La sfida info-elettromagnetica nel multidominio

L'approccio multidominio si sta diffondendo oltre la Difesa, estendendosi alla capacità di uno Stato, o della Nato, di attivare l'impiego sincronizzato di tutti gli strumenti del potere nazionale. Ai cinque domini si aggiungono, come terreni di sfida militare, gli ambienti "informativo ed elettromagnetico" che costituiscono nuove sfide e minacce. Nell'ambiente informativo e nel *warfare* cognitivo la padronanza nell'impiego e nella gestione dei dati sarà alla base della superiorità militare

MARCO BRACCIOLI
co-direttore Cybersec initiatives Fondazione Icsa
e vice presidente Defense & cybersec Digital platforms

Partiamo con una definizione di "dominio" come un insieme di capacità e attività che vengono applicate al campo di battaglia, in un ambiente di riferimento. Recentemente ai domini tradizionali di terra, mare e aria si sono aggiunti i nuovi domini *cyber* e spazio. Quello *cyber* è stato introdotto dalla Nato come dominio al vertice di Varsavia del 2016, stabilendo che un attacco cibernetico può causare danni paragonabili a quelli di un attacco armato, rappresentando un caso di difesa collettiva ai sensi dell'articolo 5 del Trattato di Washington. Il dominio spazio da parte della Nato è stato introdotto in occasione dell'incontro di Bruxelles nel 2019 tra ministri degli Esteri. L'approccio multidominio si sta diffondendo oltre il comparto Difesa, estendendosi alla capacità di uno Stato, o della Nato, di attivare l'impiego sincronizzato di tutti gli strumenti del potere nazionale (diplomatico, informativo, economico e militare) all'interno del cosidetto "Continuum of competition" per opporsi agli avversari e contrastarne le azioni tutelando i propri interessi. Il multidominio non è la semplice somma dei singoli domini e delle singole capacità, ma la fusione sincronizzata in un "unicum" all'interno del quale è necessario armonizzare gli strumenti del potere nazionale e orchestrare le azioni delle diverse capacità per conseguire effetti multidimensionali. Le Multi-domain operations (Mdo) devono eliminare la separazione verticale e fisica delle singole componenti (terra, aria, mare, *cyber* e spazio) reiterando tale postura e combinandola con le attività di deception anticipando l'azione avversaria e creando una linea difensiva prudente in ogni dominio. Tale postura di contrasto si muove tra quattro pietre angolari: cooperazione e rivalità, che rappresentano uno stato di pace; confronto e conflitto armato che rappresentano la guerra. Immaginando anche situazioni fluide, però, gli attori avversari possono in un certo momento cooperare in un settore, scontrarsi in un altro oppure combattersi in un terzo. Ai cinque domini si aggiungono, come terreni di sfida militare, gli ambienti "informativo ed elettromagnetico" che costituiscono nuove sfide e nuove minacce (sia di attacco che difesa). Proprio nell'ambiente informativo e nel warfare cognitivo, la capacità di leggere e gestire la grande mole di dati in gioco sarà vitale per determinare il peso di ciascun attore statuale in ambito economico e politico, tanto che si parla di sovranità digitale. La padronanza nell'impiego e nella gestione dei dati sarà quindi alla base della superiorità militare, come fattore abilitante per il comando e controllo e per

Una definizione

Il "dominio" è da intendere come un insieme di capacità e attività che vengono applicate al campo di battaglia, in un ambiente di riferimento. Recentemente ai domini tradizionali di terra, mare e aria si sono aggiunti i nuovi domini *cyber* e spazio. Ma il multidominio non è la semplice somma dei singoli domini e delle singole capacità, ma la fusione sincronizzata in un "unicum" all'interno del quale bisogna armonizzare gli strumenti del potere nazionale e orchestrare le azioni delle diverse capacità per conseguire effetti multidimensionali.

Missioni multidominio

Le Multi-domain operations (Mdo) devono eliminare la separazione verticale e fisica delle singole componenti (terra, aria, mare, *cyber* e spazio) reiterando tale postura e combinandola con le attività di deception anticipando l'azione avversaria e creando una linea difensiva prudente in ogni dominio. Tale postura di contrasto si muove tra quattro pietre angolari: cooperazione e rivalità, che rappresentano uno stato di pace; confronto e conflitto armato che rappresentano la guerra.

condurre operazioni. Inoltre, l'impiego di software all'interno dei sistemi d'arma, combinato con la connettività e interoperabilità tra gli stessi, allarga il perimetro di vulnerabilità a minacce provenienti non solo dai domini tradizionali ma anche da quello *cyber*, richiedendo nuove misure a protezione delle Forze armate. Il *cyber-space* permette di proteggere l'anonimato degli attori avversari. Poiché è difficile monitorare le fonti degli attacchi che operano attraverso falsi indirizzi Ip e server stranieri, chi attacca gode di una certa impunità (non attribution) che porta man mano alla dematerializzazione, deterritorializzazione, decentralizzazione e denazionalizzazione dei conflitti digitali. E l'Italia? Il nostro Paese sta organizzando un complesso sistema di comandi proprio per sincronizzare gli sforzi provenienti da varie aree dello Stato. Partendo dal mondo civile, la costituzione dell'Agenzia cibernetica nazionale (Acn) fissa una pietra angolare sul tema della difesa delle infrastrutture critiche italiane così come la presidenza del Consiglio dei ministri si avvale del Comitato politico strategico (Cops) e del Nucleo interministeriale situazione e pianificazione (Nisp), mentre la Difesa contribuisce con il Comando operativo reti (Cor) e per lo spazio con il Comando operazioni spaziali (Cos). Sicuramente il dominio *cyber* è l'unico che riesce a concentrare al suo interno tutti gli strumenti del *national power*: militare, economico, diplomatico e quello che attiene il controllo dei media e la gestione delle informazioni. In tale contesto, per consentire al Paese di affrontare le sfide della minaccia cibernetica nelle sue molteplici forme, a partire da quella statuale, con la legge 133/2019 l'Italia ha istituito il "Perimetro di sicurezza nazionale cibernetica" quale risposta alla necessità di innalzare la resilienza di reti, sistemi informativi e servizi informatici degli attori nazionali (pubblici e privati) che esercitano una funzione o un servizio essenziale dello Stato, ovvero hanno carattere strategico per gli interessi del Paese. In definitiva le Mdo si basano sulla consapevolezza che non è possibile mantenere la supremazia in tutti i domini rispetto a un peer competitor, quindi l'obiettivo è di mantenere la libertà d'azione sincronizzando le azioni cross-domain per ottenere un vantaggio complessivo e non su una singola componente. Per concludere, il Nato Warfighting capstone concept, definisce così questo nuovo modo di confronto militare: *orchestrate and synchronize military and non-military activities across all domains and environment that enable commanders to deliver converging effects*. È iniziata la guerra dei sistemi contro sistemi.