovo centro per la sicurezza informatica che proteggerà tutti i sistemi dell'Agenzia dalle interferenze esterne, estendendosi dalle infrastrutture di terra dell'ESA in tutto il mondo ai satelliti in orbita.
Entrando in attività nel 2024, il nuovo Cyber-Security Operations Center (C-SOC) dell'ESA fornirà una capacità di monitoraggio e gestione informatica a livello di Agenzia, sotto la responsabilità tecnica dell'Ufficio di sicurezza dell'ESA (fig. 5).
In ambito Unione Europea, le attività di EUSPA e della "EC Space Security" sono svolte principalmente dal "Security Accreditation Board" (SAB).
Il SAB è l'autorità di accreditamento di sicurezza per tutte le componenti del programma spaziale dell'UE e prende le sue decisioni in modo completamente indipendente. È composto da un rappresentante di ciascuno Stato membro, un rappresentante della Commissione e un rappresentante dell'Alto rappresentante per l'Unione per gli affari esteri e la politica di sicurezza.
Il SAB garantisce che i sistemi spaziali sviluppati a livello istituzionale europeo siano conformi ai requisiti di sicurezza pertinenti e fornisce dichiarazioni di autorizzazione per le operazioni di sistemi e servizi.
Le sue decisioni sono adottate sulla base delle valutazioni effettuate dalle autorità nazionali di accreditamento di sicurezza competenti, delle verifiche eseguite dal Dipartimento di accreditamento di sicurezza dell'EUSPA e delle raccomandazioni del suo gruppo tecnico.
In conclusione, vale la pena di ricordare che il SAB sarà sempre più coinvolto nelle tematiche relative alla sicurezza dei programmi europei Copernicus e GOVSATCOM.

PAROLE CHIAVE
GNSS; sicurezza spaziele; conflitti; jamming; spoofing

ABSTRACT
In recent years it has been repeatedly discussed, even on the pages of this Magazine, of the dependence of our society from space systems and attacks, more or less evident, worked against them in various forms.
Particularly worrying, for whom deals with geomatics, were the various and often repeated episodes of "jamming" and "spoofing" towards signals GNSS, especially GPS, in various areas of the world, such as the Middle East, Strait of Hormuz, China Sea, Korea. No less serious, though perhaps less well known, the attempts at attacks cybernetic versus satellite systems for Earth observation and the communications.

AUTORE
Marco Lisi
ingmarcolisi@gmail.com