Comando Operazioni in Rete della DIFESA

Framework per la cyber sicurezza dei sistemi spaziali

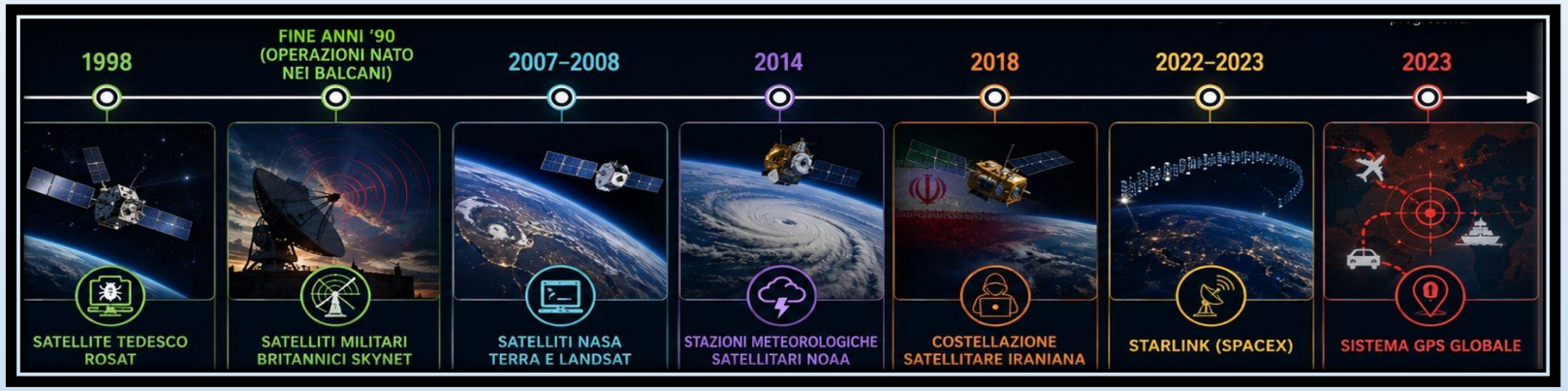
Roma, 3 Giugno 2026

C.A. Giovanbattista RAIMONDI
Vice Comandante del COR

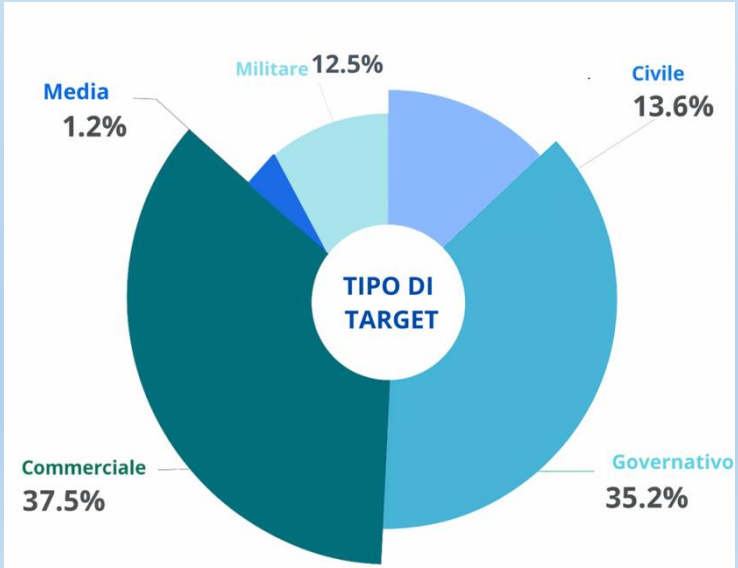
COMANDO PER LE OPERAZIONI IN RETE

CYBERSECURITY SPAZIALE: 20 ANNI DI MINACCE IN ESCALATION

L'attacco a KA-SAT del 24 febbraio 2022 il culmine di un'escalation



Conflitto Israelo-Palestinese:
234 operazioni cibernetiche contro il Settore spaziale.
73 Threat Actors
77 Space Entities Targeted



Fondazione Serics su dati Enisa marzo 25 «SPACE THREAT LANDSCAPE»

ASSET STRATEGICI, non solo militari

SUPERFICIE D'ATTACCO estesa complessa da difendere (Space, Ground, IT, OT e Supply Chain) e in aumento.

EVOLUZIONE DELLA MINACCIA
Threat actors statuali e non utilizzano TTP avanzate e AI

COMANDO PER LE OPERAZIONI IN RETE

Quale sensibilità per la sicurezza cyber nel dominio spaziale?

- ***La sicurezza del dominio spaziale e quello cyber fortemente interdipendenti***

- ***La cyber sicurezza nel dominio spaziale non ancora gestita con opportuna sensibilità e attenzione***

LA CYBER SICUREZZA NEL CYBER SPACE È UN'AREA DI CONFINE TRA DOMINIO CYBER E SPACE

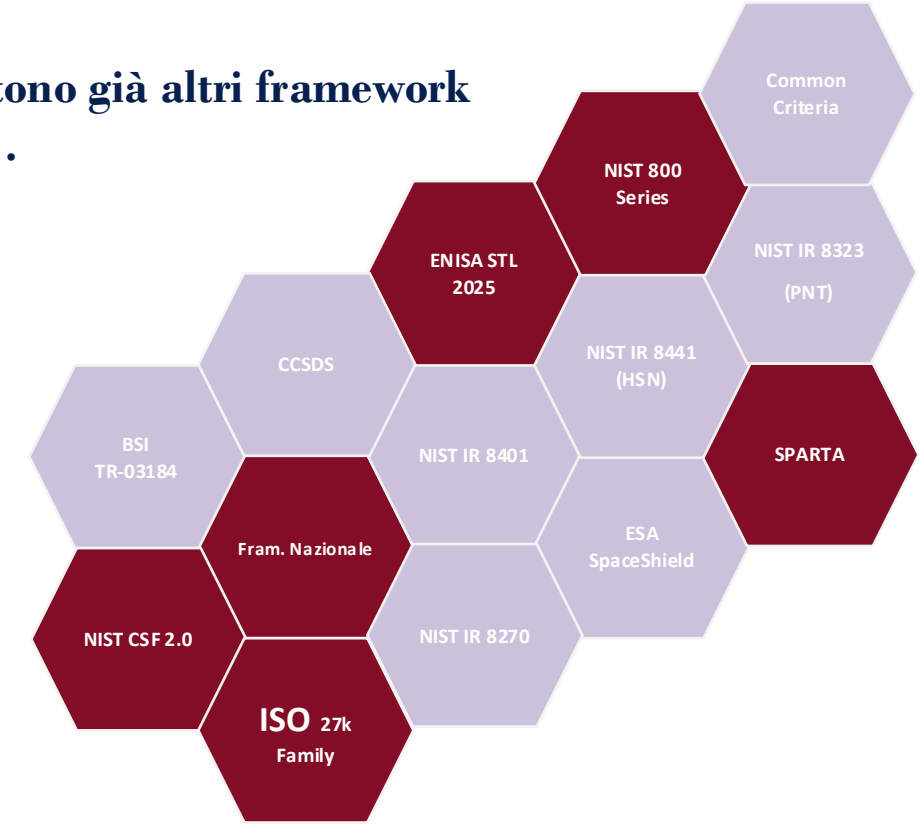
Fortunatamente COMINT del 19 febbraio 2025 ha finanziato progetto di sicurezza cyber nel dominio spaziale

COMANDO PER LE OPERAZIONI IN RETE

FRAMEWORK CYBERSECURITY PER IL DOMINIO SPAZIALE

STANDARD E FRAMEWORK DI RIFERIMENTO

Esistono già altri framework ma…



SFIDE DELL'APLICAZIONE DEL FRAMEWORK NEL DOMINIO SPAZIALE

1. **Framework Generalisti**
   Dispendioso impelementare i Framework, perché richiedono lavoro di declinazione nel caso specifico
2. **Frammentazione dei framework**
   Standard non integrati e difficili da applicare al dominio spaziale.
3. **Eterogeneità tecnologica**
   Tecnologie proprietarie ed eterogenee (segmenti Space, Ground e Communication) ostacolano l'applicazione dei Framework esistenti e la gestione della supply chian
4. **Specifiche minacce cyber poco considerate**
   Meccanismi inefficaci per integrare nei Framework il contesto operativo e la minaccia cyber
5. **Difficoltà di prioritizzazione**
   Risorse limitate impongono decisioni basate su rischio, missione e contesto.

L'obiettivo non era sostituire i framework esistenti, ma integrarli e renderli adattabili alle specificità del dominio spaziale facilitandone al contempo il loro impiego.

COMANDO PER LE OPERAZIONI IN RETE

enisa STL

DEFINIZIONE DEL CONTESTO

Identificazione di segmento, asset

- Missione
- Asset e architetture
- Segmento (Space, Ground, Communication)
- Ruolo e responsabilità

STL | SPARTA | ISO 27000 | NIST CSF 2.0 | FRAMEWORK NAZIONALE

BASELINE LAYER

- Controlli fondamentali sempre applicabili
- Protezione minima dell'infrastruttura
- Foundation security

CONDITIONAL LAYER

MANDATORY MEASURES

Selezione e attivazione dei controlli minimi necessari

- Aumento misure di **resilienza**, di **detection** e di **continuità operativa** necessario in funzione minaccia attesa
- Misure proporzionate al rischio residuo **massimo accettabile**

ENHANCING MEASURES

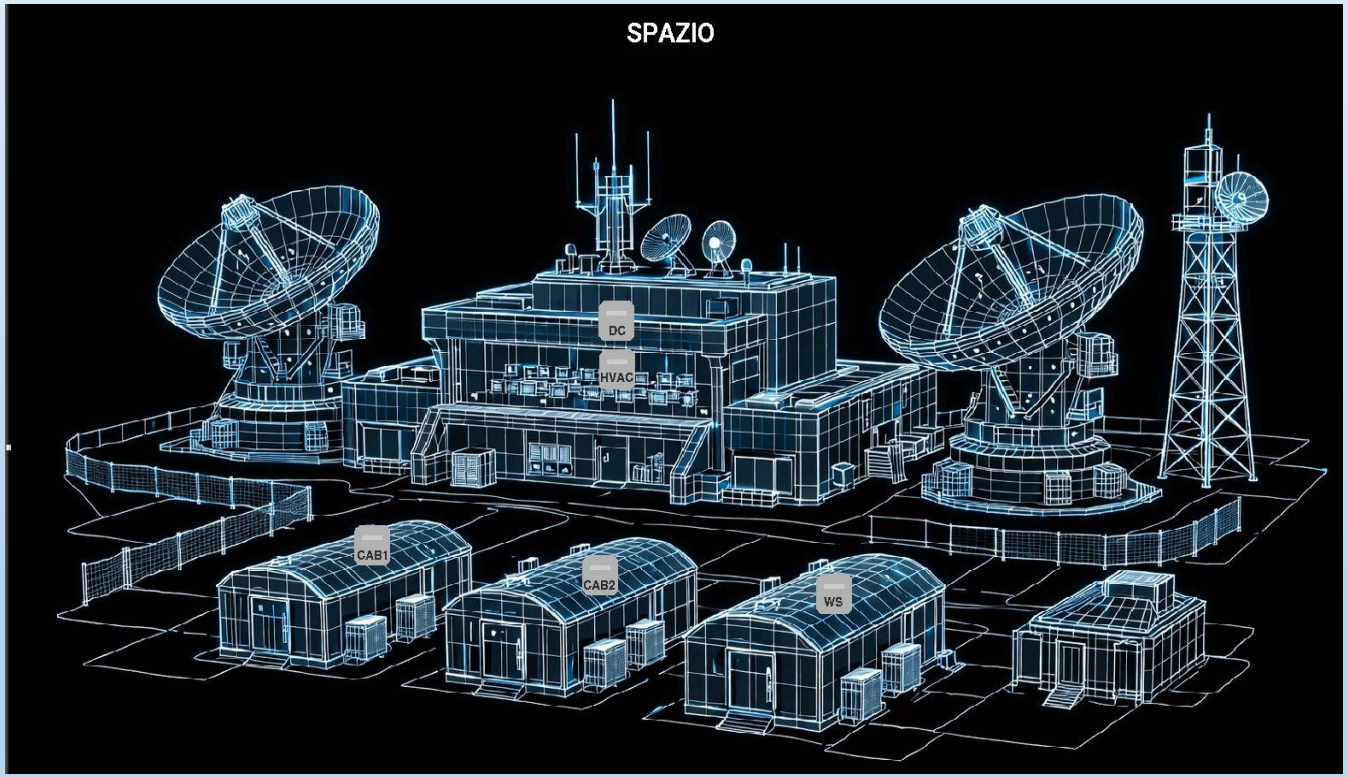
Selezione dei controlli di rafforzamento

- Ulteriore aumento misure di **resilienza**, di **detection** e di **continuità operativa** per ridurre il rischio residuo al **livello desiderato**

VALIDAZIONE OPERATIVA NEL CYBER RANGE

- Esecuzione scenari attack & defense
- Misurazione efficacia controlli
- Ottimizzazione costi benefici

ULTIMA FASE: VALIDAZIONE ATTRAVERSO IL CYBER RANGE

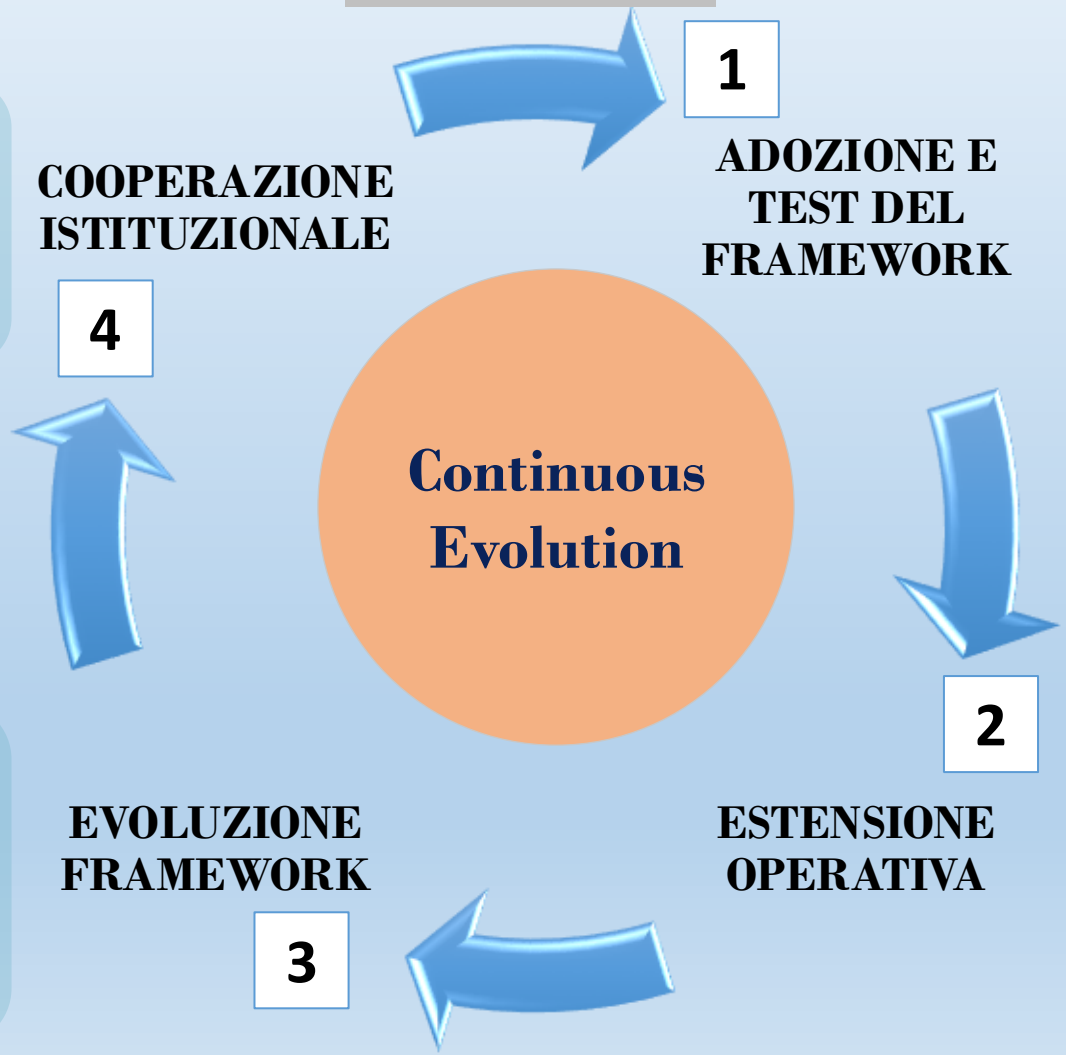


- **Validazione dei risultati teorici** del framework**,** attraverso **infrastruttura virtuale IT/OT molto simile a quella reale.**
- Servizi e flussi tipici del **Ground Segment** e dell'intero ciclo operativo Telecommand → On-board handling → Telemetry ➔ **esercitazioni di attacco e difesa realistiche**
- **Grado di complessità anche maggiore di quello reale** (per gli aspetti di cyber sicurezza) ➔ si possono testare capacità e moduli prima di farlo effettivamente.
- **Verifica capacità e procedure indicate dal Framework** ➔ Reale efficacia dell'organizzazione attuale o di quella che recepisce i processi migliorativi.
- **Individuare priorità nell'implementare nuove capacità tecniche e organizzative**
- Cyber Range potenzialmente aperto a collaborazioni fuori dal Dicastero

COMANDO PER LE OPERAZIONI IN RETE

Il progetto pone le basi per un framework evolutivo a supporto della sicurezza cyber nel dominio spaziale

NEXT STEPS



- Raccolta feedback e Tavoli tecnici
- Confronto con operatori
- Consolidamento metodologico

- Ampliamento a scenari multi-dominio
- Estensione controlli
- Supply chain

- Aggiornamento continuo TTP
- Estensione casi d'uso
- Evoluzione maturity model
- AI

- Difesa
- Altri Enti istituzionali
- Cooperazione Pubblico – Industria Privata
- Possibili sperimentazioni

Comando Operazioni in Rete della DIFESA

Framework per la cyber sicurezza dei sistemi spaziali

Roma, 3 Giugno 2026

C.A. Giovanbattista RAIMONDI
Vice Comandante del COR