

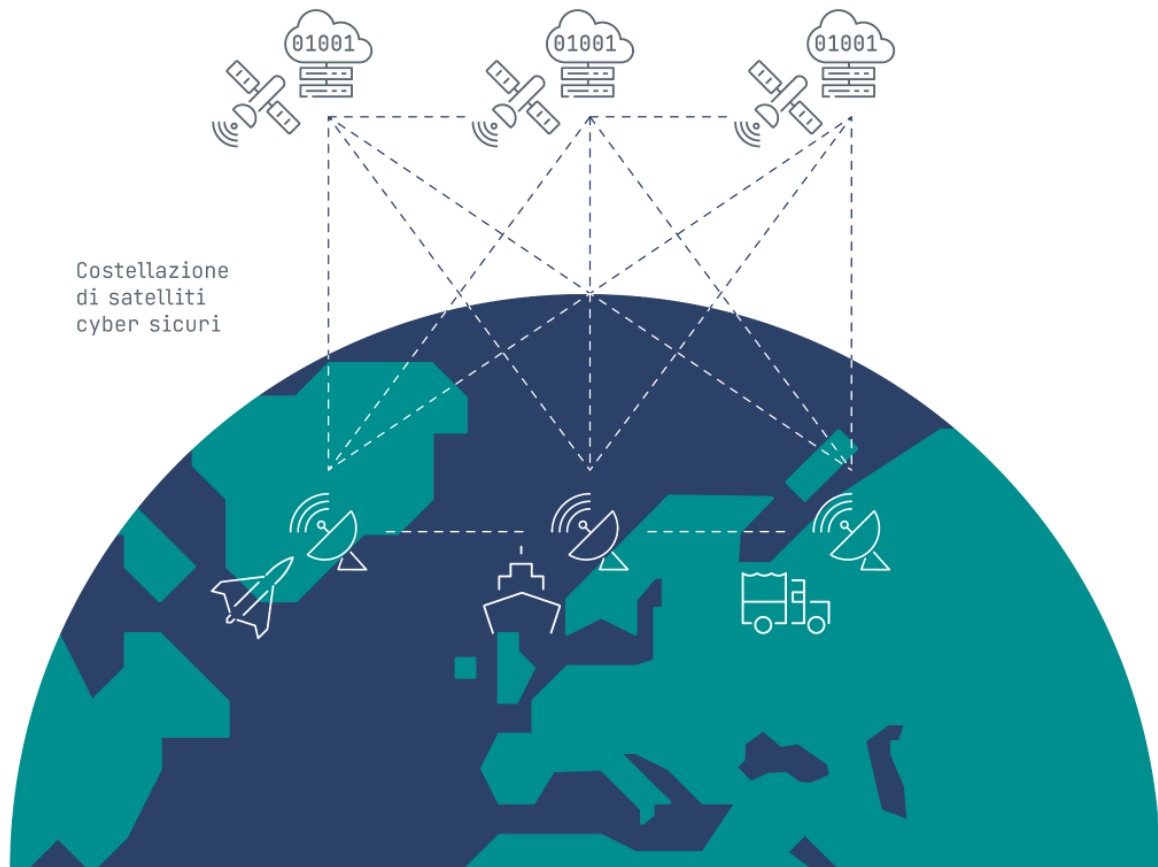


# I DOMINI IMMATERIALI

REDAZIONE OHIMAG  
OHIMAG REPORT NR. 81 – APRILE 2025

OHi MAG – REPORT GEOPOLITICO

I CONTRIBUTI SONO DIRETTA RESPONSABILITÀ DEGLI AUTORI E NE RISPECCHIANO LE IDEE PERSONALI. LE FOTO PRESENTI IN QUESTA CPM SONO STATE DI MASSIMA PRESE DAL WEB, CITANDONE SEMPRE LA FONTE. SE QUALCUNO DOVESSE RITENERE NECESSARIO RIMUOVERLE O MODIFICARNE GLI AUTORI, PUÒ CONTATTARCI SUL SITO OHIMAGAZINE.COM E SARÀ PRONTAMENTE ACCONTENTATO. LA RIPRODUZIONE, TOTALE O PARZIALE, È AUTORIZZATA A CONDIZIONE DI CITARE LA FONTE.



[https://www.leonardo.com/it/focus-detail/-/detail/tecnologie-multi-dominio\\_focus](https://www.leonardo.com/it/focus-detail/-/detail/tecnologie-multi-dominio_focus)

## Cyber e spazio nel nuovo scacchiere geopolitico

Il panorama strategico contemporaneo è teatro di una trasformazione radicale, indotta da un'inarrestabile progresso tecnologico e da un'interconnessione globale sempre più pervasiva. In questo scenario dinamico, i concetti tradizionali di

conflitto e sicurezza nazionale appaiono inadeguati a interpretare le nuove sfide. La presente analisi si propone di esplorare questa metamorfosi, focalizzandosi sull'ascesa dei domini digitali e aerospaziali, i quali non rappresentano più semplici teatri operativi, ma si configurano come elementi imprescindibili di una strategia militare multidominio integrata.

La complessità intrinseca del contesto attuale si manifesta attraverso eventi eterogenei, apparentemente scollegati dalle dinamiche militari classiche. L'incagliamento di una mega-nave nel Canale di Suez e il tragico crollo del ponte di Baltimora, pur nella loro diversità, agiscono da potenti simboli della vulnerabilità insita nei sistemi complessi, una fragilità che risuona con particolare intensità nel delicato ecosistema del dominio cibernetico. Comprendere appieno questa intricata rete di interdipendenze diviene, pertanto, un imperativo strategico di primaria importanza.

L'efficacia di un'analisi strategica si misura anche nella sua capacità di connettere la teoria con la realtà empirica. In tal senso, l'aneddoto riguardante il Presidente Reagan e la sua reazione al film "War Games" non è un semplice richiamo nostalgico, ma un premonitore avvertimento sulla potenziale fragilità dei sistemi di comando e controllo di fronte a minacce informatiche. Analogamente, i riferimenti a incidenti marittimi e le preoccupazioni relative all'uso dei social media da parte del personale militare illustrano come le vulnerabilità possano manifestarsi in contesti inattesi, radicandosi nelle sfide concrete del presente. L'analisi sinergica delle dinamiche di cooperazione e confronto, unitamente all'esplorazione multidimensionale degli effetti delle operazioni, offre un solido quadro concettuale per navigare la complessità del moderno teatro operativo.

Per affrontare questa inedita complessità, si è progressivamente affermato il concetto di Operazioni Multidominio (MD). Questo approccio rivoluzionario postula l'integrazione sinergica dei domini tradizionali – terra, mare, cielo – con i nuovi e cruciali ambiti del Cyber e dello Spazio, supportati e influenzati dagli ambienti elettromagnetico e informativo. L'obiettivo primario delle operazioni MD risiede nella creazione di un effetto moltiplicatore di forze, ottenuto attraverso una sincronizzazione meticolosa e una coordinazione senza precedenti delle attività in tutti i domini pertinenti, culminando nel conseguimento di una superiorità strategica decisiva. L'integrazione nativa delle capacità, la fluidità della sincronizzazione, la rapidità di reazione e l'agilità nell'adattamento, unitamente a

una flessibilità intrinseca, costituiscono i pilastri fondanti di questo nuovo paradigma operativo.

In questo scenario evolutivo, il campo di battaglia si estende ben oltre i confini fisici del conflitto armato, abbracciando un ampio spettro di interazioni che coinvolgono le sfere diplomatica, informativa, militare ed economica (DIME). Attori statali e non statali perseguono con tenacia i propri interessi strategici, spesso attraverso una competizione continua e multiforme che si manifesta al di sotto della soglia del conflitto aperto. In tale contesto, il dominio Cyber si distingue per la sua natura intrinsecamente virtuale, ubiquitaria e profondamente trasversale. Esso permea e influenza in modo inedito tutti gli altri domini operativi, agendo come un connettore invisibile e un moltiplicatore di vulnerabilità e opportunità. L'ambiente operativo multidominio si configura, quindi, come un ecosistema dinamico e interconnesso, composto da infrastrutture fisiche e digitali, risorse materiali e immateriali, la dimensione umana con le sue intricate interazioni e le crescenti dipendenze tecnologiche.

Le implicazioni geopolitiche di questa trasformazione paradigmatica sono di portata considerevole. La competizione tra potenze si intensifica, la guerra ibrida emerge come una modalità di confronto sempre più sofisticata e la deterrenza assume nuove e sfaccettate connotazioni, estendendosi al di là dei tradizionali arsenali.

Le dinamiche delle relazioni internazionali si muovono lungo un continuum fluido, che oscilla tra la cooperazione pragmatica e il confronto aperto, con il rischio costante di un'escalation verso il conflitto armato. Oltre ai domini fisici e al cyberspazio, acquisiscono crescente rilevanza strategica l'ambiente elettromagnetico – cruciale per le comunicazioni e la guerra elettronica –, l'ambiente informativo – fulcro della propaganda e della guerra psicologica – e la dimensione cognitiva – che influenza percezioni e processi decisionali. Non va inoltre trascurata la crescente importanza strategica della dimensione subacquea, teatro silenzioso di infrastrutture critiche e potenziali operazioni clandestine.

In questo complesso scenario, la "dimensione degli effetti" nelle operazioni multidominio impone una valutazione simultanea delle conseguenze fisiche tangibili, degli impatti virtuali sulle infrastrutture digitali, delle ripercussioni cognitive sulle percezioni e delle implicazioni informative sulla narrazione e la manipolazione dei dati.

È imperativo, inoltre, riconoscere la crescente complessità che caratterizza questo nuovo scenario strategico. La persistente "zona grigia" di incertezza, alimentata dalla difficoltà di attribuzione degli attacchi cibernetici e dalla fluidità delle minacce ibride, si somma a un progresso tecnologico incalzante, al superamento dei tradizionali confini geografici nel dominio digitale e a un elevato rischio di manipolazione informativa su scala globale. Elementi interconnessi quali i domini operativi specifici, gli effetti strategici ricercati, l'esperienza operativa accumulata, gli ambienti informatico ed elettromagnetico – sempre più interdipendenti –, le considerazioni Politiche, Militari, Economiche, Sociali, Infrastrutturali e Diplomatiche (PMESIID) e le continue innovazioni tecnologiche contribuiscono a delineare un quadro strategico di straordinaria complessità e criticità.

Il dominio Cyber si manifesta come un elemento intrinsecamente intangibile e trasversale, dotato della capacità di penetrare e manipolare un'immensa quantità di informazioni. La sua pervasività si esprime nella sua capacità di generare effetti significativi non solo nel mondo virtuale, attraverso l'attacco a infrastrutture critiche e la sottrazione di dati sensibili, ma anche nella sfera cognitiva, influenzando l'opinione pubblica, polarizzando il dibattito e minando la fiducia nelle istituzioni. In questo contesto, la sovranità digitale e la capacità di esercitare superiorità informativa divengono elementi cruciali per la sicurezza nazionale. L'anonimato garantito agli attori nel cyberspazio rappresenta una sfida formidabile per l'attribuzione degli attacchi e, di conseguenza, per l'efficacia delle strategie di deterrenza. Le caratteristiche distintive di questo dominio – dematerializzazione degli asset, deterritorializzazione delle operazioni, decentralizzazione delle infrastrutture e potenziale denazionalizzazione degli effetti – lo configurano sempre più come uno strumento fondamentale del potere nazionale, capace di proiettare influenza su scala globale con costi e rischi apparentemente inferiori rispetto alle operazioni militari convenzionali.

Il dominio spaziale si configura come un'arena strategica di importanza crescente, caratterizzata da una rapida evoluzione tecnologica e da significative barriere d'accesso. La proliferazione di tecnologie a duplice uso, i rischi di spionaggio, sabotaggio di assetti spaziali e la crescente minaccia dei detriti orbitali ne sottolineano il ruolo cruciale per la sicurezza e la prosperità delle nazioni. La militarizzazione dello spazio, che spazia dall'impiego di satelliti per migliorare le forze convenzionali fino al potenziale dispiegamento di armi in orbita, lo rende un elemento critico per la proiezione di potenza e la deterrenza nel XXI secolo.

Le attività spaziali sono profondamente integrate nel tessuto economico globale, influenzando politiche governative, istituzionali e lo sviluppo socio-economico, con applicazioni quotidiane in telecomunicazioni, navigazione e sicurezza. Un mancato sfruttamento di questo dominio comporterebbe gravi conseguenze per un paese come l'Italia, potenza marittima con interessi globali. La dipendenza dal commercio internazionale rende il paese vulnerabile a interferenze con le vie di comunicazione marittime, la cui sicurezza è strettamente legata alle capacità spaziali per la navigazione, le comunicazioni e la sorveglianza.

La mancata autonomia nel settore spaziale e la dipendenza da fornitori esterni per servizi satellitari creano vulnerabilità significative, con potenziali ripercussioni sulla sicurezza nazionale e sulla capacità di proteggere gli interessi marittimi, inclusa la sicurezza informatica, sempre più dipendente da infrastrutture spaziali. Un ritardo nello sviluppo di capacità spaziali autonome, inclusa la sorveglianza, le comunicazioni sicure e l'intelligence, porterebbe a un pericoloso gap capacitivo, limitando la capacità di operare efficacemente in uno scenario geopolitico in evoluzione e di tutelare gli interessi nazionali sul mare. In un contesto in cui lo spazio è riconosciuto come un dominio operativo, rimanere indietro significherebbe perdere un elemento fondamentale per la sicurezza, la difesa e la competitività economica del paese.

Nel concludere questa breve relazione sui domini e per navigare questo complesso panorama, ci è sembrato opportuno se non essenziale comprendere le definizioni chiave nel campo della cybersecurity che ne delineano i contorni.

Il Cyber Spazio può essere definito come un dominio globale e dinamico, costituito dall'interconnessione di reti informatiche, sistemi di comunicazione e infrastrutture tecnologiche che elaborano e trasmettono dati digitali. Le Operazioni nel Cyber Spazio comprendono azioni offensive e difensive condotte attraverso o all'interno di questo dominio, con l'obiettivo primario di preservare la propria libertà d'azione e negarla all'avversario.

Un Cyber Attack consiste in un tentativo di violare la riservatezza, l'integrità o la disponibilità di un sistema informatico o dei dati in esso contenuti.

Il Cyber Crime sfrutta il cyberspazio per attività illegali a scopo di lucro, spesso con una portata transnazionale e un elevato grado di anonimato.

Seda un lato lo Spionaggio Informatico mira alla sottrazione illecita di informazioni sensibili per ottenere vantaggi militari, politici o economici, dall'altro il Sabotaggio

Cyber ha come obiettivo la compromissione o la distruzione di sistemi informatici e infrastrutture critiche.

Il Cyber Terrorismo rappresenta l'uso del cyberspazio da parte di organizzazioni terroristiche per scopi di propaganda, reclutamento, finanziamento o per lanciare attacchi destabilizzanti.

La Cyber War si configura come un conflitto nel dominio cibernetico tra stati o attori statali, caratterizzato da operazioni offensive e difensive su larga scala.

Infine, la Cyber Security si concentra sull'implementazione di misure per proteggere i sistemi e le informazioni digitali da minacce, garantendone riservatezza, integrità e disponibilità, mentre la Cyber Defence comprende le strategie e le capacità volte a prevenire, rilevare, rispondere e ripristinare sistemi e dati in seguito a un attacco informatico.

La disamina di queste definizioni, unitamente all'esposizione dei principi operativi che guidano la protezione del cyberspazio – quali responsabilità, precisione e calibratura – e alla panoramica delle possibili risposte agli incidenti cyber – che spaziano dalla resilienza informatica all'azione di contrasto, dalle sanzioni all'intervento diplomatico e, in ultima istanza, all'impiego di capacità informatiche offensive – evidenzia la necessità di un approccio multidimensionale e proattivo alla salvaguardia del dominio digitale.

La menzione dell'Etica Cybernetica, che indaga le implicazioni morali dell'uso delle tecnologie digitali, della Cyber Escalation, che esplora il rischio di un'escalation incontrollata nel conflitto cibernetico, e della Cyber Deterrence, una strategia volta a dissuadere potenziali aggressori dal lanciare attacchi informatici, attraverso la minaccia credibile di ritorsioni significative ovvero puntare sulla minaccia di ritorsione. Ciò induce a ulteriori considerazioni critiche per il futuro del confronto digitale.

Le riflessioni di esperti come Ian Bremmer, con la sua analisi del "momento tecnopolare", e Joseph Nye, che interroga la potenziale fine dell'"anarchia cibernetica", offrono preziose prospettive sul contesto geopolitico in continua evoluzione. Bremmer evidenzia come la concentrazione di potere nelle mani di poche aziende tecnologiche e le dinamiche concorrenziali tra blocchi di potere stiano frammentando il panorama digitale globale. Nye, dal canto suo, sottolinea i pericoli economici e geopolitici derivanti dall'assenza di un ordine normativo consolidato

nel cyberspazio e la necessità di strategie di deterrenza efficaci per garantire la stabilità.

In conclusione, l'analisi dei nuovi domini delle operazioni militari, con una particolare attenzione al Cyber e allo Spazio, delinea un quadro strategico globale in profonda trasformazione. Sebbene la complessità e la rapidità dell'innovazione tecnologica rendano ogni valutazione intrinsecamente dinamica, emerge con chiarezza la centralità di questi domini immateriali sulle dinamiche di potere del XXI secolo. La consapevolezza della natura pervasiva e insidiosa della minaccia, spesso celata in un'ambigua "Area Grigia" di difficile attribuzione, e del suo potenziale dirompente in continua crescita – come vividamente rappresentato da scenari futuri di conflitto quali quelli ipotizzati nel romanzo "2034" – impone una riflessione strategica incessante e un investimento costante nello sviluppo di capacità multidominio integrate e resilienti. Solo attraverso una comprensione approfondita di queste nuove dinamiche, unitamente a un quadro normativo internazionale più robusto e condiviso, sarà possibile navigare con successo le incertezze e le sfide dell'era digitale e preservare la sicurezza e la stabilità globale.