Lo Spazio all’Aeronautica, il Subacqueo alla Marina: perché il Cyber spetta all’Esercito

Pubblicato il 04/06/2026

Il dibattito sulla governance dei nuovi domini della conflittualità si sta accendendo a livello globale. Negli Stati Uniti, la proposta bipartisan di inserire la nascente **Cyber Force** sotto l'egida dell'U.S. Army (all'interno del National Defense Authorization Act) traccia una via che molti alleati occidentali, Italia inclusa, guardano con attenzione.

Perché questa tripartizione – **Spazio all'Aeronautica, Subacqueo alla Marina e Cyber all'Esercito** – non è solo una spartizione burocratica, ma una scelta dottrinale simmetrica, equilibrata e strategicamente coerente?

La simmetria dei Domini: Prolungamenti Naturali

L'assegnazione dei domini tradizionali e di quelli emergenti segue una logica di "prolungamento naturale" delle competenze storiche delle singole Forze Armate.

- **Aeronautica e Spazio:** Lo spazio orbitale è la prosecuzione verticale dell'atmosfera. Chi domina la terza dimensione (il volo) possiede già la cultura tecnologica, la gestione dei vettori, dei satelliti e dei sistemi di sorveglianza radar necessari per la *Space Economy* e la *Space Defense*.
- **Marina e Subacqueo:** Il mondo sottomarino (il cosiddetto *underwater*) è la continuazione abissale della superficie del mare. La protezione dei cavi dati sottomarini, dei gasdotti e la guerra acustica richiedono una cultura d'ambiente che solo chi naviga possiede.
- **Esercito e Cyber:** A prima vista, il cyberspazio sembra immateriale. In realtà, **la rete poggia sulla terraferma**. Server farm, nodi di comunicazione, dorsali in fibra ottica e infrastrutture critiche sono fisicamente radicati sul territorio. L'Esercito, forza territoriale per eccellenza, ha come missione la protezione e il controllo della terraferma, rendendolo il guardiano naturale dell'infrastruttura fisica del web.

Le 3 Buone Ragioni per dare la Lead della Cyber all'Esercito

Oltre alla continuità geografica, ci sono ragioni operative, demografiche e dottrinali che rendono l'Esercito il candidato ideale per la *leadership* del dominio Cyber.

La centralità del "Fattore Umano" (Manpower e Reclutamento)

La guerra cibernetica non si fa con le macchine, si fa con le menti. Come evidenziato dai recenti studi analitici (tra cui quelli della *Foundation for Defense of Democracies*), una forza Cyber richiede una massa critica di personale (circa 10.000 unità per una struttura autonoma).

L'Esercito, essendo storicamente la Forza Armata più grande per numero di effettivi, possiede la struttura logistica, accademica e di reclutamento su larga scala adatta ad assorbire, formare e gestire una quantità enorme di specialisti, senza cannibalizzare le proprie capacità operative interne.

Cyber come "Artiglieria Moderna" nel Combattimento Terrestre

Nelle guerre contemporanee, l'attacco Cyber non è solo uno strumento di spionaggio, ma un'arma tattica di supporto. Spegnere i radar nemici, hackerare i droni avversari o interrompere le comunicazioni di un quartier generale prima di un attacco sono operazioni sovrapponibili

all'uso dell'artiglieria o del genio militare. L'integrazione degli *effetti cyber* nella dottrina del combattimento terrestre (interarma) è vitale per l'Esercito per proteggere i propri soldati e mezzi sul campo.

La resilienza delle Infrastrutture Critiche Nazionali

In caso di un attacco cyber massiccio che metta in ginocchio la rete elettrica, idrica o i trasporti di un Paese, la risposta non avviene nel mondo virtuale, ma nelle strade. È l'Esercito l'unica forza dotata di capacità logistiche pesanti e capillarità territoriale per garantire la continuità dello Stato, proteggere i nodi fisici della rete ed esercitare la difesa civile mentre i tecnici ripristinano i sistemi.

Un equilibrio di specchi

Affidare la *lead* del Cyber all'Esercito non significa sminuire il ruolo di Marina e Aeronautica (che manterranno comunque le loro indispensabili componenti cyber specializzate per navi e aerei), ma significa creare un **perfetto triumvirato dei domini emergenti**.

In questo schema, ogni Forza Armata riceve la responsabilità del dominio che più si adatta alla propria natura intrinseca:

Forza Armata	Dominio Tradizionale	Dominio Emergente	Focus Strategico
Aeronautica	Aria	**Spazio**	Alti vettori e sorveglianza orbitale
Marina	Mare	**Subacqueo**	Protezione fondali e linee di comunicazione marine
Esercito	Terra	**Cyber**	Difesa delle infrastrutture fisiche del web e supporto tattico

Questa ripartizione garantisce un bilanciamento perfetto del potere interforze, evita sovrapposizioni e assicura che nessun dominio venga trascurato. Il cyber ha bisogno di massa, terra e integrazione tattica: tre elementi che l'Esercito ha nel proprio DNA da secoli.

Link notizia: https://www.defenseone.com/policy/2026/05/cyber-force-service-branch-proposal/413863/?oref=d1-homepage-river