



Reparto Sistemi Informativi Automatizzati



CeSMA

Le IoT in operazioni multidominio

ICT SERVICE PROVIDER

Casa dell'aviatore, 04 Maggio 2022



Agenda



Vision e Mission

Reparto in breve

L'Infosfera

Multidominio e IoBT

Cyber Security

Conclusioni

ICT SERVICE PROVIDER



VISION

Polo ICT dell'Aeronautica Militare, in grado di promuovere **innovazione tecnologica** e la qualità dei servizi tipici del settore, in un contesto di **sicurezza cyber** nel quale esercitare un ruolo di attore principale di Forza Armata e di contributore per la Difesa ed il Paese.

ICT SERVICE PROVIDER





MISSION

- **Promuovere l'innovazione** attraverso la ricerca e la sperimentazione di nuove tecnologie nel settore ICT;
- **Progettare, realizzare e mantenere in esercizio** i servizi, i sistemi e le reti telematiche per l'automazione delle aree funzionali dell'Aeronautica Militare;
- **Garantire la Cyber Security** della F. A.;
- Provvedere all'**addestramento basilico** del personale ICT della F.A.

ICT SERVICE PROVIDER



Aree di Competenza



ICT SERVICE PROVIDER



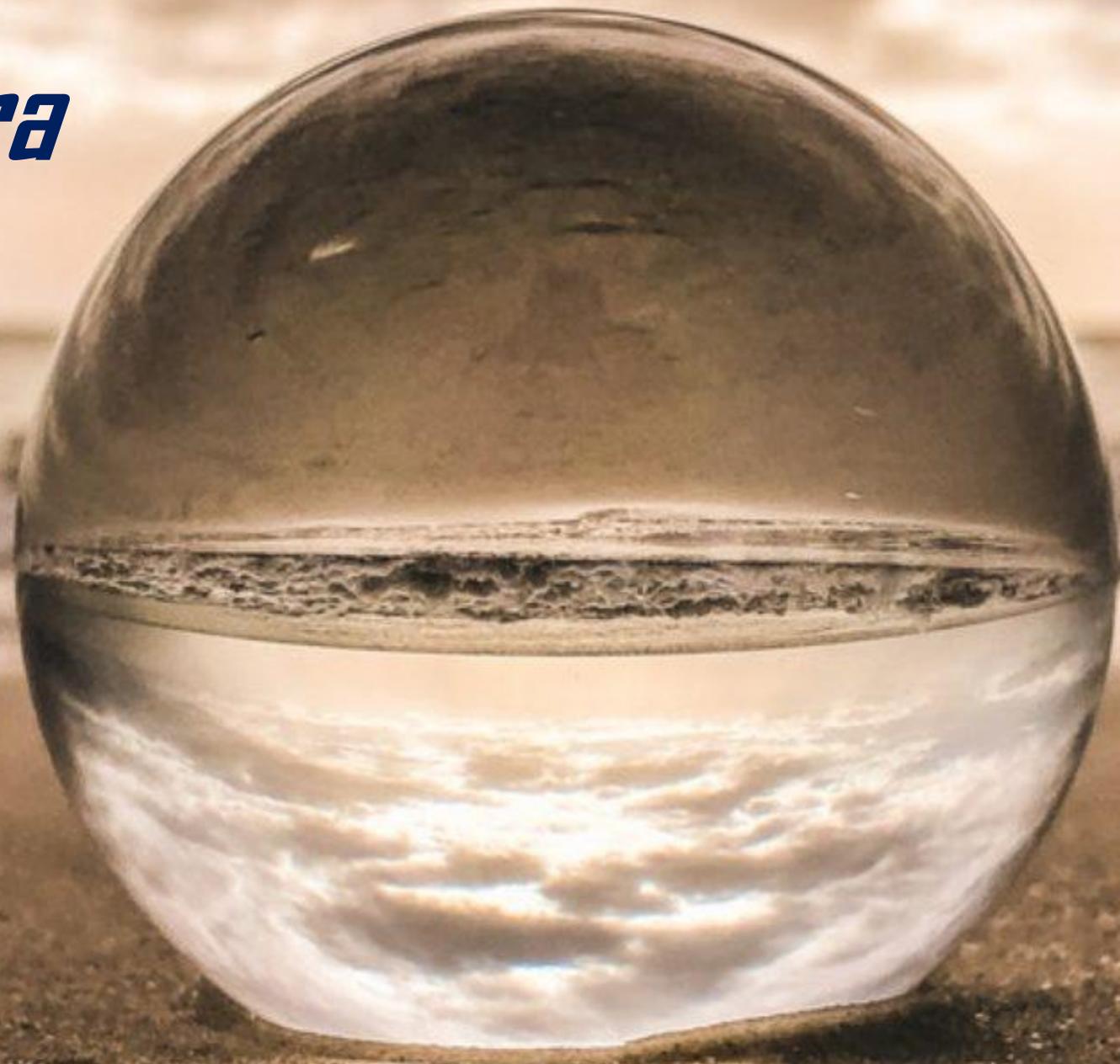
The mangroves society

OFF-LINE

ON-LINE



L'infosfera



“Siamo testimoni di una migrazione epocale e senza precedenti dell'umanità dallo spazio fisico newtoniano al nuovo ambiente dell'infosfera, anche perché quest'ultimo sta gradualmente assorbendo il primo”

Luciano Floridi



Multi-Dominio

Non si tratta di una semplice sommatoria di forze a cui aggiungere Satelliti e Computer ai classici domini

Sincronizzazione di obiettivi e strumenti capace di assicurare alle proprie forze la libertà di azione sempre e dovunque (anche nell'immateriale e nello spazio)



Imporre all'avversario dei dilemmi strategici irrisolvibili che facciano pendere l'ago della bilancia a suo sfavore.

«Consegnare lo strumento giusto al momento giusto al combattente sul campo di battaglia» - Gen. Philip Breedlove (17esimo comandante supremo alleato in Europa)

Multi-Dominio

La dimensione cyber unisce il dominio tradizionale (fisico) a quello immateriale trasformando la triade di fattori spazio, tempo e forze



- Comprime il tempo
- Dilata lo spazio
- Rende meno rilevanti le forze

IoT

Internet of Things

Oggetti del mondo digitale portati nell'esperienza quotidiana
(lavorativa e personale)

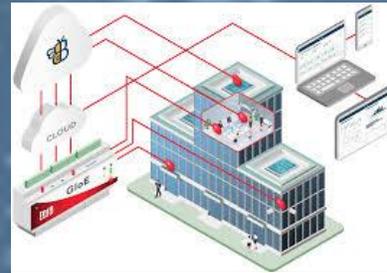
Privata



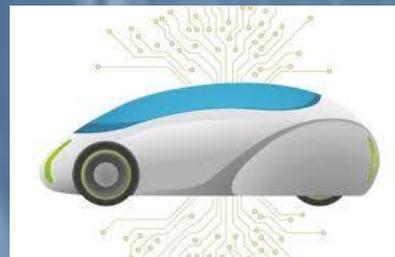
Lavorativa



Smart Home



Smart Building



Auto Intelligenti



Smart Health



Smart Factory



IoBT

IoBT / IoMT

Internet of Battlefield Things / Internet of Military Things

Oggetti del mondo IoT (rete di sensori e dispositivi interconnessi) che permettano di aumentare la consapevolezza situazionale degli operatori impegnati sul campo



Intelligence

Ricognizione



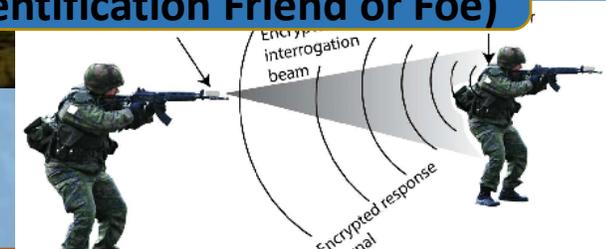
Sorveglianza



IFF
(Identification Friend or Foe)



Logistica



Percezione
extrasensoriale
dell'ambiente

Upgrade tattico /
decisionale

Multi-Dominio

Spazio

Aria

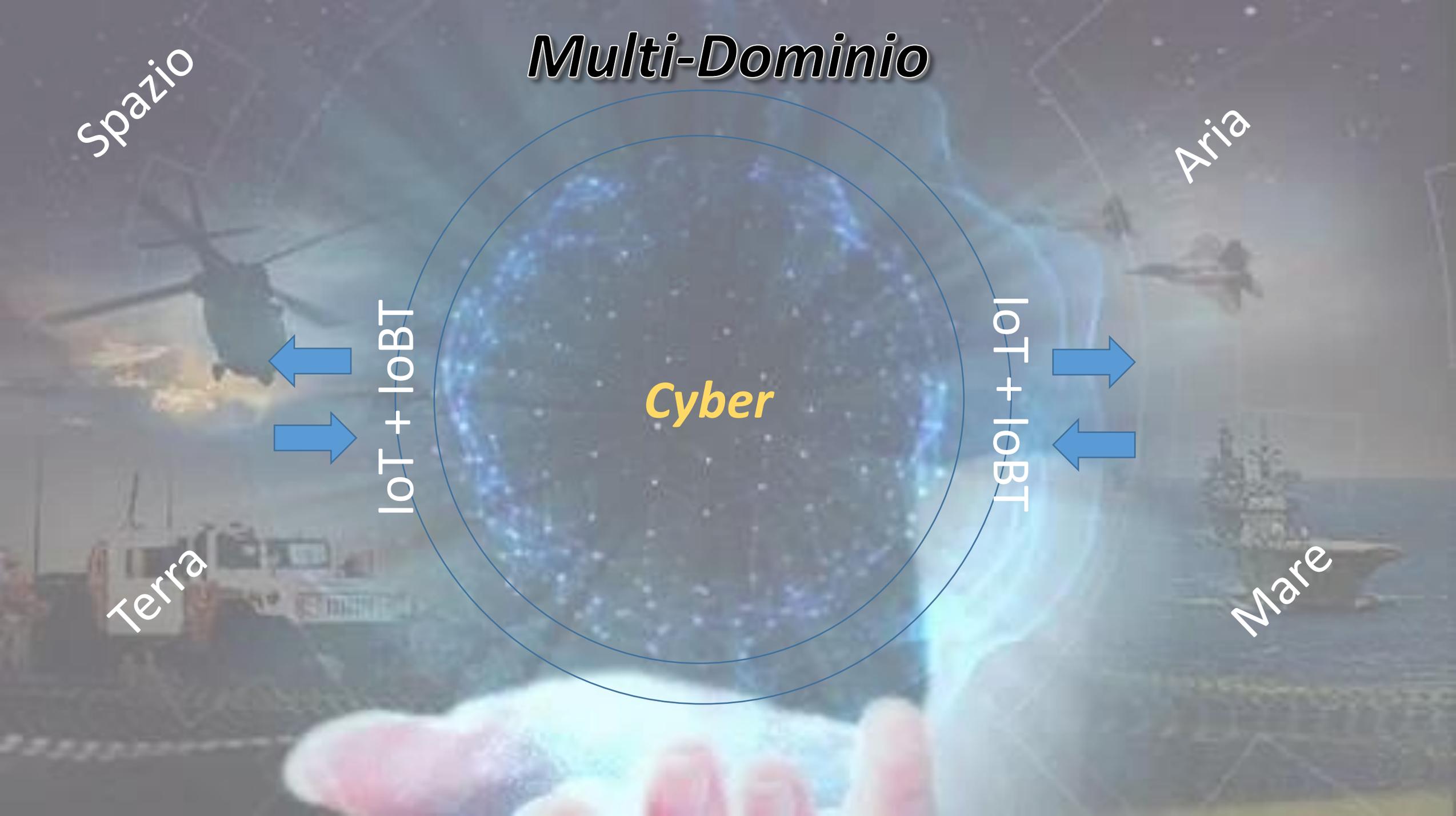
Cyber

IoT + IoBT

IoT + IoBT

Terra

Mare





IoBT

Reali Applicazioni in ambito militare

- Capacità C5ISR
- Sistemi logistici con l'impiego di sensori montati su aerei, UAV, satelliti e navi
- Monitoraggio delle condizioni fisiche dei soldati con sensori incorporati nelle uniformi dei militari.
- Manutenzione predittiva dei vari dispositivi attraverso l'analisi dei big data relativi alle condizioni delle piattaforme.



ICT SERVICE PROVIDER



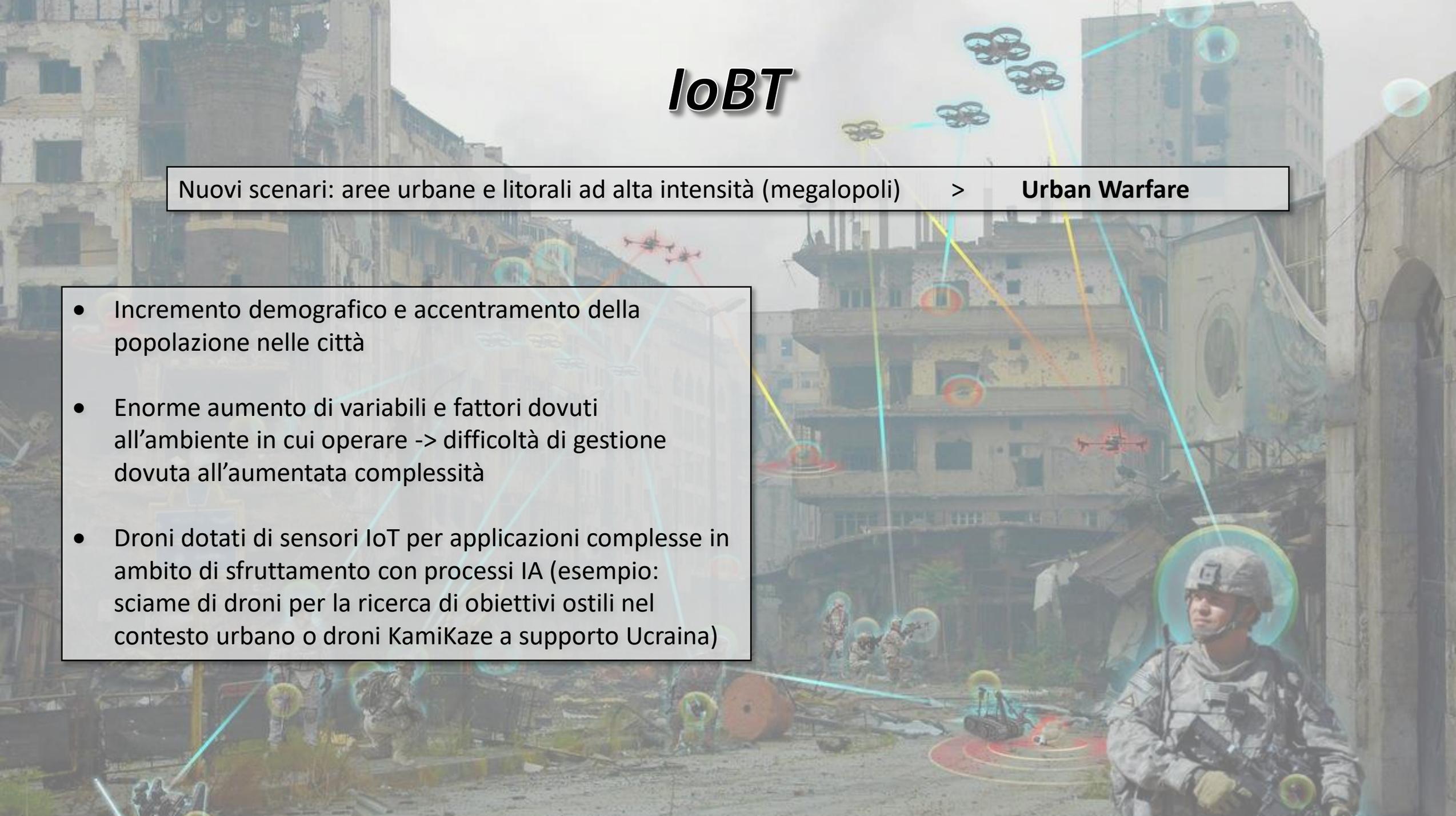
IoBT

Nuovi scenari: aree urbane e litorali ad alta intensità (megalopoli)

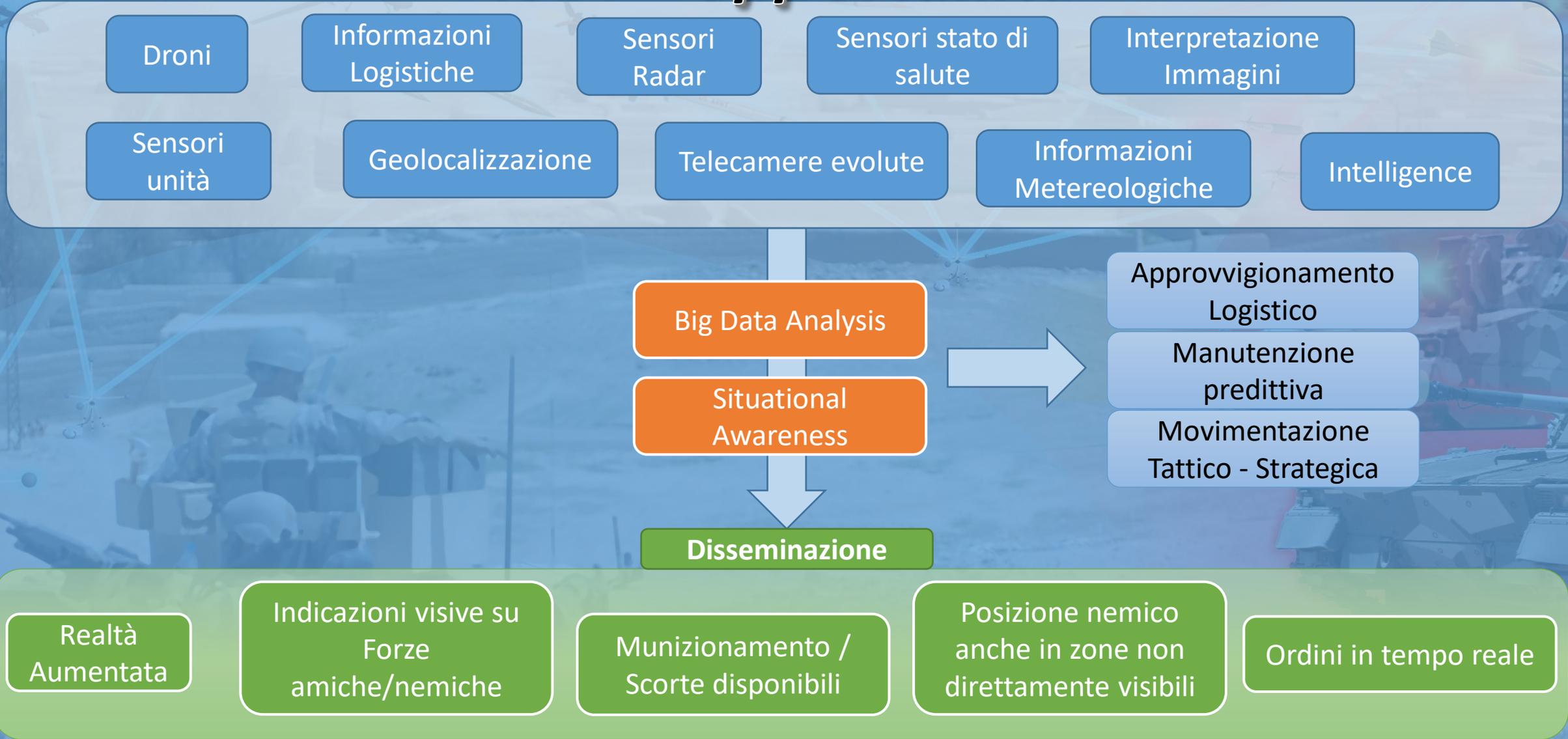
>

Urban Warfare

- Incremento demografico e accentramento della popolazione nelle città
- Enorme aumento di variabili e fattori dovuti all'ambiente in cui operare -> difficoltà di gestione dovuta all'aumentata complessità
- Droni dotati di sensori IoT per applicazioni complesse in ambito di sfruttamento con processi IA (esempio: sciame di droni per la ricerca di obiettivi ostili nel contesto urbano o droni KamiKaze a supporto Ucraina)

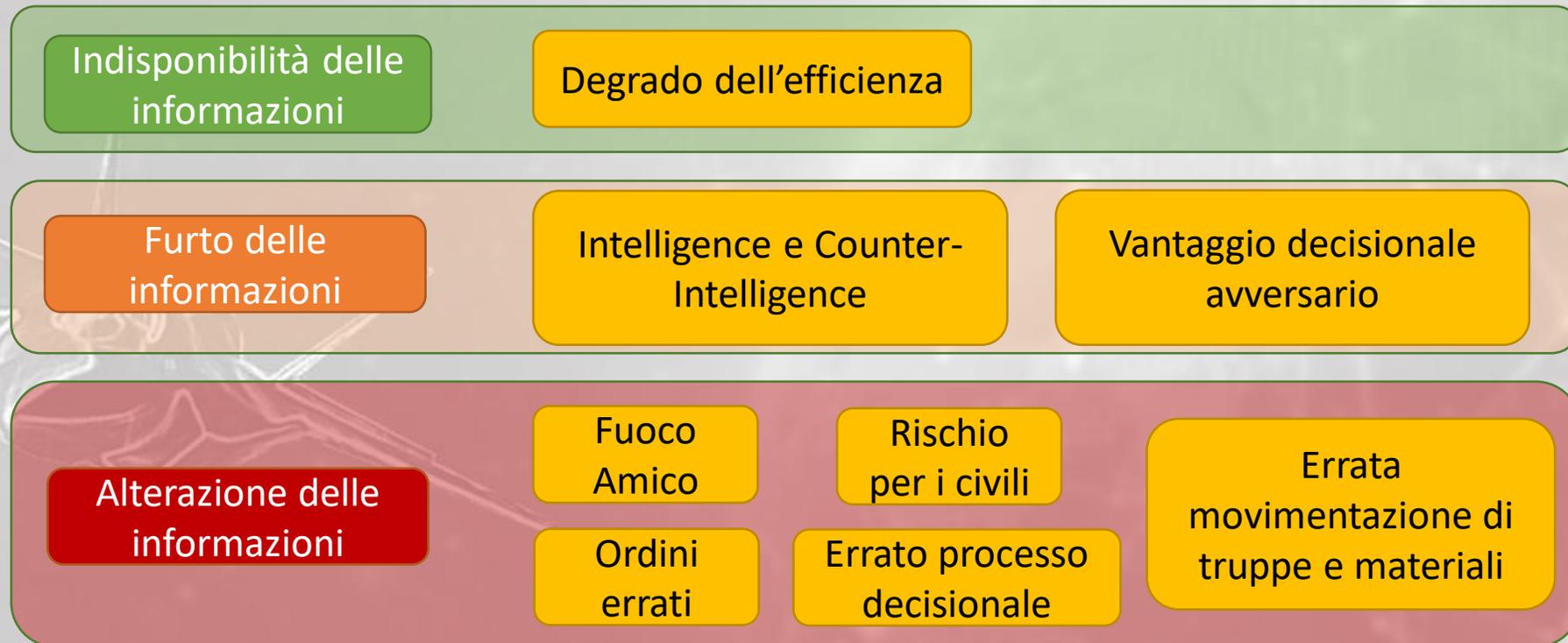


IoBT - Opportunità



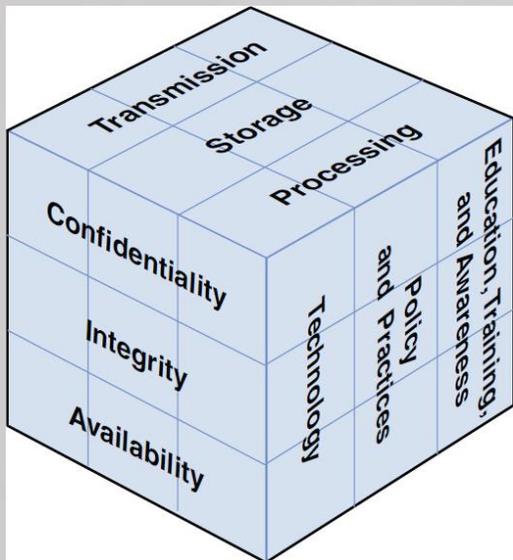
IoBT - Rischi

Impatto – Alla stregua dei dispositivi casalinghi... ma con impatti sulle operazioni militari



ICT SERVICE PROVIDER

IoT - Contromisure



Crittografia delle comunicazioni

Dove il canale di comunicazione non è protetto, è necessario utilizzare VPN o tecnologie similari

Accurata selezione dei dispositivi

Privilegiare Vendor «eticamente» corretti e affidabili

Network Access Control (NAC)

Accurato controllo dell'accesso fisico alla rete

Compartimentazione

Separazione fisica e logica delle reti

Asset catalog

Censimento stringente dei dispositivi connessi alla rete e manutenzione/aggiornamento costante

Monitoring

Monitoring Capillare

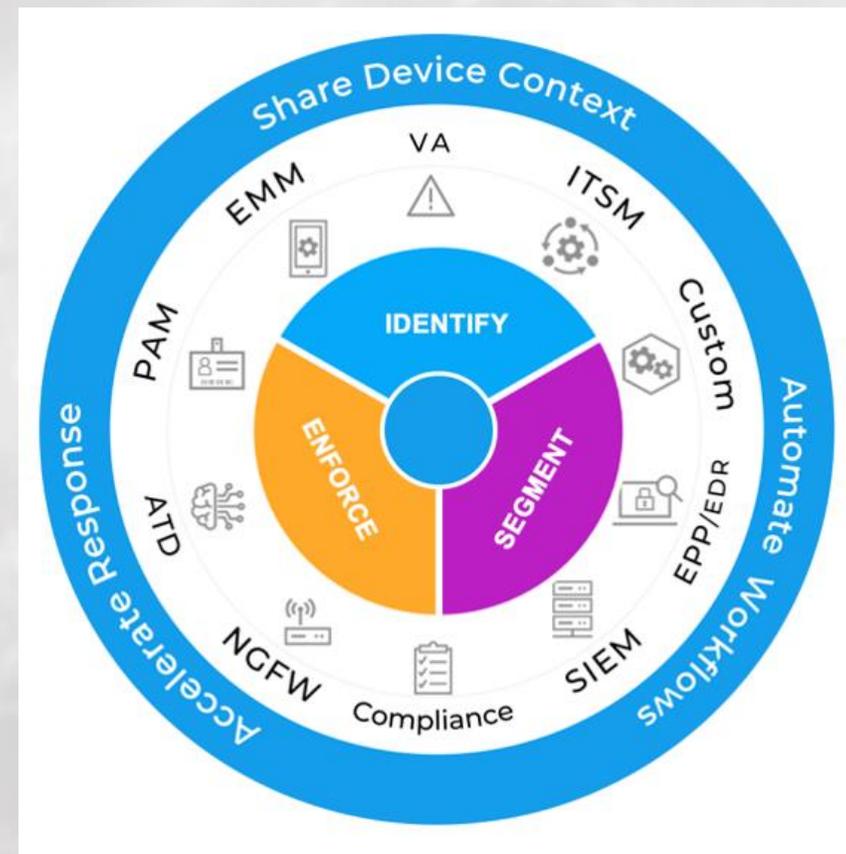
ICT SERVICE PROVIDER





Come si protegge l'Aeronautica

- **SEGMENTAZIONE DELLE RETI**
- **CONTROLLO FISICO DELL'ACCESSO ALLA RETE**
- **CONTROLLO COMPORTAMENTALE DEI DISPOSITIVI CONNESSI**
- **VERIFICA DELLA COMPLIANCE DEI DISPOSITIVI**
- **THREAT HUNTING E DECEPTION**
- **MONITORAGGIO ATTIVO**
- **COMPARTIMENTAZIONE DELLE RETI**
- **COSTANTE ATTIVITA' DI BONIFICA E TUNING VOLTE ALLA RIDUZIONE DEL RUMORE**



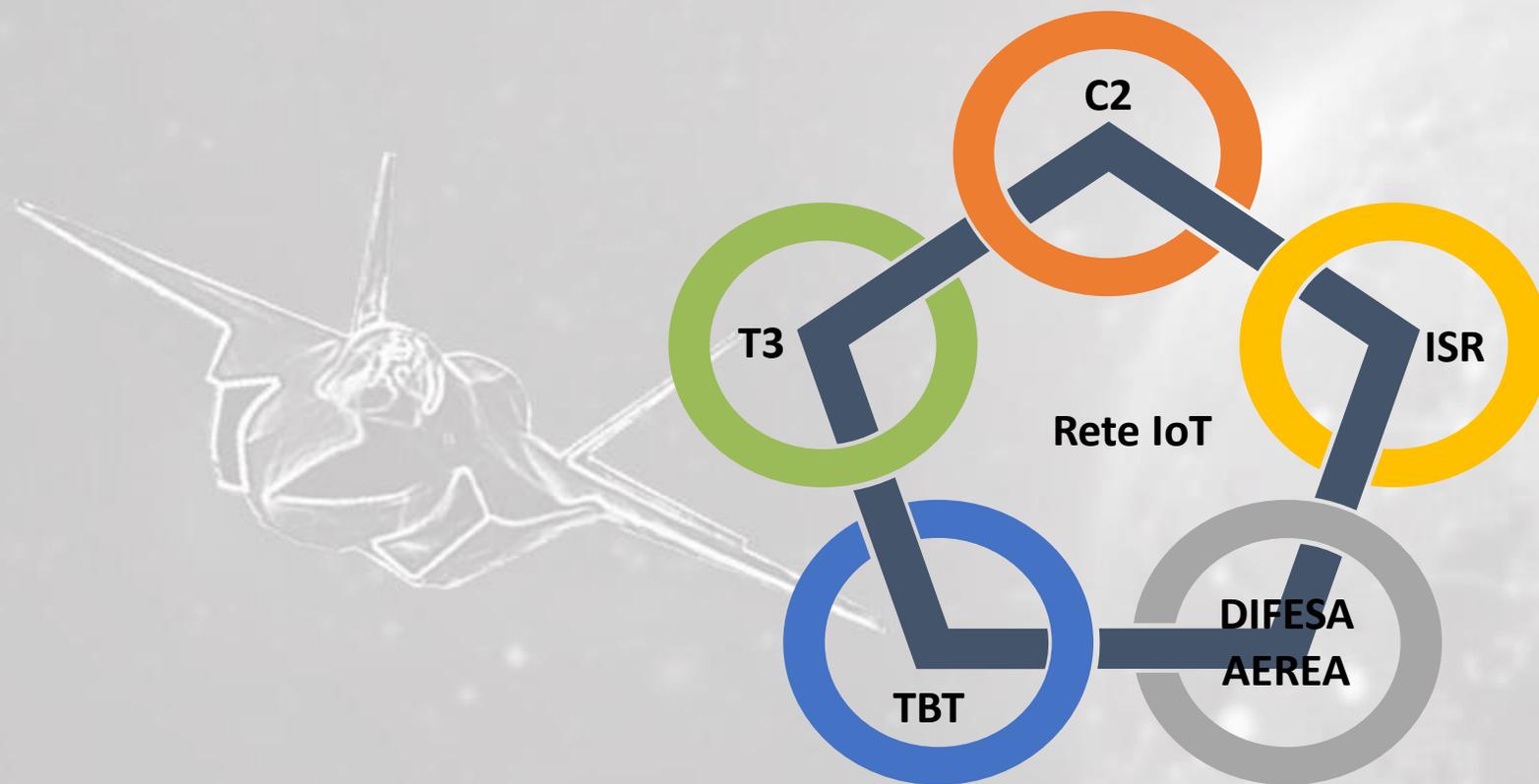
ICT SERVICE PROVIDER





Come si protegge l'Aeronautica

**RETE IOT DELL'AERONAUTICA MILITARE
SERVIZI E SISTEMI OPERATIVI**



ICT SERVICE PROVIDER



Compliance

- Comply to connect
- «Conosci te stesso»
- Configuration Management Data Base (CMDB)



Percezione dei segnali deboli

- Falsi positivi/falsi negativi
- Federazioni
- Multi-tenancy
- Impiego SIEM (Security Information & Event Management)

Riduzione del rumore



A hand in a dark suit jacket is shown holding a glowing blue digital circuit board. The board is filled with intricate white circuit traces and numerous bright white dots, representing data points or nodes. The background is a gradient of light blue to white, with the circuit board appearing to be held up against it.

Sfide per il futuro

Trasformazione digitale

Adeguamento dei sistemi legacy

Digital persona

Mindset adeguato ad operare nell'infosfera

Conclusioni

- Continuo aggiornamento per restare al passo con le **innovazioni** e soddisfare le esigenze specifiche di una Forza Aerea moderna;
- Impegno per garantire la **Cyber Security** dei sistemi di F.A., con un occhio alle **nuove tecnologie** e **nuove opportunità** che si presentano;
- Continuo studio finalizzato all'**integrazione** della tecnologia con il mondo militare

ICT SERVICE PROVIDER





Domande ?