

FORUM CYBER 4.0

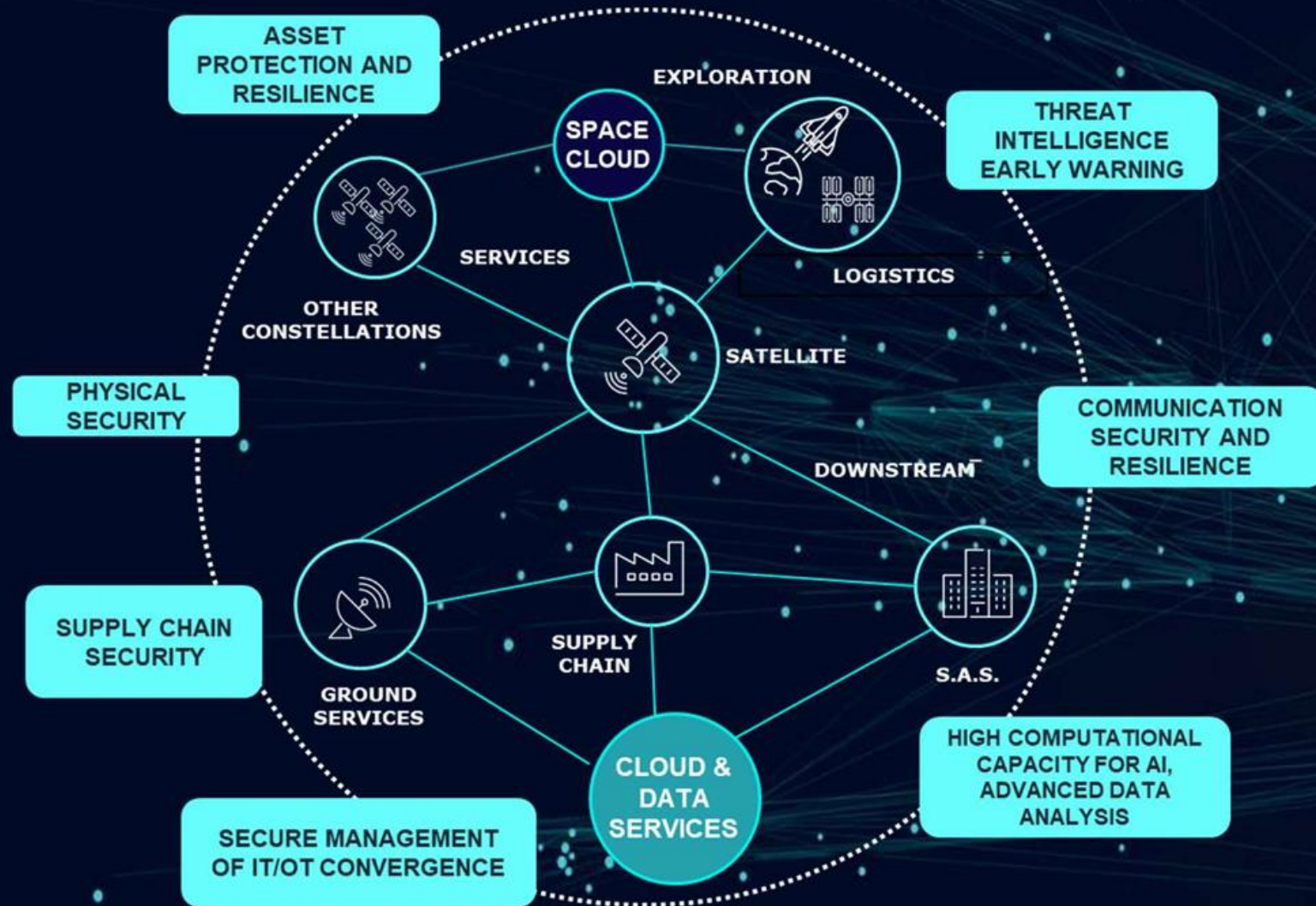
Panel: Difesa, spazio e dominio marittimo: la protezione delle infrastrutture strategiche

Giacomo Speretta, SVP Line of Business Space, NATO & EU Institutions
Divisione Cyber & Security Solutions

ROMA, 3 Giugno 2026

Please avoid printing this colourful slide. Let's save the planet together.

Leonardo: un approccio olistico alla sicurezza e resilienza dell'ecosistema Spazio



Un ecosistema complesso ed eterogeneo con asset (IT /OT) e servizi spaziali relativi al segmento di terra, ai sistemi in orbita e al segmento downstream /utente

La sicurezza e resilienza di questo ecosistema devono essere affrontate con un **approccio "olistico"** coerente con la complessità e l'elevato livello di interdipendenze del sistema stesso

E' essenziale operare per priorità, identificando le **contromisure più efficaci ed efficienti** anche miglior rapporto costi e benefici per contrastare la minaccia



Dal Framework alle regole da applicare sul campo

Un virtuoso coordinamento pubblico-privato per contribuire al **rafforzamento della postura di sicurezza dell'intera filiera spaziale**, rendendo applicabili le misure di sicurezza anche alle PMI secondo baseline sostenibili

Il Framework consente di:

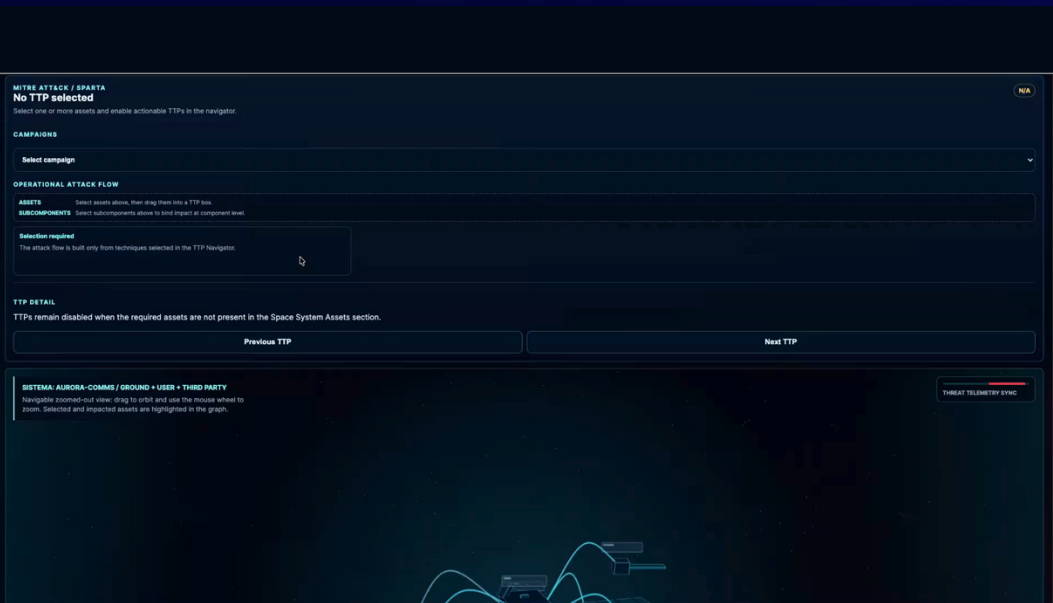
Identificare i controlli associati ad asset specifici delle infrastrutture spaziali e tracciabili rispetto alle tattiche tecniche e procedure utilizzate dai threat actor per violare gli assetti spaziali.

Applicare un approccio di threat informed defense

Prioritizzare gli interventi preventivi e difensivi secondo le modalità di attacco utilizzate dai threat actors

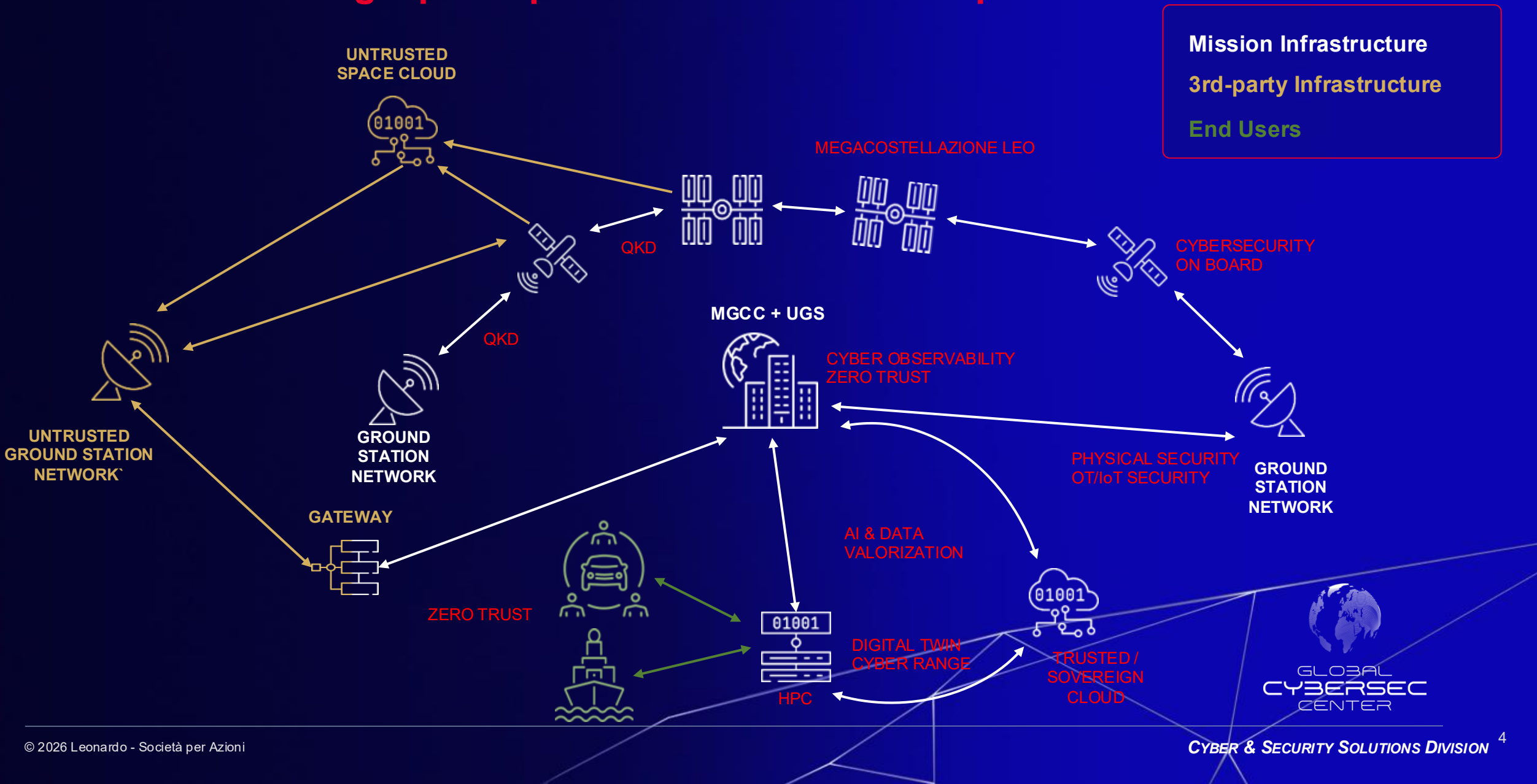
Mappare i pattern di attacco e controllare sistemi, sottosistemi e componenti HW/SW per la cyber resilience di prodotto

Valutare e gestire il rischio a livello di missione attraverso una visione "system of systems"





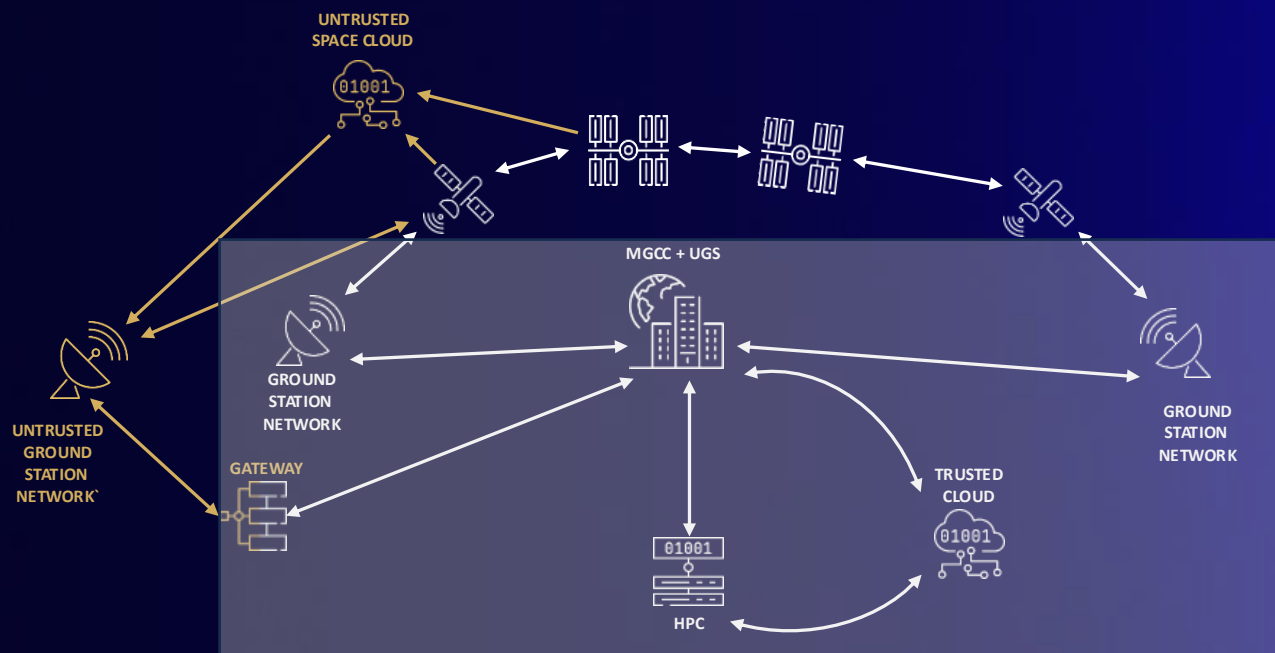
Soluzioni e tecnologie per la protezione del dominio Spazio





Focus su: ZERO TRUST

Ecosistemi complessi ed eterogenei con asset (IT /OT) richiedono di applicare il principio del “mai fidarsi, verificare sempre”



PAM IT /OT Agentless access management platform providing just-in-time credentials, centralized control, and session monitoring for secure, scalable privileged access to servers and cloud environments.

Policy-Based Access Control A dynamic authorization framework using user, resource, action, and context attributes to enforce fine-grained, policy-based access control across application platforms and distributed enterprise environments.

Encryption and Post-Quantum Cryptography Post-quantum network encryption platform delivering high-speed, crypto-agile, end-to-end protection using hybrid PQC algorithms, ensuring secure data transmission across data centers, cloud, and critical infrastructures.

Cross-Domain Gateway
Gateways and Diodes to implement Cross Domain network security solutions without impairing work process efficiency.



Thank you
for your attention

Please avoid printing this colourful slide. Let's save the planet together.

leonardo.com

