STATO MAGGIORE DELLA DIFESA

Approccio della Difesa alle Operazioni Multidominio

Edizione 2022

Titolo: “Approccio della Difesa alle Operazioni Multidominio” Anno 2022

PREFAZIONE DEL CAPO DI STATO MAGGIORE DELLA DIFESA

Operare in un contesto altamente competitivo e complesso, impone alla Difesa di pensare al futuro attraverso un'ottica predittiva ed integrata, con l'obiettivo di preservare efficienza e credibilità, fattori decisivi sul campo di battaglia moderno.

La minaccia ibrida, le campagne di disinformazione, i conflitti ad intensità variabile ed i cosiddetti shock *naturali (disastri naturali, pandemie, ecc.), nel caratterizzare le traiettorie evolutive del futuro, richiederanno risposte integrate, tempestive e sinergiche a vantaggio del sistema Paese, soprattutto in tempi dominati da uno stato di competizione permanente tra attori statuali capaci di operare indistintamente in più domini con tutte le risorse disponibili.*

Per poter decifrare e comprendere le minacce circostanti, gestendone al contempo risposte efficaci, tempestive e capaci di generare effetti stabili nel tempo in tutti i domini di riferimento (terra, mare, aria, cyber e spazio), oltre che nell'ambiente informativo e della sfera cognitiva, la Difesa ha l'ineludibile necessità di disporre di reali capacità multidominio in grado di assicurare la sincronizzazione delle azioni e degli effetti.

Tuttavia, non è possibile generare una concreta capacità multidominio della Difesa prescindendo da una decisa e coordinata accelerazione del già avviato processo di integrazione interforze, destinato, giocoforza, ad essere superato e compreso nello stesso concetto di Multi-Domain Operations *(MDO).*

Tale integrazione, non più procrastinabile, è dunque un passaggio intermedio fondamentale in termini di programmazione, di formazione e di approccio complessivo, che deve essere perseguito, pur nel rispetto delle competenze e specificità di componente, con determinazione costante, superando con slancio ritrosie al cambiamento ed anacronistiche logiche di parte.

Date tali premesse, emerge quanto sia necessario definire una visione strategica nazionale unitaria e trasversalmente condivisa che delimiti il perimetro all'interno del quale le operazioni possano essere condotte. Occorre, quindi, superare con slancio rigide separazioni concettuali e dare coerenza alle informazioni raccolte, implementando una struttura di Comando e Controllo compiutamente multidominio, sulla base della quale garantire tempestività decisionale ed efficacia operativa. In tal senso, sarà necessario fondare tale

processo sui principi dell'integrazione e dell'interoperabilità tra sistemi, sensori, processi ed attori coinvolti nei diversi domini, sia a livello nazionale, sia a livello internazionale.

*Sarà inoltre importante favorire il confronto, l'interscambio ed il coordinamento inter-dicasteriale ed inter-agenzia, nonché un pragmatico dialogo con entità ed attori privati di settore, al fine di stimolare sinergie ed azioni condivise in modo strutturato, realizzando un autentico approccio di Sistema Paese (*Whole of Government*).*

In parallelo, sarà imprescindibile definire il nuovo ruolo dell'uomo rispetto all'evoluzione delle tecnologie emergenti per il quale risulterà strategico il rinnovamento del processo di selezione, formazione e valorizzazione del capitale umano (competenze tecnico-specialistiche ed educazione dei leader*).*

La leadership *è chiamata, quindi, ad aggiornare il proprio schema di riferimento alle operazioni, superando la logica di settore ed abbracciando consapevolmente l'idea dell'interconnessione. Si tratta dell'unica chiave di lettura possibile per ripensare al modo stesso di condotta delle operazioni e per adeguare, con coraggio, rapidità di risposta e lungimiranza, i processi e le organizzazioni. Tale indirizzo, peraltro, sarà alla base anche del necessario rinnovamento in termini di* policy*, dottrine, procedure e tattiche innovative, in modo da affrontare al meglio l'evoluzione del contesto e delle potenziali minacce.*

Questo documento rappresenta un passo significativo nel processo di evoluzione del pensiero strategico della Difesa, già intrapreso da tempo, ed intende contribuire a diffondere la consapevolezza, tra gli attori istituzionali, della necessità di sviluppare e perseguire un approccio nazionale efficace ed uniforme rispetto ad uno scenario multidimensionale che cambia e si trasforma rapidamente imponendo, quindi, risposte necessariamente di sistema.

È, questa, la premessa fondamentale per concretizzare una riflessione coerente sul tema, consentendo così, alla Difesa di realizzare speditamente operazioni multidominio efficaci, convergenti e rilevanti, moltiplicando in tal modo i ritorni positivi per il Paese anche attraverso adeguate capacità d'azione e deterrenza.

Buona lettura!

Ammiraglio
Giuseppe CAVO DRAGONE

INDICE

INTRODUZIONE
COMPRENDERE IL MULTIDOMINIO

IL CONCETTO DI MULTIDOMINIO

L'uso del termine *Multi-Domain* (MD) si è fortemente diffuso negli ultimi anni per lo sforzo profuso da parte di alcuni Paesi, principalmente occidentali, che hanno cercato di codificare il loro approccio alle operazioni militari oltre i **domini** tradizionali di terra, mare e cielo, al fine di integrare i nuovi domini *Cyber*[1] e Spazio[2], con conseguente estensione del campo di battaglia, e di fronteggiare le possibili strategie dei potenziali *peer-competitor* che, attraverso l'impiego coordinato di tutti gli strumenti del potere nell'ambito del *continuum of competition*[3], mirano a negare la possibilità di risposta alla controparte e a perseguire incontrastati i propri interessi strategici.

DOMINIO delle operazioni

Un insieme di capacità e attività che vengono applicate al campo di battaglia, in un ambiente di riferimento (marittimo, terrestre, aereo, cibernetico e spaziale).

Nonostante l'ampia diffusione del termine esistono molteplici definizioni, lasciando ampi spazi di interpretazione. Dalla sua prima concettualizzazione è stato, infatti, avviato un ampio dibattito internazionale che ha portato allo sviluppo di differenti approcci sul tema, riconducibili comunque alla necessità di fronteggiare le aggressioni ibride dei potenziali *peer-competitor*.

AMBIENTE

Contesto in cui si opera, compresi l'aria, le acque, il terreno, lo spazio, il *cyberspace*, le risorse naturali, la flora, la fauna, gli essere umani e le loro interazioni. Gli ambienti di riferimento per le operazioni militari sono: marittimo, terrestre, aereo, spaziale, cibernetico, a cui si aggiungono l'ambiente informativo e quello elettromagnetico.

L'effetto di robuste campagne di disinformazione ha altresì evidenziato la centralità dell'**ambiente** elettromagnetico e l'importanza della **dimensione** cognitiva del confronto al punto che l'ambiente informativo ha assunto una sempre maggiore rilevanza. In tale quadro, il concetto di Multidominio sta naturalmente evolvendo verso un approccio che miri a sviluppare, a prescindere dall'eventuale esigenza di riconoscimento ufficiale di un nuovo dominio, la capacità di generare effetti in tutte le possibili dimensioni del confronto (fisica, cognitiva e virtuale).

DIMENSIONE degli effetti

Schema concettuale che permette di valutare gli effetti da conseguire con le operazioni militari nel campo di battaglia nelle tre dimensioni: fisica, virtuale e cognitiva.

[1] Il *Cyber* è stato identificato dalla NATO quale dominio in occasione del vertice di Varsavia del 2016, riconoscendo che un attacco cibernetico può arrivare a causare danni paragonabili a quelli di un attacco armato e, quindi, diventare un caso di difesa collettiva ai sensi dell'articolo 5 del Trattato di Washington.

[2] Il riconoscimento del dominio Spazio da parte della NATO è avvenuto in occasione dell'incontro tra i Ministri degli Esteri dell'Alleanza svoltosi a Bruxelles nel 2019, in considerazione della sua rilevanza per la deterrenza e la Difesa, dalla navigazione all'*intelligence* sino all'individuazione delle minacce.

[3] NATO *Allied Joint Publication* - AJP-01-F (*draft*).

Dalla consapevolezza che la superiorità nei domini tradizionali potrebbe non essere facilmente ottenibile in un'era in cui si assiste ad una proliferazione di tecnologie a disposizione di attori statuali e non, nasce quindi l'esigenza di un cambio di paradigma verso un nuovo approccio Multidominio. Tale approccio si deve ispirare all'esigenza di generare effetti (letali e non letali) non al fine di avere la supremazia nel singolo dominio, ma di mantenerne la libertà d'azione generando effetti in tutte le dimensioni del confronto, migliorando la comprensione degli interessi e delle azioni dei potenziali avversari (*enhanced strategic anticipation and situational awareness*) e limitandone l'azione.

Inoltre, seppur nato e consolidato in un contesto esclusivamente militare volto a sviluppare la capacità di penetrare eventuali bolle *Anti-Access/Area Denial* (A2AD) avversarie, l'approccio Multidominio sta subendo una significativa espansione ben oltre il solo comparto Difesa, estendendosi alla capacità di uno Stato, o dell'Alleanza, di impiegare il proprio *power projection* attraverso l'impiego sincronizzato di tutti gli strumenti del Potere nazionale (Diplomatico, Informativo, Militare ed Economico – DIME) nell'ambito del *continuum of competition* per influenzare gli avversari e contrastarne le azioni tutelando i propri interessi. In tal senso, il Multidominio va inteso come esigenza di coniugare l'impiego del *Military Instrument of Power* (MIoP) con gli altri *Instruments of Power* (IoP).

LE RELAZIONI TRA I DOMINI

La distinzione tra i domini delle operazioni costituisce un utile strumento per la pianificazione e la condotta delle operazioni militari. Tale classificazione non tiene tuttavia conto dell'intero spettro di capacità a disposizione di una singola componente e della possibilità di generare effetti negli altri domini attraverso azioni di tipo c*ross-domain*.

Sebbene i cinque domini delle operazioni presentino caratteristiche differenti sono fortemente legati tra di loro. I tre domini classici (terrestre, marittimo e aereo), tradizionalmente legati alle singole componenti, non hanno precisi confini ma aree di congiunzione e sovrapposizione (es. aree litorali e costiere tra domini terrestre e marittimo, piattaforme aeree delle componenti terrestre e marittima che operano nel dominio aereo, piattaforme aeree che generano effetti sulla superficie, ecc.).

Il dominio Spazio è globale e autonomo, ma al contempo abilitante per i domini classici (settore civile e militare sono profondamente dipendenti dai servizi spaziali) per l'erogazione di funzioni critiche quali le comunicazioni satellitari ed i sistemi di *positioning, navigation and timing*.

Il dominio *Cyber*, infine, è caratterizzato dalla sua connotazione virtuale e *ubiquitas* e risulta trasversale a tutti gli altri domini.

LE DIMENSIONI DEGLI EFFETTI

Partendo dalle relazioni tra i domini, le azioni vengono pianificate e condotte avendo chiara la dimensione da influenzare o in cui far ricadere gli effetti desiderati per il raggiungimento della missione. Ciò può realizzarsi nelle seguenti dimensioni:

- **Fisica**, dove avvengono le attività fisiche e si verificano gli effetti fisici attraverso l'interazione tra geografia, infrastrutture, flora e fauna, individui, Stati, culture e società; tale dimensione è stata modellata dall'uomo nel tempo e può essere ulteriormente manipolata solo con uno sforzo considerevole che richiede tempo ed energie.
- **Virtuale**, dove avvengono le attività intangibili da parte di entità non tangibili che possono essere virtuali (come nel caso dei *social media*) o particolari *software*; questa dimensione può essere oggetto di manipolazione in quanto creata artificialmente.
- **Cognitiva**, afferente alla sfera delle percezioni e delle decisioni, nella quale possono essere conseguiti effetti sociali e psicologici che influenzano il comportamento di un individuo ottenendo così un risultato duraturo.

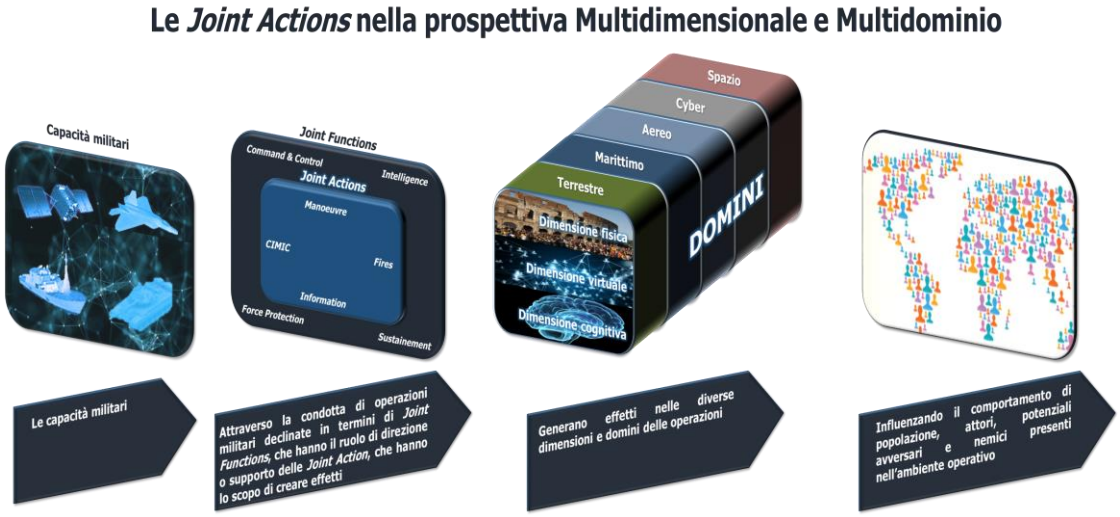
AZIONI ED EFFETTI NELLE DIVERSE DIMENSIONI

Il Multidominio non rappresenta la semplice somma dei singoli domini e, dunque, delle singole capacità. In questa nuova prospettiva sfumano i confini tra i domini ottenendo un *unicum* all'interno del quale è necessario armonizzare gli strumenti del Potere nazionale ed orchestrare le azioni delle diverse capacità per conseguire effetti multi-dimensionali. Nello specifico, i domini delle operazioni sono visti come un unico contesto interconnesso, in cui la condotta sincronizzata delle azioni e la modulazione dello sforzo permettono di conseguire un risultato di portata maggiore rispetto alla visione del dominio singolo. Sulla base degli obiettivi da conseguire, si determinano gli effetti da realizzare influenzando in più dimensioni gli attori dell'ambiente operativo di riferimento, dove gli effetti sono il risultato di azioni/attività condotte dalle capacità disponibili nei diversi domini (compreso l'ambiente elettromagnetico e l'ambiente informativo). Queste azioni, grazie alla permeabilità dei domini e alle caratteristiche dell'ambiente informativo, possono essere ulteriormente amplificate.

In questa prospettiva, occorre rilevare come cambiano la percezione e il comportamento degli attori al fine di poterli influenzare nel momento giusto attraverso una serie di azioni ("cinetiche" e "non-cinetiche") che producono effetti nelle dimensioni fisica, cognitiva e virtuale, correlate tra loro.

Date queste premesse, un approccio alle operazioni Multidominio (*Multi-Domain Operations* – MDO) deve permettere di superare la separazione verticale e fisica delle singole componenti ricercando e migliorando la comprensione e l'impiego delle diverse capacità/risorse (militari e civili) per sviluppare contemporaneamente più azioni convergenti e produrre più effetti nelle diverse dimensioni. La reiterazione nel tempo di questa postura, combinata con la sorpresa e le attività di *deception*, permetterà di conquistare e di mantenere l'iniziativa obbligando l'avversario ad adottare un atteggiamento prudente e difensivo in tutti i domini e in tutte le dimensioni.

Applicando il *framework* delle *joint actions* alla condotta delle operazioni militari è, pertanto, necessario tenere conto della relazione tra le *joint functions* (*intelligence, command and control, manoeuver, fires, Information*, CIMIC[4], *force protection e sustainment*), gli obiettivi multi-dimensionali e i domini. Le *joint functions* offrono la struttura che consente ai Comandi e alle unità di focalizzare le capacità militari nel luogo e nel momento più opportuno e di condurre efficacemente le operazioni nel *continuum of competition* (a qualsiasi livello di intensità), assicurando la protezione e sostenibilità delle forze. Il conseguimento degli effetti nelle dimensioni fisica, cognitiva e virtuale avviene attraverso la sincronizzazione e l'armonizzazione delle quattro *joint actions* che generano effetti (*manoeuver, fires, Information*, CIMIC) sotto l'azione guida della funzione Comando e Controllo.



[4] *Civil Military Cooperation*.

CAPITOLO 1
COMPLESSITÀ DELLO SCENARIO

1.1 EVOLUZIONE DEL CONTESTO

Lo scenario di riferimento è influenzato da molteplici dinamiche (*mega-trend*) di natura politica, sociale, demografica, ambientale, economica e tecnologica nonché dal manifestarsi (in taluni casi, dal riproporsi) di minacce e sfide che incideranno in modo sostanziale sugli equilibri geopolitici mondiali degli anni a venire alimentando situazioni di **instabilità pervasiva e persistente** ("*pervasive instability*")[5]. In questo contesto, connotato da fenomeni dinamici e volatili, aumentano e continueranno ad aumentare forme manifeste e latenti di competizione che coinvolgono attori statuali e non-statuali.

Il numero di *peer/ near-peer competitor* e la natura sempre più interconnessa del sistema internazionale rappresentano i principali fattori che contribuiscono ad aumentare il potenziale disordine e l'incertezza del contesto geopolitico, rendendo l'attuale sistema sempre più complesso. La presenza d'incertezza all'interno degli equilibri geostrategici, l'affermazione sulla scena internazionale di nuovi attori (statuali e non) con la risorgenza della *Great Power Competition*, la corsa continua per lo sfruttamento delle risorse energetiche e la facilità di accesso alle tecnologie emergenti moltiplicano le possibili forme di competizione internazionale nelle quali tutti gli attori cercano di proteggere i propri interessi nazionali applicando strumenti di *soft*, *hard* o *smart power*[6], tessendo una fitta rete di interazioni con gli altri attori.

Rispetto al passato in cui la pericolosità di una controparte era principalmente legata alla sua valenza politica e al potenziale militare, oggi, in un contesto incerto, instabile, ambiguo e congestionato, il peso ed il ruolo dei potenziali *competitors* è di difficile individuazione in quanto determinato dal concorso di svariati elementi, non tutti legati al quadro istituzionale politico e militare. Tra i principali fattori che contribuiscono a questo cambiamento vi sono:

[5] Stato Maggiore Difesa - Concetto Scenari Futuri 2021.

[6] L'*hard power* prevede l'impiego di strumenti di coercizione (militari ed economici) per influenzare il comportamento di altri attori, mentre il *soft power* prevede, invece, l'uso di strumenti attrattivi (diplomatici, culturali e storici). Lo *smart power* combina *hard* e *soft power*, anche attraverso l'uso strategico di diplomazia, persuasione, influenza, *capacity building* e proiezione di potere secondo un modello di legittimità sociale e politica.

– **la globalizzazione**, che agevola la creazione di *network* di varia natura (economici, religiosi, politici, lobbistici, culturali, ecc.), oggi possibile con una velocità e una capillarità un tempo inimmaginabili
– **lo sviluppo tecnologico**, inteso non solo come accesso sempre più facile ed economicamente sostenibile a sistemi di potere, incluse le armi (comprese quelle non convenzionali e/o di distruzione di massa), ma anche come disponibilità di nuove tecnologie che consentano di operare da e in ogni parte del globo, in domini e ambienti che spesso non consentono la chiara individuazione dell'aggressore (quali ad esempio le attività cibernetiche e quelle condotte nell'*information environment*).

Si assiste, pertanto, ad una contrapposizione che attraversa in modo spregiudicato l'intero spettro della competizione in cui i protagonisti principali possono essere individuati, come già citato in precedenza, tra due categorie di soggetti:

– **attori statuali,** la cui rinnovata assertività ha visto anche Paesi un tempo minori che, grazie ad economie in rapida espansione, assumono un ruolo sempre più importante anche negli equilibri globali;
– **attori non statuali**, entità non governative capaci di avere un ruolo determinante, se non paritetico, negli equilibri delle controversie internazionali, influenzando opinioni, masse e interessi economici, a volte più dei governi stessi. Nell'ambito di cornici statuali fragili, caratterizzate da istituzioni deboli, sono andati diffondendosi attori non statuali che hanno condotto e potranno rinnovare anche in futuro attività insurrezionali, terroristiche, criminali, di sabotaggio, sovversive ed anche di offesa cibernetica nei confronti degli Stati.

1.2 IL *CONTINUUM OF COMPETITION*

L'evoluzione del contesto delinea un quadro in cui il sistema di relazioni internazionali risulta caratterizzato da uno stato di competizione permanente in cui l'atteggiamento e il comportamento degli attori possono essere rappresentati secondo il modello NATO del cd. *continuum of competition* su quattro differenti livelli incrementali: partendo da Cooperazione e Rivalità, che rappresentano uno stato di pace, per arrivare al Confronto e al Conflitto Armato.

Più in dettaglio questi livelli possono essere descritti nei seguenti termini:

– **Cooperazione**: si verifica quando l'atteggiamento degli attori su una determinata questione è di allineamento e di cooperazione per raggiungere obiettivi comuni (la NATO è un esempio di cooperazione per proteggere e difendere la sicurezza delle nazioni). La cooperazione fornisce la base ideale per una stabilità duratura.
– **Rivalità**: quando due attori sono in uno stato di pace ma hanno obiettivi o visioni contrastanti. Gli attori competono con un atteggiamento o un comportamento

conforme al *Rules Based International Order* (RBIO), inteso come impegno condiviso da tutti i paesi a condurre le proprie attività in conformità con le regole concordate che evolvono nel tempo attraverso trattati multinazionali. La rivalità è lo stato normale nelle relazioni internazionali e, se ricondotta all'interno delle RBIO, può essere vantaggiosa per tutte le parti e per il sistema internazionale nel suo insieme. Esempi di rivalità includono le regole delle Nazioni Unite sui beni comuni globali (*Global commons*) o sulla libertà di navigazione.

- **Confronto**: si verifica quando gli attori sono in uno stato di crisi adottando comportamenti o atteggiamenti ostili sotto forma di minacce e violenza quale strumento di competizione per risolvere le questioni a proprio favore. Non esiste una soglia definita che separa il confronto dal conflitto armato, perché molti attori cercano intenzionalmente di oscurare o confondere questa soglia. Gli attori cercheranno consapevolmente di allungare o restringere tale soglia nel tentativo di aumentare o limitare la libertà di azione. *Proxy warfare*[7], terrorismo e la coercizione economica sono tutti esempi di attività sotto la soglia del conflitto armato. In risposta, altri Stati condurranno attività deterrenti e difensive per ridurre lo scontro oppure intensificheranno le attività per arrivare al conflitto armato.
- **Conflitto Armato**: quando l'uno o l'altro attore decidono di usare la forza militare. Poiché il conflitto armato include atti di violenza diretta, questo ha invariabilmente un effetto esponenziale sulla dimensione cognitiva[8].

I confini tra Cooperazione, Rivalità e Confronto e la soglia tra Confronto e Conflitto Armato sono complessi e dinamici con una progressione né lineare né facilmente definita. Inoltre, le relazioni interstatali sono tipicamente settoriali: gli Stati possono cooperare in un settore, confrontarsi in un altro e potenzialmente combattere un conflitto armato in un terzo.

1.3 COMPLESSITÀ E MULTIDIMENSIONALITÀ

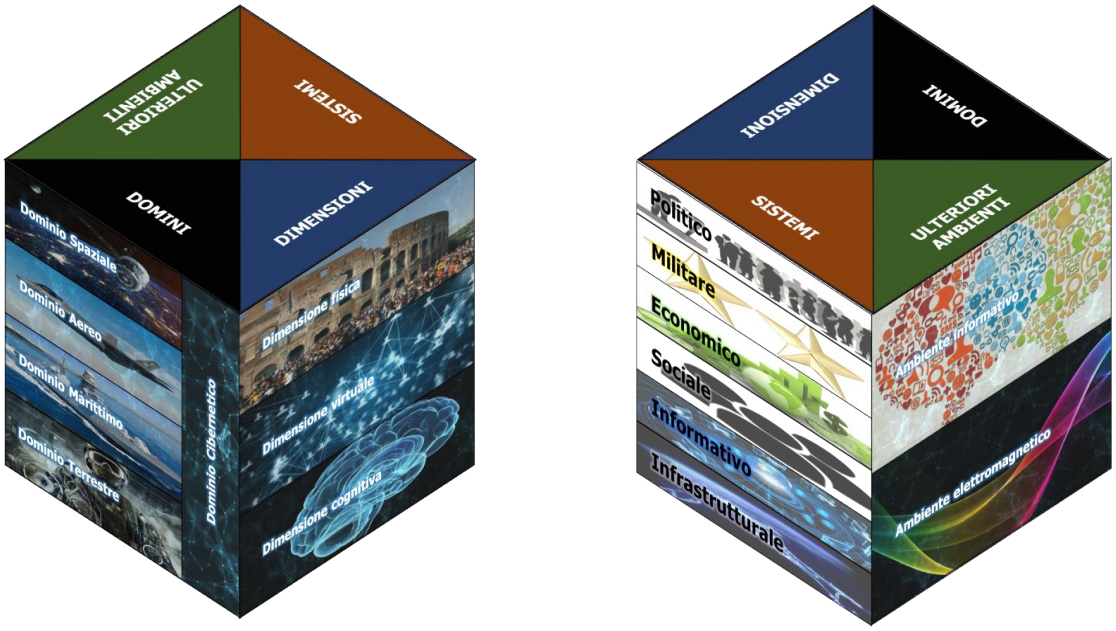
L'attuale paradigma di *jus ad bellum*[9] e *jus in bello*[10] ("*Law of War*") si ritrova profondamente incerto dinanzi alla nuova realtà della "*gray zone*" all'interno del quale si sviluppa la competizione. Inoltre, il processo di globalizzazione, correlato allo sviluppo tecnologico e alla trasversalità della connessione digitale, sta trasformando le società attraverso la creazione di un sistema di aggregazione che supera la tendenza alla separazione e ridimensiona il concetto di confine fra Nazioni, creando uno scenario in cui le interrelazioni uniscono diversi ambiti in un unico complesso sistema di sistemi in cui le singole variabili non sono indipendenti, ma si influenzano l'un l'altra creando nuove complessità. Risulta, quindi, necessario comprendere l'insieme di relazioni che

[7] Conflitto armato tra due Stati o tra attori non statali che agiscono su provocazione o per conto di altre fazioni che non sono direttamente coinvolte nelle ostilità.
[8] L'esponenzialità degli effetti di un conflitto armato sulla dimensione cognitiva è considerata talmente rilevante che la NATO ha inserito uno specifico studio sui "*Warfighting effects on cognitive dimension*" nelle *Lines of Deliveries* discendenti dal NATO *Warfighting Capstone Concept*.
[9] Insieme di norme e principi che gli Stati hanno l'obbligo di rispettare prima di poter intraprendere un conflitto armato o di prendere parte ad un conflitto già esistente.
[10] Insieme di norme e principi che si applica durante un conflitto armato.

caratterizzano la complessità dell'ambiente operativo e i rischi legati all'atteggiamento degli attori che possono tentare di manipolare il sistema a proprio vantaggio,

1.3.1 L'ambiente operativo Multidominio

Tale quadro di complessità richiede la definizione del contesto operativo di riferimento in cui esercitare l'azione degli strumenti del Potere nazionale attraverso una modellazione che metta in relazione ambienti, domini, dimensioni e sistemi. In questo senso, il nuovo contesto operativo di riferimento deve essere considerato come un elemento in continua evoluzione in cui le singole variazioni che agiscono lo modificano portandolo ad un nuovo stato, diverso da quello iniziale. Torna utile per comprendere meglio tale complessità semplificare come le diverse componenti interagiscono e si influenzano reciprocamente per mezzo di una figura tridimensionale sulle cui facce possono essere rappresentati:



- i domini delle operazioni militari (terrestre, marittimo, aereo, spaziale e cibernetico);
- le tre dimensioni degli effetti (fisica, virtuale e cognitiva);
- i sistemi Politico, Militare, Economico, Sociale, Informativo e Infrastrutturale – PMESII[11];
- gli ulteriori ambienti "informativo" ed "elettromagnetico" nei quali, in aggiunta ai cinque fondamentali su sui si fondano i domini, vengono già condotte operazioni militari e che, in prospettiva, presenteranno nuove sfide e nuove forme di minaccia.

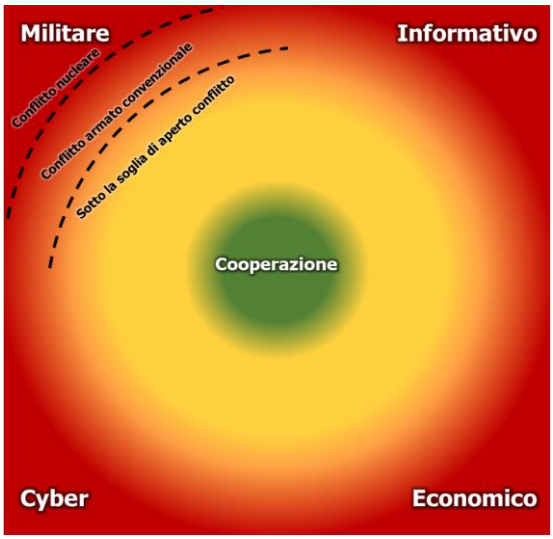
Tali elementi non sono tuttavia da considerare come fattori distinti, ma come parte di un unico "sistema di sistemi" in cui tutti gli aspetti sono legati da una serie di interrelazioni attraverso una serie di nodi collocati su differenti piani: si configura così l'ambiente operativo Multidominio.

[11] Modello di analisi che, attraverso la suddivisione in 6 elementi di sistema (Politico, Militare, Economico, Sociale, Informativo e Infrastrutturale), consente di delineare l'organizzazione politico-sociale della popolazione nell'ambiente operativo.

1.3.2 L'atteggiamento degli attori

Dalla complessità dell'ambiente operativo Multidominio deriva la possibilità, per taluni attori, di mantenere un atteggiamento ambiguo e aggressivo, adoperando tutti gli strumenti del proprio potere nazionale (Diplomatico, Informativo, Militare ed Economico – DIME), attraverso tutti i domini operativi, gli ambienti informativo ed elettromagnetico, per sfruttare le vulnerabilità avversarie nell'intero spettro PMESII e generare effetti nelle dimensioni fisica, virtuale e cognitiva con l'obiettivo di creare attrito tra popoli, nazioni, organizzazioni e minare la fiducia delle popolazioni nei loro governi, nelle istituzioni e nei loro alleati e *partner* al fine di perseguire i propri interessi, negando all'avversario la possibilità di risposta.

In tale contesto va osservato che lo sfruttamento dell'ambiente informativo rappresenta un fattore chiave e determinante per influenzare i processi decisionali dei molteplici attori presenti (per es. dall'utilizzo a proprio vantaggio delle informazioni disponibili, usandole in modo rapido e flessibile, all'acquisizione di superiorità nella raccolta, nella trattazione e nella disseminazione, finanche all'impedire, nel contempo, attività analoghe da parte di elementi o forze avversarie). Si comprende pertanto come talvolta i mezzi non militari costituiscano i principali strumenti scelti dagli aggressori per conseguire i loro obiettivi strategici. In questo caso il concetto lineare di *escalation* militare risulta non essere più valido e le attività condotte nelle varie dimensioni del confronto al di sotto della soglia di conflitto rappresentano una significativa minaccia per la sicurezza nazionale al pari delle minacce puramente militari.



Pertanto, la moderna minaccia appare **multidimensionale** e **trasversale**, capace di indebolire l'intero sistema Paese anche colpendone un singolo interesse vitale a causa della capacità di produrre effetti o conseguenze in tutte le altre dimensioni. Dalla complessità del sistema e delle relazioni che legano tra loro i singoli fattori e dalla multidimensionalità e trasversalità della minaccia, nasce quindi l'esigenza di pensare sempre più al tema della Sicurezza e Difesa in un'ottica di sistema Paese in cui tutti gli interessi sono collegati e interdipendenti (*whole of government* e *whole of society*).

1.4 LE NUOVE SFIDE DELLA COMPETIZIONE

La velocità di sviluppo e diffusione di tecnologie innovative, emergenti e dirompenti sta profondamente modificando il carattere della competizione, estendendone la portata ben oltre i confini tradizionali della dimensione fisica. In tale contesto, particolare rilevanza assumono la competizione nei nuovi domini "*Cyber*" e "Spazio" e gli effetti prodotti attraverso gli ambienti "informativo" ed "elettromagnetico".

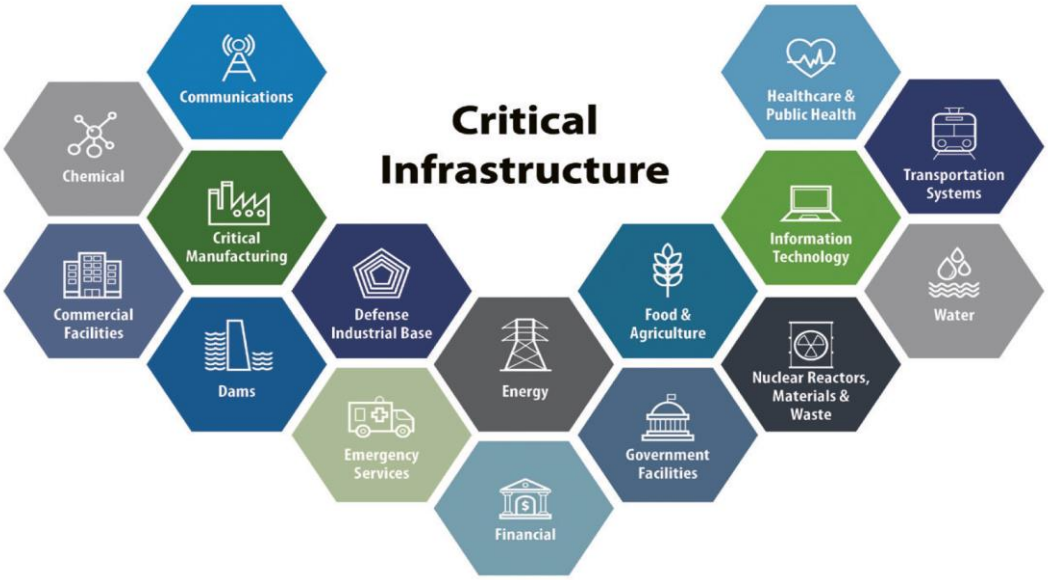
1.4.1 Il dominio *Cyber* e la dimensione virtuale

Il dominio cibernetico, caratterizzato a differenza dei domini tradizionali da una connotazione intangibile e trasversale, sta assumendo sempre maggiore rilevanza anche a livello geostrategico. Lo sviluppo e la sicurezza di una nazione dipendono sempre più dalla fruibilità d'accesso alle informazioni. Da tempo si pone chiaramente attenzione al controllo del flusso dei dati digitalizzati, inevitabilmente correlati alle tecnologie esposte ad internet, o comunque tra loro "connesse" nel senso più vasto del termine. In tale ottica, la pervasività della dimensione cibernetica determina la necessità del controllo delle reti e dei dati quale *conditio sine qua non* per assicurare servizi essenziali e più in generale la difesa di una nazione. Difatti, un uso malevolo di tali tecnologie potrebbe comportare da una parte il collasso dei sistemi e dei servizi essenziali, dall'altra mettere in luce potenzialità destabilizzanti, con effetti nella dimensione cognitiva, contribuendo al condizionamento delle opinioni pubbliche attraverso il "controllo" delle reti e dei dati.

La capacità di gestione della grande mole di dati sarà uno dei parametri fondamentali per determinare il peso di ciascun attore in ambito economico e politico, tanto che si parla di sovranità digitale ovvero della possibilità che soggetti, anche privati, siano in grado di intercettarli e renderli fruibili, riscrivendo gli equilibri geostrategici ed imponendo nuove regole ad una realtà *internet-based.*

Se ne deduce, pertanto, che la padronanza nell'impiego e nella la gestione dei dati sia alla base della superiorità militare, in quanto, agevolando la gestione delle informazioni, facilita l'esercizio del comando e controllo e la condotta di operazioni. Inoltre, l'impiego sempre più pervasivo di *software* all'interno dei sistemi d'arma, combinato con la sempre maggiore domanda di connettività e interoperabilità tra gli stessi, ha allargato il perimetro di vulnerabilità a minacce provenienti non solo dai domini tradizionali ma anche da quello *Cyber*, richiedendo nuovi approcci e ulteriori misure a protezione delle capacità operative delle Forze Armate.

Una migliore comprensione e consapevolezza dell'impatto dello sviluppo tecnologico sarà un elemento portante della capacità di protezione delle infrastrutture



critiche[12] le cui risorse, sistemi e reti, fisiche o virtuali, sono considerate così vitali che la loro distruzione o inefficienza potrebbe avere un effetto debilitante sulla sicurezza pubblica, sull'economica, sulla salute o qualsiasi combinazione di questi.
Il *Cyberspace* permette, infatti, di poter preservare l'anonimato degli attori a causa della difficoltà oggettiva di tracciare la fonte degli attacchi: grazie alla possibilità di operare attraverso falsi IP e *server* stranieri, chi attacca gode di una relativa impunità (*non attribution*). Ciò porta alla dematerializzazione, deterritorializzazione, decentralizzazione e denazionalizzazione delle relazioni, trattandosi di un dominio fluido che si modifica e si riconfigura in modo estremamente rapido, travalicando le frontiere geografiche ed espandendosi in tutto il globo. Inoltre, quello *Cyber* può considerarsi come l'unico dominio che riesce a concentrare al suo interno tutti gli strumenti del *national power*: quello diplomatico, quello militare, quello economico e quello riguardante il controllo dei media e la gestione delle informazioni. In tale contesto, per consentire al Paese di affrontare le sfide poste dall'evolversi 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.

1.4.2 Il dominio Spazio

Il forte sviluppo tecnologico ed il rinnovato interesse per l'esplorazione e lo sfruttamento dello Spazio, hanno contribuito ad espandere le possibilità di accesso allo Spazio, creando nuove opportunità e nuove sfide.

[12] Le infrastrutture critiche sono le risorse materiali, i servizi, i sistemi di tecnologia dell'informazione, le reti e i beni infrastrutturali che, se danneggiati o distrutti, causerebbero gravi ripercussioni alle funzioni cruciali della società, tra cui la catena di approvvigionamenti, la salute, la sicurezza e il benessere economico o sociale dello Stato e della popolazione.

Le tradizionali barriere finanziarie e tecnologiche nel campo satellitare sono in costante attenuazione e, grazie alla riduzione dei costi di accesso e gestione, sempre più utenti possono usufruire dei servizi spaziali. La proliferazione di applicazioni ad uso duale, sia civili che militari, ha definitivamente ampliato gli usi militari dello Spazio. Nate da esigenze di ottimizzazione delle risorse, tali applicazioni si sono rivelate una strategia vincente per ottenere un maggiore sostegno pubblico e privato all'industria spaziale, sfumando il confine tra utilizzo militare e civile. A fare da contraltare a tutto ciò, esiste un *dark side* del dominio Spazio correlato alla crescente esposizione a nuovi rischi e vulnerabilità sistemiche quali spionaggio, sabotaggio e moltiplicazione dei detriti. Pertanto, è fortemente auspicabile il pieno raggiungimento della capacità di operare in qualsiasi condizione, ivi compresa quella in cui i servizi *Space-based* possano risultare limitati o addirittura negati.

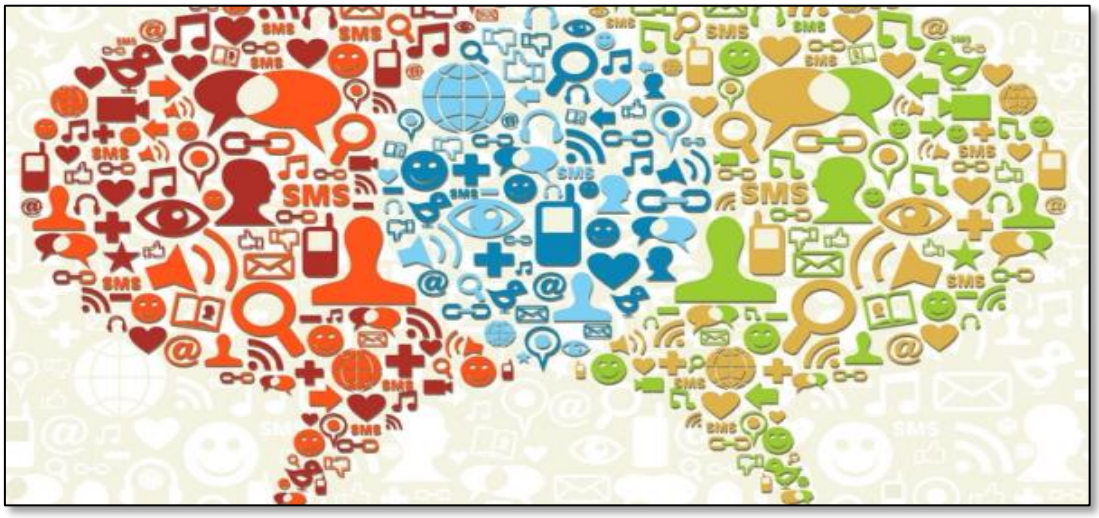
Nel *continuum of competition* l'architettura spaziale e, più nello specifico, i suoi singoli segmenti rappresenteranno sempre più un'area di confronto. In particolare, le tecnologie spaziali saranno il settore strategico, giocando un ruolo determinante in tutte le attività sia pubbliche che private di un Paese (es. contribuire alla connessione delle persone a livello globale, fornire dati essenziali in caso di disastri naturali, supportare la condotta delle operazioni militari).

Con riferimento alla condotta delle operazioni militari, dal punto di vista dei trattati internazionali vigenti, ci si limita ad identificare nella mera condotta aggressiva, piuttosto che negli usi militari in genere, la violazione della norma che prescrive usi e scopi pacifici nello Spazio, accettando tutti gli usi militari non espressamente vietati dalla lettera dell'art. IV del Trattato sullo Spazio e coerenti con i principi contenuti nella Carta delle Nazioni Unite. Si tratta di un approccio originale, fondato sull'idea che vi sia un *continuum* tra pace e aggressione, e che la questione critica riguardi la quantità di forza che può essere impiegata senza oltrepassare la linea ideale che separa la condotta pacifica da quella propriamente aggressiva e, dunque, inaccettabile per il diritto internazionale.

Un netto distinguo va fatto, infine, tra *militarization* e *weaponization* dello Spazio. La "militarizzazione dello Spazio" si riferisce all'utilizzo di dispositivi che hanno base nello Spazio (*Space-based*) allo scopo di aumentare l'efficacia militare di forze

convenzionali ed individua gli usi militari ritenuti, attualmente, leciti. La *weaponization of space*, invece, si riferisce propriamente al posizionamento in orbita di armamenti spaziali. In definitiva, gli usi militari dello Spazio attualmente consentiti sono di carattere "passivo", mentre la *weaponization* implicherebbe un loro salto qualitativo verso usi militari "attivi" dello Spazio, intrinsecamente dotati di natura dirompente.

1.4.3 L'ambiente informativo e la dimensione cognitiva



L'ambiente informativo e la dimensione cognitiva, sebbene non definiti ufficialmente come domini delle operazioni, hanno un loro peso specifico che probabilmente tenderà ad aumentare nella condotta delle operazioni, soprattutto in un quadro geostrategico in cui il *trend* è quello di evitare il confronto cinetico ricorrendo sempre di più a forme di *warfare* indirette.

Nelle operazioni Multidominio la posizione di vantaggio che si vuole conseguire non è solamente fisica, ma è anche psicologica prendendo, di fatto, coscienza che da una situazione di dominanza militare (fortemente abilitata dalla tecnologia) si passa a una situazione di potenziale parità nel campo virtuale o, eventualmente, di soggezione. Delle differenti modalità con le quali manovrare, si è progressivamente scelto di adottare un approccio indiretto, cioè di giungere alla sconfitta dell'avversario conquistando le posizioni di vantaggio psicologico, senza necessariamente ottenere la sua distruzione. In questo quadro, l'informazione e la comunicazione hanno sempre rivestito un ruolo fondamentale negli eventi storici con evidenti riflessi sociali dovuti anche alla loro capacità di orientare l'opinione pubblica. L'evoluzione nel tempo del mezzo di comunicazione (dalla carta stampata, alla radio, alla televisione) ha profondamente modificato il mondo dell'informazione e della comunicazione, grazie alla crescente capacità di trasmettere messaggi "immediati" ad *audience* sempre più larghe. Tuttavia, l'utilizzo degli strumenti di comunicazione per fini di propaganda e contropropaganda è stato, almeno in parte, limitato dalle forme di controllo esercitate sugli strumenti di comunicazione e dal numero limitato di professionisti che operavano nel mondo dell'informazione.

La rivoluzione digitale e l'avvento dei *social media* e di tutti gli altri canali di comunicazione digitale hanno profondamente rivoluzionato il mondo

dell'informazione, soppiantando, di fatto, tutti gli strumenti precedenti e aprendo il mondo della comunicazione a una nuova schiera di attori che veicolano i loro messaggi e contribuiscono, talvolta in maniera determinante, a orientare l'opinione pubblica e ad alimentare il dibattito politico. Apparare evidente come, in un contesto come quello attuale, il Centro di Gravità[13] per l'avversario sarà il modo di pensare della popolazione sia in termini reali che virtuali. Non più "programmare" le menti, ma far scegliere "spontaneamente" un comportamento piuttosto che un altro attraverso una strategia informativa e cognitiva chiara e precisa.

La pervasività dell'ambiente informativo, con particolare riferimento alla sua dimensione digitale, necessita quindi di un approfondimento che consenta di comprendere le principali problematiche legate alla sua gestione:

- la mole di informazioni disponibili ha reso e renderà sempre più difficile per il singolo utente la possibilità di farsi una propria opinione informata. Infatti, la quantità e la tempestività, a discapito della credibilità delle informazioni verificate e/o scientificamente validate, hanno intaccato l'autorevolezza stessa dell'informazione e dei professionisti che vi operano;
- la diffusione di *fake news* che puntano a screditare personaggi, istituzioni e posizioni politiche sarà difficilmente distinguibile dalla verità. I casi relativi al periodo della Pandemia da COVID-19 dimostrano come la diffusione di notizie, più o meno verificate, non solo provochi reazioni nell'opinione pubblica, ma divenga centrale anche nel dibattito politico;
- la manipolazione dell'informazione potrebbe rappresentare un fattore strategico nelle mani di chi saprà usarlo. Da un lato, potrebbe essere utilizzato per provocare divisioni e fratture in quegli Stati a debole identità nazionale o a forte instabilità interna, aprendo la via ad iniziative di penetrazione economica e/o militare. Dall'altro, potrebbe aumentare attriti tra Stati per favorire altre potenze che si avvantaggerebbero dallo scontro innescato, oppure facilitare la disgregazione di organizzazioni multinazionali. Tale fiducia diviene il *target* delle capacità offensive informative/ cognitive dell'avversario.

Appare, quindi, evidente come la capacità di comprendere l'ambiente informativo e le dinamiche correlate diventerà sempre più un elemento di alto valore strategico. All'interno di un sistema che garantisca il controllo democratico e la massima trasparenza, risulta infatti necessario dotarsi di una capacità di monitoraggio costante e permanente, al fine di evitare, soprattutto in momenti di particolare tensione internazionale, che la manipolazione delle informazioni possa indebolire la compagine nazionale e favorire iniziative, se non militari, senz'altro di carattere finanziario ed economico che potrebbero intaccare *asset* importanti e strategici del sistema paese.

La pervasività dell'ambiente informativo e gli sviluppi tecnologici nel comparto delle neuroscienze stanno significativamente estendendo la portata della competizione

[13] La fonte primaria di potere che fornisce a un attore la sua forza, libertà di azione e/o volontà di combattere.

nella dimensione cognitiva tanto che le funzioni PSYOPS[14] ed INFO-OPS[15], pedine fondamentali del contrasto della minaccia esplicitata fino ad ora, potrebbero con il tempo evolvere ad uno stadio maggiormente integrato ed omnicomprensivo tradotto in quel concetto di *cognitive warfare*, inteso quale nuova modalità di confronto permanente che mira ad attaccare la sfera delle convinzioni e delle opinioni di una popolazione con lo scopo di destabilizzare la coesione, la sicurezza e la prosperità di una Nazione.

In particolare, il *cognitive warfare* impiega campagne di disinformazione ed immensi flussi di *fake news* potenzialmente supportati da sistemi di Intelligenza Artificiale (IA) per disarticolare un processo decisionale, indebolire la coesione interna, erodere la fiducia nelle istituzioni democratiche e generare dubbi e indecisione per perseguire un piano ideologico svuotando di significato elementi identitari della popolazione.

In tale contesto, i rapidi progressi nelle neuroscienze e nelle sue tecnologie stanno suscitando sempre maggior interesse per un potenziale uso di questi strumenti e metodi per esercitare influenza e potere sulla scena globale (*weaponization* delle neuroscienze).

L'impiego di sistemi basati su IA, sviluppati in ambienti simulati per testare la capacità di un obiettivo di rispondere ad una crisi o per validare l'efficacia di decisioni strategiche e operazioni militari in un contesto globale, potrebbe consentire al potenziale aggressore di occultare la propria identità ed agire direttamente contro un obiettivo specifico, destabilizzando l'opponente e impedendone la risposta attraverso, solo per citare qualche esempio, la sollevazione di movimenti di protesta popolare o di auto-determinazione.

In tale contesto, le democrazie occidentali risultano più esposte a questo tipo di rischio rispetto ai sistemi autoritari e, pertanto, necessitano di un approccio *whole of government* che, attraverso una stretta collaborazione tra dicasteri, dipartimenti e agenzie per il raggiungimento di obiettivi comuni, consenta di mitigare il rischio derivante da questa nuova frontiera della competizione.

1.4.4 L'ambiente elettromagnetico

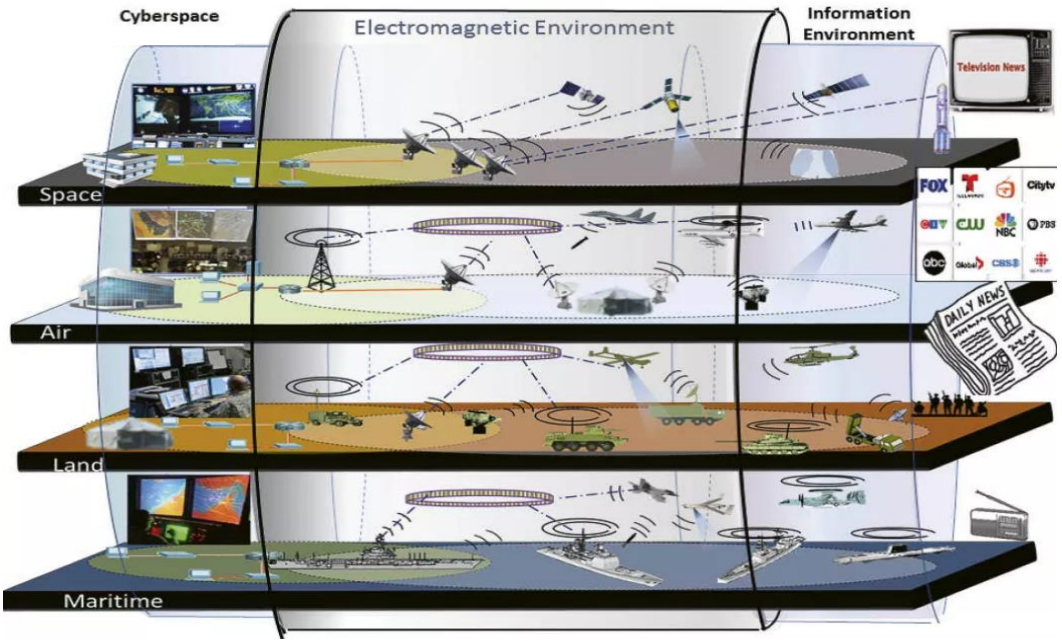
L'utilizzo militare dello spettro elettromagnetico è normalmente ricondotto alla *Electronic warfare* (EW), che include ogni azione che utilizza lo spettro elettromagnetico o l'energia diretta per controllare, alterandolo, lo spettro delle emissioni radio. La EW viene impiegata per attaccare le forze nemiche, inabilitando alcuni suoi strumenti, oppure assalirle tramite lo spettro elettromagnetico con

[14] Attività pianificate attraverso l'utilizzo di metodi di comunicazione e altri mezzi diretti per influenzare percezioni, atteggiamenti e comportamenti di un pubblico autorizzato (*target audience*), allo scopo di conseguire obiettivi politici e militari.

[15] Funzione di *staff* che ha lo scopo di analizzare, pianificare, valutare e integrare le attività informative per creare gli effetti desiderati sulla volontà, la comprensione e la capacità di avversari e pubblico, a sostegno degli obiettivi della missione.

l'obiettivo di ottenere un vantaggio (sia tattico che strategico) neutralizzando i sistemi meccanici e/o robotici avversari.

La sua trasversalità rispetto ai domini fisici rende lo spettro elettromagnetico, unitamente al dominio cibernetico e all'ambiente informativo, particolarmente



rilevante. In tal senso risulta necessario dotarsi della capacità di monitorare, disturbare ed interdire l'ambiente elettromagnetico (*Electromagnetic Environment*) a eventuali *competitors*.

Tra le principali capacità di cui è necessario disporre per poter operare nello spettro elettromagnetico con l'obiettivo di acquisirne la superiorità temporanea e sfruttare eventuali finestre di opportunità, si possono evidenziare (in modo non esaustivo) le seguenti macro-tipologie:

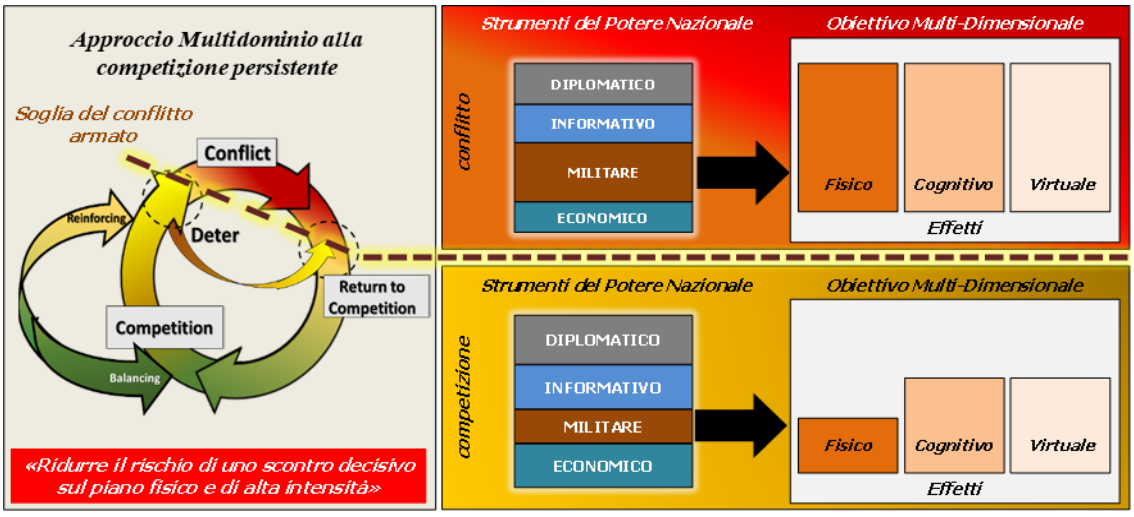
- ***signal detection***: rilevazione in un contesto elettromagnetico congestionato, caotico e conteso di uno o più segnali;
- ***signal classification***: classificazione di un segnale a seguito dell'estrazione delle principali caratteristiche tecniche;
- ***spectrum monitoring***: sorveglianza dello spettro elettromagnetico nei teatri operativi per recuperare informazioni sulla posizione dell'opponente e sulla insorgenza di possibili minacce (*spectrum awareness*).

Acquisire capacità con cui operare efficacemente consente, infatti, di disporre di un significativo valore aggiunto nel gestire la delicata fase di competizione, poiché le attività svolte nello spettro elettromagnetico potrebbero non essere identificabili come un esplicito ed intenzionale atto di guerra. Inoltre, lo spettro elettromagnetico è caratterizzato da un'estrema mutabilità nel tempo e nello spazio. Occorre quindi sviluppare competenze (in merito alla propagazione dell'onda elettromagnetica nello spazio aereo, superficiale, terrestre o subacqueo, all'interazione fra più onde elettromagnetiche e ai diversi criteri di modulazione di una portante), sensori e *tools* specifici per garantire una *situational awareness* anche nello spettro elettromagnetico e, al tempo stesso, capacità dedicate per sviluppare azioni e generare effetti, fisici e non fisici, duraturi o temporanei.

CAPITOLO 2
L'APPROCCIO NAZIONALE

2.1 DEFINIZIONE DEL PROBLEMA MILITARE

Le moderne forme di minaccia assumono rilevante criticità e carattere di particolare complessità quando perpetrate nell'ambito di un unico disegno di *Grand Strategy* in modo combinato, controllato e centralizzato da un'unica regia in grado di cogliere e gestire l'efficacia complessiva delle azioni in atto. In tale circostanza, l'attacco agli interessi vitali del Paese può infatti essere condotto da una varietà di assetti (non necessariamente sistemi d'arma) e attori (combattenti e non) mantenendo comunque lo scontro al di sotto della soglia di "aperta aggressione". L'ambiguità e la pervasività di tale forma di aggressione, unitamente alla difficoltà di individuazione dell'aggressore stesso, ostacolano il chiaro e tempestivo riconoscimento dell'attacco, specie se mosso verso obiettivi apparentemente scollegati fra loro, esponendo al rischio di una risposta tardiva o non efficace. Nasce quindi l'esigenza di analizzare come in uno scenario quale quello appena delineato, lo Strumento Militare nazionale possa contribuire efficacemente, nell'ambito di un'azione integrata e sincronizzata con gli altri strumenti del Potere nazionale (Diplomatico, Informativo, Militare ed Economico – DIME) a garantire la Difesa del Paese e degli interessi nazionali nonché il contributo alla Sicurezza internazionale, nell'ambito delle Organizzazioni Internazionali di riferimento. Il *continuum of competition* richiede una sinergia ad assetto variabile tra i suddetti strumenti, in uno sforzo condiviso e bilanciato per ridurre il rischio di uno scontro di tipo cinetico, inteso come *extrema ratio*. Lo Strumento Militare deve agire sempre, con peso specifico differente a seconda del momento, anche sotto soglia, così come avviene per esempio nella *Enhanced Forward Presence*[16] della NATO, dove si contribuisce a generare non solo effetti nella dimensione fisica, ma anche in quella cognitiva e virtuale.



[16] Presenza militare di forze NATO, approvata durante il vertice di Varsavia del 2016 in risposta a una maggiore assertività della Federazione Russa, con lo scopo di rassicurare i Paesi dislocati sul fianco Est dell'Alleanza e dissuadere qualsiasi atto ostile.

2.2 FATTORI DI RISCHIO

Partendo dalle maggiori linee di tendenza e dall'analisi dei potenziali avversari, si identificano alcuni principali fattori di rischio che concorrono ad aumentare la pericolosità della minaccia in chiave Multidominio:

- **Asimmetria strategica**: lo sviluppo di nuove tecnologie e il moltiplicarsi di quelle a carattere dirompente (*Emerging & Disruptive Technologies* - EDT), di sempre più facile accesso da parte di attori statuali e non statuali, generano un impatto diretto con effetti sul lungo periodo su ogni dimensione della competizione scatenando accelerazioni inaspettate, imprevedibili e complesse da gestire, controllare e prevedere. La spregiudicatezza nella scelta di mezzi, metodi e strategie per conseguire, incontrastati, i propri interessi strategici può costituire un elemento di significativo vantaggio strategico per taluni attori internazionali, caratterizzati da sistemi valoriali concorrenti al nostro e meno vincolati al rispetto delle regole.
- ***Lawfare***: l'impiego di innovazioni tecnologiche avanzate può incrementare la vulnerabilità ad una possibile applicazione asimmetrica della legge – *wars on law/wars through law* - nell'ambito più ampio della minaccia multidimensionale. Infatti, la carenza di norme o la loro inadeguatezza in alcuni settori potrebbe esporre alcuni Paesi, principalmente le democrazie occidentali, ad un rispetto del quadro regolamentare non favorevole alla stessa innovazione tecnologica, promuovendo una sostanziale manipolazione del diritto internazionale, una distorsione negli usi della giustizia all'interno di diversi Paesi. Per prevenire tali vuoti normativi, che possano essere sfruttati come strumento di *hybrid threats*, è essenziale anticipare il fenomeno regolamentando, con finalità operative, l'impiego delle innovazioni tecnologiche. Tale evidenza di *Lawfare* si manifesta palesemente proiettandosi nei nuovi domini *Cyber* e Spazio, campi dalla connotazione marcatamente tecnologica, ove gli sviluppi dell'Intelligenza Artificiale potranno portare effetti dirompenti.
- **Forme accentrate di potere**: la capacità di taluni attori internazionali di impiegare tutti gli strumenti del proprio potere nazionale nell'ambito di un unico disegno di *Grand Strategy* può costituire un significativo fattore di rischio. In tal senso, la capacità di assumere decisioni anche impopolari in tempi rapidissimi, permette a tali forme di potere di rispondere tempestivamente all'insorgere di situazioni di crisi che richiedono un approccio *whole of government*. In tal senso, la citata evoluzione del c.d. *cognitive warfare* apre nuove frontiere etico-legali nella competizione che richiedono, sin da subito, soluzioni comuni e condivise nell'ambito di un approccio nazionale integrato.

2.3 FATTORI DI CONTRASTO

L'effetto combinato dello sviluppo delle nuove tecnologie, dell'interdipendenza dei sistemi moderni e dell'utilizzo innovativo di nuove modalità di aggressione e conflitto, creano scenari in cui la capacità di gestione della competizione internazionale e delle possibili forme di aggressione travalica i convenzionali confini per assumere una dimensione a tutto campo e che necessita di risposte complesse. Ne consegue che la protezione del Paese passa attraverso una continuità d'azione tra la Sicurezza e la Difesa

con quest'ultima che ha assunto un significato più ampio, estendendosi dal solo campo militare a tutti gli altri interessi e necessità vitali dei cittadini, inserita in un sistema sinergico che preveda la partecipazione, ciascuno per il proprio settore di competenza, di tutti gli attori che contribuiscono a formare l'insieme del sistema stesso.

In tale contesto generale, al fine di mitigare i potenziali rischi e gli effetti di un'*escalation* della competizione, si riconoscono alcuni fattori utili a contrastare l'instaurarsi di situazioni di crisi:

- **Comprensione della complessità:** la complessità del sistema nella sua globalità e la forte interdipendenza dei singoli elementi che lo costituiscono richiedono la necessità di rilevare le singole variazioni che agiscono sul sistema, attraverso la definizione di specifici indicatori, e l'esigenza di correlarle ai possibili effetti generati sulle altre variabili. In tal senso, occorre innanzitutto comprendere la necessità di superare il modello binario di pace e guerra e considerare come le moderne forme di minaccia possano essere portate attraverso l'impiego prevalente di mezzi non-militari.

  Occorre agire in maniera integrata, a tutti i livelli, per sviluppare la capacità di comprendere la complessità del sistema nel suo insieme anziché come sommatoria degli elementi che lo costituiscono.

  La capacità di osservare e comprendere le connessioni attraverso l'uso di *tools* (militari e non), nel tempo diventa cruciale al fine di riconoscere le modalità attraverso le quali attività ostili minacciano gli interessi nazionali.
- **Deterrenza multidimensionale:** intesa quale capacità di dissuadere i possibili *competitors* dall'avviare o continuare la propria aggressione, la funzione di deterrenza risulta determinante per garantire la mitigazione dei possibili rischi derivanti dalla complessità dello scenario globale. Capacità e credibilità sono i fattori principali che conferiscono piena efficacia alla deterrenza.

  La capacità è legata alla disponibilità di strumenti e procedure idonee a interrompere un'azione aggressiva e rispondere all'aggressione stessa, in qualunque contesto (inclusi i domini *Cyber* e Spazio e l'ambiente informativo) essa venga perpetrata. La credibilità è, invece, legata alla effettiva capacità e volontà di rispondere ad un'aggressione e allo sviluppo di una narrativa strategica coerente ed efficace attraverso l'uso dei differenti strumenti del Potere nazionale. In tale prospettiva, anche le azioni atte a mantenere la capacità di agire in modo indipendente, attraverso la resilienza cooperativa (*Collaborative Resilience*)[17] quale *first line of defence*, possono contribuire a conseguire un effetto deterrente.
- **Agilità decisionale:** la complessità e la volatilità della minaccia e l'evoluzione rapidissima della situazione comportano una significativa compressione dei tempi decisionali, esigendo di disporre di strumenti e procedure che garantiscano, a tutti i livelli, un'agilità decisionale che, nell'ambito di una strategia complessiva, permetta l'assunzione di decisioni rapide e attagliate alla continua evoluzione della situazione.

[17] Resilienza delle Organizzazioni internazionali, da valutare attraverso il riconoscimento e la quantificazione della dipendenza delle forze militari da servizi e infrastrutture critiche nazionali e di come eventuali criticità e/o inefficienze possano influenzare la condotta di operazioni militari.

2.4 L'ATTUALE ORGANIZZAZIONE NAZIONALE

L'organizzazione nazionale è caratterizzata da una rigida separazione delle competenze tra i vari dicasteri e, in tale contesto, gli strumenti del Potere nazionale (Diplomatico, Informativo, Militare ed Economico) sono principalmente riconducibili ai rispettivi dicasteri dell'esecutivo, che contribuiscono, nelle aree funzionali di competenza, all'attuazione della Strategia Nazionale di Sicurezza. A tale sforzo si aggiungono poi altri attori della cosiddetta "società civile", cioè le organizzazioni nazionali e internazionali che non fanno capo direttamente alle Autorità Politiche e che sono coinvolte in maniera graduale in funzione della situazione specifica. Eventuali tematiche di interesse trasversale a più dicasteri, vengono trattate nell'ambito di specifici comitati interministeriali.

L'elemento di convergenza dell'organizzazione politico-strategica nazionale è rappresentato dalla Presidenza del Consiglio dei Ministri a cui l'impianto normativo italiano attribuisce la responsabilità di Autorità Nazionale per la Sicurezza.

Inoltre, per la gestione di possibili situazioni di crisi, l'Italia si è dotata di una specifica organizzazione[18] che opera, a seguito di determinazione del Presidente del Consiglio dei Ministri, in ogni situazione che richieda l'assunzione di decisioni governative nazionali, coordinate in sede interministeriale, quando il coordinamento non possa essere effettuato attraverso i consessi interministeriali esistenti. Al riguardo, presso la Presidenza del Consiglio dei Ministri vengono istituiti:

- il "**Comitato Politico Strategico**" (CoPS), per l'indirizzo e la guida strategica nazionale nelle situazioni di crisi. Il CoPS valuta gli elementi di situazione, esamina e definisce i provvedimenti da sottoporre all'approvazione del Consiglio dei Ministri e, quando necessario, autorizza in via temporanea l'adozione delle misure di contrasto nel rispetto degli indirizzi generali governativi e dei trattati ed accordi internazionali;
- il "**Nucleo Interministeriale Situazione e Pianificazione**" (NISP), nelle situazioni di crisi, o in quelle che appaiono suscettibili di divenire tali, formula una o più ipotesi di "posizione nazionale" da assumere nell'ambito delle organizzazioni internazionali, in ordine alle misure di contrasto proponibili/proposte da altri Paesi, per le decisioni del Presidente del Consiglio dei Ministri o del CoPS. Si avvale, inoltre, del supporto della Commissione Interministeriale Tecnica di Difesa Civile (CITDC)[19].

Il sistema di Sicurezza e Difesa nazionale sopra delineato mira ad amplificarne gli effetti combinando efficacemente gli strumenti di potere coercitivo (*hard power*) e quelli c.d. "attrattivi" (*soft power*). Tuttavia, il modello italiano è di natura eminentemente "coordinamentale" tra distinti apparati pubblici, dove un'autorità individuata, di norma per legge o, nel caso contingente, per mezzo di provvedimenti straordinari, assicura la necessaria sinergia tra le amministrazioni.

Il concetto di sicurezza nazionale è, quindi, essenzialmente incentrato sulla cooperazione e la condivisione delle risorse di attori istituzionali, cui si aggiungono, qualora

[18] DPCM 5 maggio 2010 Organizzazione nazionale per la gestione di crisi.

[19] La CITDC ha il compito di attuare le decisioni e le misure assunte dal CoPS e fornire supporto al NISP nonché di coordinare le attività di tutti i soggetti coinvolti in materia di Difesa Civile. La composizione ed i compiti sono indicati nel decreto 28 settembre 2001 del Ministro dell'Interno.

necessario, anche componenti del mondo privato (industriale, accademico e della ricerca). Tale cooperazione presuppone, tuttavia, un articolato processo di collaborazione in considerazione dell'eterogeneità organizzativa, metodologica e di funzionamento dei soggetti coinvolti. Le differenze sussistono non solo tra pubblico e privato, per via di comprensibili differenze di approccio e di linguaggio, ma anche tra soggetti diversi della Pubblica Amministrazione ove le modalità di funzionamento delle istituzioni civili sono per alcuni aspetti molto diverse da quelle delle Forze Armate e di altri Corpi similmente organizzati.

Pertanto, rispetto alla complessità dello scenario e alla pervasività delle variabili in gioco, l'attuale organizzazione presenta alcune potenziali aree di vulnerabilità di cui tenere conto tra le quali:

- i tempi e le modalità di attivazione dell'organizzazione nazionale per la gestione di crisi;
- l'ambito di applicazione "ristretto" alla sola gestione delle situazioni di crisi:
- la carenza di una capacità previsionale;
- il ruolo di limitato coordinamento tra distinti apparati e le difficoltà di cooperazione tra soggetti diversi che non dispongono di metodologie e processi comuni.

2.5 L'IDEA DI UN APPROCCIO NAZIONALE INTEGRATO

Rispetto al periodo della contrapposizione bipolare, in cui l'Italia poteva godere di rendite di posizione in virtù dell'appartenenza all'Alleanza Atlantica, la fluidità del quadro internazionale evidenzia l'esigenza di valutare attentamente la rimodulazione di assetti e procedure a tutela dei suoi interessi e della sua sicurezza. La dinamicità e la fluidità dei fattori di rischio sono causa di una maggiore complessità, a cui si associa specularmente una minore prevedibilità. La distinzione tra la sicurezza interna e quella esterna tende a scomparire, e con essa anche i confini tra politica estera, di difesa e di sicurezza con la politica estera che si è sempre più intersecata alla politica interna con la crescente interdipendenza economica e la comunicazione globale in tempo reale.

Lo Strumento Militare e quello Diplomatico non possono più, in tale contesto, limitarsi ad un mero ruolo difensivo e statico, dovendo agire dinamicamente in un mondo complesso e imprevedibile.

In particolare, il concetto di Sicurezza nazionale è profondamente mutato ampliandosi da una sicurezza quasi esclusivamente militare e "Stato-centrica" a cui è ormai subentrata una sicurezza multidimensionale e non più connessa a sorgenti di rischio o minaccia riconducibili solamente ad attori statuali. Tuttavia, come evidenziato dalla crisi innescata dalla pandemia da COVID-19, la compressione dei tempi decisionali ha messo il Governo di fronte alla necessità di scongiurare, in piena fase emergenziale, una frammentazione, anche decisionale, nella considerazione che nel nostro ordinamento è assente uno strumento formale di coordinamento centrale permanente.

In virtù delle sfide che si profilano nell'arena internazionale, un adeguamento dell'architettura istituzionale di vertice in materia di sicurezza nazionale appare auspicabile. Ciò deve avvenire parallelamente ad una riforma delle strutture e delle procedure al fine di assicurare coerenza ed efficienza all'azione governativa, agilità

decisionale, flessibilità e capacità di adattamento ai mutamenti, anche repentini, nell'ambito di scenari di sicurezza caratterizzati da un elevatissimo livello di volatilità.
Nelle organizzazioni statuali prevale la visione analitica settorializzata, non sintetizzata da una procedura sistemica. Ciò vale per il comparto della Difesa, per quello Diplomatico e per gli altri, laddove si osservano determinate tipologie di rischio e minaccia, trascurandone altre. Individuare primariamente minacce di tipo militare, ad esempio, rischia di non tenere in adeguato conto altre minacce indirette o ibride, oltre che di non programmare la tempestiva reazione ad una sorpresa. La varietà delle minacce, in particolare di quelle indirette, tende ad eccedere quella delle soluzioni di controllo reattivo o preventivo.
Risultando carente una capacità di sintesi strategica, le priorità stesse e gli interventi tendono, quindi, ad essere valutati senza una visione del quadro complessivo sia dei possibili problemi, sia delle soluzioni, con il rischio concreto di aprire spazi di vulnerabilità, anche di media o alta intensità, per le società e le rispettive organizzazioni statuali democratiche.
Con l'obiettivo di potenziare la capacità di rispondere ad un quadro sempre più complesso e imprevedibile, diverse democrazie hanno creato un organismo sul modello del *National Security Council* statunitense, istituito nel lontano 1947 contestualmente alla *Central Intelligence Agency* (CIA). Mutando, quindi, la scelta strategica di diversi Paesi che si sono dotati di un Consiglio di Sicurezza Nazionale (Francia, Gran Bretagna, Israele, Canada, Australia, Brasile, Romania e Sud Africa) appare possibile ipotizzare l'istituzione di un organismo similare anche per l'Italia. Esso costituirebbe innanzitutto un foro interministeriale permanente nel quale il Presidente del Consiglio dei Ministri e i titolari dei dicasteri più direttamente responsabili di ambiti specifici connessi con la sicurezza nazionale possano discutere e pianificare gli indirizzi strategici delle politiche estera, di difesa e di sicurezza, dedicando la necessaria attenzione soprattutto alla predisposizione di strategie a medio e lungo termine volte alla tutela degli interessi nazionali. Tale organismo garantirebbe anche un elevato livello di coordinamento e integrazione tra tutti i ministeri e dipartimenti preposti alla gestione della Sicurezza nazionale.
L'introduzione nel sistema politico-istituzionale italiano di un tale organismo consentirebbe inoltre il superamento di possibili disfunzioni tali da mettere a repentaglio l'efficacia dei processi decisionali in una materia sensibile come la Sicurezza nazionale. Nel novero di queste criticità vi sono: la difficoltà di coordinamento tra i diversi dicasteri e dipartimenti responsabili della gestione dei vari aspetti della sicurezza nazionale, che genera talvolta politiche contraddittorie; la tendenza a far fronte a problemi immediati tramite reazioni di breve termine, spesso non adeguatamente meditate, anziché ad elaborare politiche strategiche di più lungo respiro; infine, l'eccessiva influenza che la dialettica politica interna talvolta esercita sulle scelte di politica estera, di difesa e di sicurezza.
Questa struttura potrebbe essere considerata quale naturale evoluzione dell'attuale Comitato Politico Strategico presso la Presidenza del Consiglio dei Ministri, supportata da uno *staff* permanente di analisi, consulenza e pianificazione strategica, di cui

dovrebbero far parte qualificati specialisti in diversi campi, provenienti anche dal mondo accademico e della ricerca scientifica oltre che dal settore privato.
Le procedure e le tecnologie di analisi, previsione e simulazione dovrebbero essere esse stesse considerate uno strumento di sicurezza e un fattore competitivo, ragioni per cui queste dovranno collocarsi in perimetri dedicati. Tra tali procedure e tecnologie sarebbe necessario disporre di un sistema avanzato di previsione strategica, un processo per la raccolta e la condivisione - tra la pubblica amministrazione, le imprese e il mondo accademico e della ricerca - della "conoscenza" necessaria per garantire al governo le necessarie capacità di cogliere ogni segnale riguardo a possibili sorprese strategiche, ossia eventi inaspettati o altrimenti non prevedibili che possono avere un impatto sulla sicurezza nazionale (*risk assessment*).

2.6 STRATEGIA NAZIONALE DI SICUREZZA E RUOLO DELLA DIFESA

L'evoluzione della minaccia esige un nuovo modello di riferimento, in cui lo strumento Militare si collochi all'interno di una Strategia Nazionale di Sicurezza, che identifichi le priorità strategiche per il Paese.
Tale lavoro non può prescindere dall'essere condotto in un tavolo fra gli strumenti del Potere nazionale (Diplomatico, Informativo, Militare ed Economico – DIME) e comunque inclusivo di tutti coloro che siano indispensabili per definire gli elementi essenziali e qualsiasi azione discendente. Tali priorità non potranno prescindere dal loro naturale legame con la definizione e categorizzazione degli interessi nazionali (gerarchizzazione e ancoraggio geografico), in modo da consentire l'identificazione degli obiettivi e quindi la corretta "caratterizzazione" dello Strumento Militare.
Tale gerarchia di impianto guiderà la trasformazione del sistema di Sicurezza e Difesa dando il giusto spunto evolutivo per adeguarsi al mutato contesto: "*lo Strumento Militare nazionale può, in tal senso, rappresentare sia un significativo amplificatore di potenza, sia una leva, fra quelle del potere nazionale (Diplomatico, Informativo, Militare ed Economico), determinante per aprire spazi di manovra utili al conseguimento di precipui interessi nazionali, nell'ambito del più ampio sistema Paese*"[20].
La definizione di una Strategia Nazionale di Sicurezza è infatti indispensabile anche per identificare quei settori di tecnologie emergenti/dirompenti sulle quali la Difesa debba investire, al fine di impegnare risorse su quelle che necessitano di essere approfondite e sulle quali non abbia già investito un altro strumento dello Stato. Senza alcun dubbio, però, lo Strumento Militare non potrà che essere tecnologicamente evoluto e Multidominio, inteso come la capacità militare di guadagnare finestre di superiorità in ogni dominio (compresi quelli nuovi - Spazio e *Cyber*). Una superiorità che non dovrà estendersi genericamente ovunque, bensì dovrà essere in grado di difendere gli interessi nazionali (vitali, strategici o persino contingenti) che la Strategia Nazionale di Sicurezza avrà deciso.

[20] Concetto Strategico del Ca.SMD – Ed. 2020, pag 15.

CAPITOLO 3
LA DIFESA NELLE OPERAZIONI MULTIDOMINIO

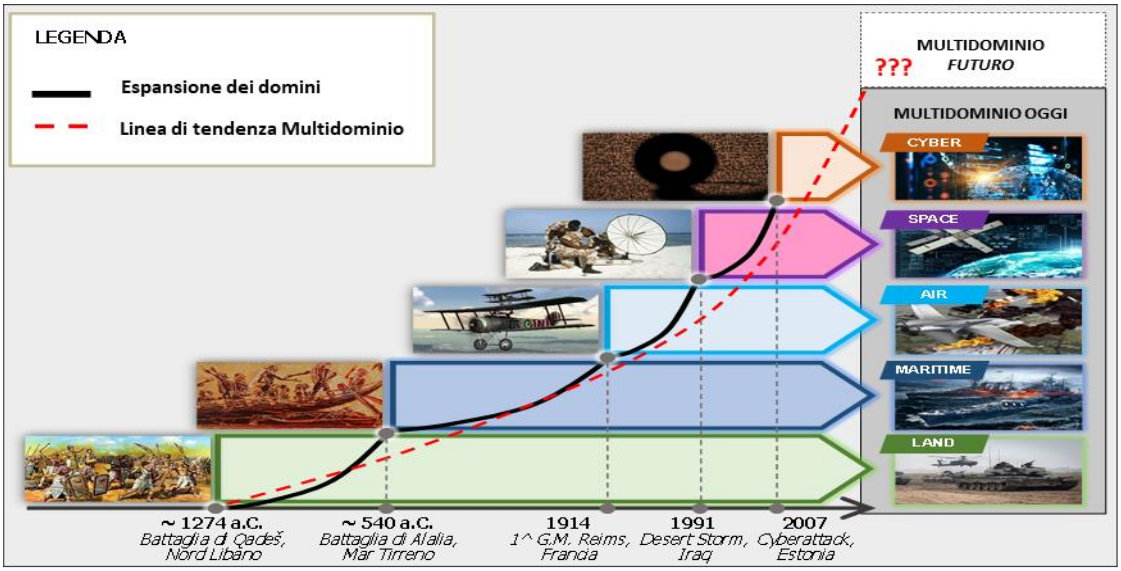
3.1 L'ORGANIZZAZIONE DELLA DIFESA NEI DOMINI

L'esigenza di sincronizzare le attività militari condotte in tutti i domini necessita preliminarmente di una valutazione dell'attuale organizzazione della Difesa per definire i possibili adattamenti che consentiranno di affrontare al meglio le future sfide nell'ambito delle operazioni Multidominio.

I domini tradizionali (terrestre, marittimo e aereo) si sono consolidati in maniera indipendente fra loro sulla base della storica contrapposizione fisica tra opponenti, tipica della guerra classica, e sono prevalentemente imperniati sulla centralità delle componenti che operano nell'ambiente di riferimento (Esercito e Arma dei Carabinieri per l'ambiente terrestre, Marina per l'ambiente marittimo e Aeronautica per l'ambiente aereo). Tuttavia, l'evoluzione tecnologica nelle operazioni militari nel tempo, unitamente alla crescente estensione degli ambienti classici, hanno di fatto influenzato anche la configurazione delle singole componenti che, in un'ottica di agilità e autonomia operativa, hanno sviluppato capacità che consentono loro di operare anche oltre i "classici" domini di riferimento.

Il confronto militare in tali domini è caratterizzato da una contrapposizione fisica con evidente manifestazione di violenza diffusa e regolato dalla *Law of War* (*ius ad bello* e *ius in bello*), universalmente riconosciuto e accettato, a cui si aggiungono alcuni principi generali nell'ambito del Diritto consuetudinario *erga omnes*.

Per la condotta delle operazioni militari nei domini classici, la Difesa aveva costituito il **Comando Operativo Interforze** (COI) che, posto alle dipendenze del Capo di Stato Maggiore della Difesa, svolgeva funzioni di pianificazione e di direzione delle operazioni nonché delle esercitazioni interforze e multinazionali, assicurando le necessarie forme di collegamento con i Comandi operativi di componente delle Forze Armate, attraverso la definizione delle competenze e responsabilità in un'ottica *supporting-supported*.



Il riconoscimento dei nuovi domini, il *Cyber* prima e lo Spazio poi, è invece avvenuto in tempi molto più recenti ed è stato caratterizzato da un elevato rateo di sviluppo tecnologico, da una pervasività e trasversalità degli effetti generabili, dalla presenza di un numero crescente di attori statuali e non statuali (pubblici e privati) che possono conseguire effetti strategici senza alcuna evidente manifestazione di violenza o essere identificati

L'assenza, ad oggi, di un quadro giuridico internazionale riconosciuto e la differente postura dei *competitors* nell'arena internazionale nei nuovi domini hanno evidenziato l'esigenza di ripensare il modo di affrontare il confronto nella dimensione militare e di sviluppare nuove capacità e metodologie per rispondere alle nuove sfide.

In questa prospettiva, tracciando una linea di tendenza dell'evoluzione storica e tecnologica dei domini, è verosimile ipotizzare che, anche in futuro, l'introduzione di ulteriori innovazioni tecnologiche, anche dirompenti, e l'utilizzo innovativo di capacità consolidate contribuiranno all'individuazione e alla definizione di nuovi domini delle operazioni.

Per adeguarsi al mutato contesto, la Difesa ha deciso di adattare la propria struttura attraverso la costituzione di specifici elementi di organizzazione a livello interforze, mantenendo la responsabilità dei due nuovi domini a livello centrale. In particolare:

- per il dominio cibernetico (*Cyber*): è stato inizialmente costituito il Comando Interforze Operazioni Cibernetiche (CIOC), poi confluito nel **Comando per le Operazioni in Rete (COR)**, cui risale la competenza di assicurare la condotta delle operazioni nel *Cyberspace*. Inoltre, il COR ha il compito di garantire il contrasto e la neutralizzazione di ogni possibile minaccia e/o azione avversaria cibernetica portata alle reti, ai sistemi e ai servizi della Difesa nei domini classificati e non classificati, nonché alle infrastrutture critiche della Difesa.
- per il dominio dello Spazio: in linea con l'evoluzione del dominio in ambito NATO[21] e nazionale[22], nel giugno 2020 è stato costituito il **Comando delle Operazioni Spaziali (COS)** con l'obiettivo di potenziare la capacità nazionale di operare nello Spazio per la protezione e la difesa dell'infrastruttura spaziale nazionale e di integrare efficacemente nelle operazioni interforze la dimensione spaziale.

  Il COS costituisce l'interfaccia di riferimento per le operazioni spaziali, sia all'interno del comparto Difesa, sia in campo interministeriale e internazionale, fatte salve le competenze nello svolgimento di attività di *intelligence* tecnico-militare che risalgono allo Stato Maggiore della Difesa/Reparto Informazioni e Sicurezza (RIS).

Tuttavia, se da un lato la costituzione di specifici Comandi per le operazioni nei nuovi domini ha consentito di acquisire conoscenze e competenze specifiche, dall'altro la reale capacità di operare nel *Cyber* e nello Spazio necessita di ulteriori azioni discendenti,

---

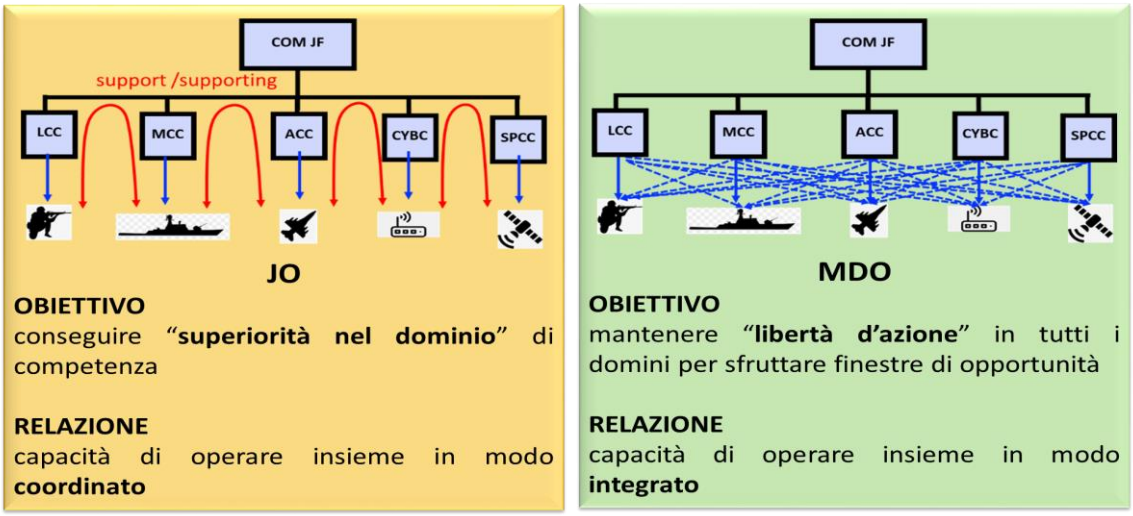
21 "*Overarching* NATO Space Policy", ed. 2019 e riconoscimento dello spazio come quinto dominio operativo.

22 A livello Nazionale, con la Legge nr.7/2018 "Misure per il coordinamento della politica spaziale e aerospaziale e disposizioni concernenti l'organizzazione e il funzionamento dell'Agenzia spaziale italiana" è stata riorganizzata la *governance* italiana sotto l'alta direzione del Presidente del Consiglio dei Ministri. Il ruolo di indirizzo e *policy* è stato attribuito al "Comitato Interministeriale per le politiche relative allo spazio e alla ricerca aerospaziale" (COMINT) nell'ambito del quale sono stati approvati nel 2019 i documenti "Indirizzi del governo in materia spaziale e aerospaziale", "Strategia Nazionale di Sicurezza per lo Spazio" e "Documento Strategico di Politica Spaziale Nazionale".

anche nella considerazione che le capacità risiedono naturalmente nelle singole Forze Armate.
In tale contesto, la necessità di operare nel contesto Multidominio ha evidenziato l'esigenza di integrare pienamente i nuovi domini nell'ambito della condotta delle operazioni militari attraverso la sincronizzazione delle azioni e degli effetti generabili.
Pertanto, per le evoluzioni in atto nell'attuale scenario geo-strategico, la Difesa, attese le attribuzioni del Capo di Stato Maggiore della Difesa (Ca.SMD)[23], necessita di una trasformazione sempre più in chiave Interforze e Multidominio, che trova espressione nell'evoluzione del COI e nella costituzione del **Comando Operativo di Vertice Interforze (COVI),** struttura volta a condurre, a livello interforze e/o multinazionale, campagne militari complesse e Multidominio in tutto lo spettro delle operazioni, garantendo unicità di Comando.

3.2 LE OPERAZIONI MULTIDOMINIO (MDO)

Inquadrare le MDO e comprenderne la reale portata in termini di esigenze di trasformazione richiede innanzitutto la necessità di comprendere il cambio di paradigma che le contraddistingue rispetto alle tradizionali operazioni *joint*. Queste ultime si basano sull'esigenza di conseguire la superiorità nel dominio di competenza, attraverso la capacità delle singole componenti di operare in maniera coordinata. Pertanto, pur mirando a un certo grado di interoperabilità, affida alle singole componenti la condotta delle attività nel proprio ambiente di riferimento, prevedendo una chiara demarcazione tra i domini, generalmente considerati contigui tra loro.



Le MDO fondano, invece, la propria essenza sulla presa di consapevolezza che non è possibile mantenere la supremazia in tutti i domini rispetto ad un *peer competitor*. Pertanto, il loro obiettivo è quello di mantenere la libertà d'azione in tutti i domini per poter sfruttare le eventuali finestre di opportunità attraverso la convergenza degli effetti da conseguire mediante la sincronizzazione delle azioni *cross-domain*. In particolare, qualora necessario, si può ipotizzare anche lo sviluppo di azioni autonome da parte di

[23] Ai sensi dell'art. 26 del d.lgs. 15 marzo 2010, n. 66 - Codice dell'Ordinamento Militare C.O.M.

una singola componente, limitata nel tempo e nello spazio, al fine di realizzare una finestra di opportunità a vantaggio delle altre componenti.
L'approccio Multidominio rielabora quindi in modo innovativo le operazioni in domini multipli per creare effetti attraverso la combinazione simultanea di diverse capacità, muovendo dall'assunto che il contesto di riferimento deve essere inteso come *un unicum*.
Ciò in ragione del fatto che:

- ogni dominio ha caratteristiche uniche che influenzano le forze, le capacità, il personale e i sistemi d'arma che in esso operano. In particolare, i tre domini classici (terrestre, marittimo e aereo) sono di fatto ampiamente associati alle singole componenti, aspetto che ha portato, nel tempo, al consolidarsi di una separazione concettuale che di fatto rischia di non agevolare la condotta delle MDO;
- esiste una relazione trasversale tra *Cyber,* Spazio e gli altri domini/ambienti, in quanto:
  - lo Spazio rappresenta un dominio in cui vengono sviluppate attività discrete che hanno una costante relazione con gli altri domini fisici. Tra queste, quelle di *space control* hanno una valenza strategica e comportano un'alta posta in gioco in termini di deterrenza;
  - le attività nel/attraverso il dominio *Cyber* e l'ambiente elettromagnetico, tese ad assicurare un vantaggio operativo inibendo e/o degradando l'utilizzo dello spettro elettromagnetico e del *Cyber*spazio all'avversario, risultano abilitanti e trasversali agli altri domini in ragione della diffusione della tecnologia digitale e della difficoltà di rilevazione delle minacce;
  - l'ambiente informativo, inteso come il luogo dove l'informazione viene ricevuta, trasformata, elaborata e trasmessa, è caratterizzato da grande complessità e dinamicità, in quanto si estende oltre i confini fisici dell'area di crisi/conflitto ed interessa tutti gli elementi nazionali e transnazionali in grado di produrre effetti nello spettro PMESII.
- il crescente impegno anche in aree sempre più contese (quali, ad esempio le aree densamente urbanizzate e, in prospettiva, le c.d. *coastal megacities*) in cui le azioni militari, ai vari livelli, devono poter influenzare[24] ambiente operativo e attori presenti. In tali contesti, infatti, tutti i fattori che contribuiscono ad accrescere la complessità dell'ambiente operativo sono compressi in un'area geografica limitata e caratterizzata dall'altissima presenza di civili. Pertanto, gli effetti nella dimensione fisica (quali la distruzione causata dal combattimento classico) possono avere effetti esponenziali sulla dimensione cognitiva.

Tracciati gli elementi essenziali delle MDO, si ritiene necessario inquadrarle, a livello concettuale, e definirne le principali caratteristiche e gli elementi di novità.

3.2.1 Inquadramento concettuale

A livello NATO ad oggi non esiste una definizione condivisa di *Multi-Domain Operations* anche se l'*Allied Command for Transformation* (ACT) ha ricevuto il compito di sviluppare il tema nell'ambito dei *Warfare Development Imperatives*

[24] Intesa come la capacità di condizionare direttamente la volontà dell'avversario (o potenziale avversario), al fine di modificarne il "comportamento" nel modo desiderato, a ogni livello di gestione delle operazioni (tattico, operativo e strategico) ovvero supportandosi reciprocamente, in relazione agli effetti che si vogliono ottenere.

discendenti dal NATO *Warfighting Capstone Concept*, prevedendo l'elaborazione di un *initial MDO Concept* entro il 2022. L'attuale bozza di definizione[25] sinteticamente descrive le MDO come:

> ***Orchestrate and synchronize military and non-military activities across all domains and environment that enable Commanders to deliver converging effects***

In un'ottica nazionale tale definizione può essere ampliata ed arricchita nei seguenti termini:

> ***Attività militari condotte anche in più domini per percepire, comprendere e, successivamente, orchestrare effetti convergenti finalizzati a generare dilemmi multipli ad una velocità tale da superare la capacità decisionale avversaria. La condotta di tali attività avviene attraverso la sincronizzazione delle azioni militari con gli altri strumenti del Potere nazionale e/o con alleati e partner, sotto una struttura di comando e controllo sincronizzata (Multi-Domain Command & Control - MDC2).***

Pertanto, in aderenza alle linee di indirizzo strategiche e alle determinazioni del livello politico sia nazionale che NATO, le operazioni Multidominio possono essere condotte nell'intero spettro della competizione e in tutte le fasi della campagna. L'approccio multidominio deve essere costantemente mantenuto nella considerazione che la competizione (*continuum of competition*) è una costante e fluida alternanza di fasi che, in misura e tempi diversi, passa dal confronto al conflitto attraverso le crisi. In tale contesto, tenuto conto dell'intangibilità del concetto stesso di soglia al di fuori della dimensione fisica classica, sarà necessario contribuire alla promozione di una regolamentazione internazionale dei nuovi domini e sviluppare, al contempo, capacità, procedure e metodologie idonee all'impiego delle potenzialità dei nuovi domini.

3.2.2 Percepire, Comprendere e Orchestrare

Il ciclo decisionale delle operazioni militari noto come *Observe*, *Orient*, *Decide* e *Act* (OODA *loop*) nelle MDO viene integrato dalle funzioni "Percepire", "Comprendere" e "Orchestrare", quale estensione dello stesso al di fuori del solo contesto militare per includere aspetti prevalentemente non militari attraverso il coinvolgimento di altri attori nazionali e internazionali, pubblici e privati. In tal senso, la portata del cambiamento richiede necessariamente una revisione del bilanciamento tra le funzioni, nella considerazione che la superiorità, rispetto ad un potenziale *competitor*, può essere raggiunta attraverso la capacità di percepire e comprendere meglio l'avversario per mantenere una certa libertà di manovra. Infatti, attraverso una maggiore comprensione sarà possibile orchestrare effetti e creare dilemmi multipli

[25] Esiti *Alliance Warfare Development Conference* (AWDC) 2021 (7-9 dicembre 2021), concepita quale evento annuale organizzato dalla NATO - *Allied Command Transformation* (ACT) che ogni anno riunisce i *Flag Officer General Officer* (FOGO) e *Decision Makers* responsabili della Trasformazione dei Paesi NATO e *Partner*, finalizzata ad indirizzare gli sforzi futuri e alla discussione di tematiche di particolare interesse connessi con l'innovazione e la trasformazione delle FA dei Paesi NATO e *partner*.

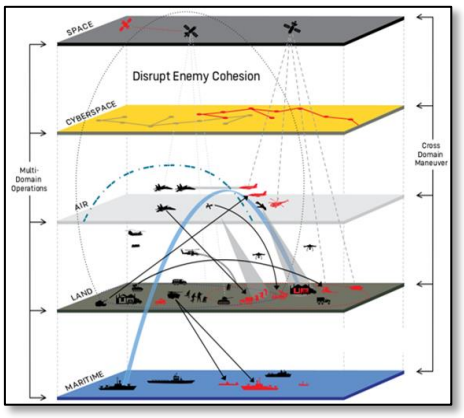
all’avversario ad un ritmo superiore a quello che lo stesso sarà in grado di affrontare e risolvere. Più nel dettaglio:

- **Percepire**, funzione propedeutica alla comprensione, nella prospettiva delle MDO viene assolta attraverso l’estensione oltre i soli sistemi di sorveglianza militare tenendo conto anche di capacità civili e commerciali (nazionali o multinazionali) così da consentire, attraverso le attività di sorveglianza, scoperta, classificazione, riconoscimento, tracciamento ed identificazione, di raccogliere dati utili per il ciclo *intelligence* e contribuire a generare comprensione. In tal senso, è richiesta la disponibilità di una vasta gamma di sensori in tutti i domini (fisici e virtuali) che coprono sia lo spettro elettromagnetico, sia l’ambiente informativo per comprendere il comportamento e l’atteggiamento di tutti gli attori in gioco.
  Inoltre, in funzione dell’evolversi della situazione e dell’andamento della competizione, disporre di sensori proattivi capaci di assolvere anche la funzione di attuatore (*every sensor is a shooter, every shooter is a sensor*) al fine di sondare e, al contempo, stimolare tempestivamente ed attivamente una risposta adeguata. In particolare, tale aspetto potrà essere conseguito attraverso l’impiego di sistemi e piattaforme automatizzati e/o autonomi.

- **Comprendere**, funzione assolta mediante l'interpretazione delle informazioni raccolte attraverso la fase percepire, ha l’obiettivo di inquadrare la situazione nel contesto di riferimento ed effettuare valutazioni (perché qualcosa è accaduto o sta accadendo) e previsioni (identificare e anticipare cosa potrebbe accadere) utili a supportare un processo decisionale rapido ed efficace.
  Nelle MDO, la comprensione deve concentrarsi sull’ambiente operativo al fine di capirne le caratteristiche, gli attori, le relazioni e prevedere come possa evolversi in relazione alle diverse interazioni. Lo sforzo dovrà concentrarsi sui potenziali avversari, su come operano nei domini, nello spettro elettromagnetico e come sfruttano l’ambiente informativo per influenzare gli attori presenti.
  In tale prospettiva, la condivisione delle conoscenze tra i diversi livelli e attori della comunità internazionale risulta imprescindibile al fine di aumentare il grado di sinergie ed orchestrare risposte adeguate valutando rischi e benefici, vulnerabilità e punti di forza per il raggiungimento degli obiettivi. Da queste valutazioni sarà possibile prevedere eventuali finestre di opportunità che permettano di competere con successo in un dominio ritenuto significativo, integrando le capacità disponibili e rimodulando il dispositivo impiegato.

- **Orchestrare**, funzione che comprende l’insieme delle attività di pianificazione ed esecuzione integrata delle azioni e delle attività per raggiungere gli obiettivi prefissati, si basa sull’efficacia continua delle funzioni percepire e comprendere e permette di condurre in modo flessibile le operazioni Multidominio tenendo conto degli effetti reali conseguiti, piuttosto che dei dati presunti o degli effetti desiderati.
  In tale contesto, la funzione orchestrare deve essere garantita da una struttura resiliente che sia in grado di garantire la propria efficienza ed efficacia anche quando l'ambiente diventa conteso e/o degradato, situazione in cui potrà risultare particolarmente complesso ottenere un'immagine chiara della situazione operativa.

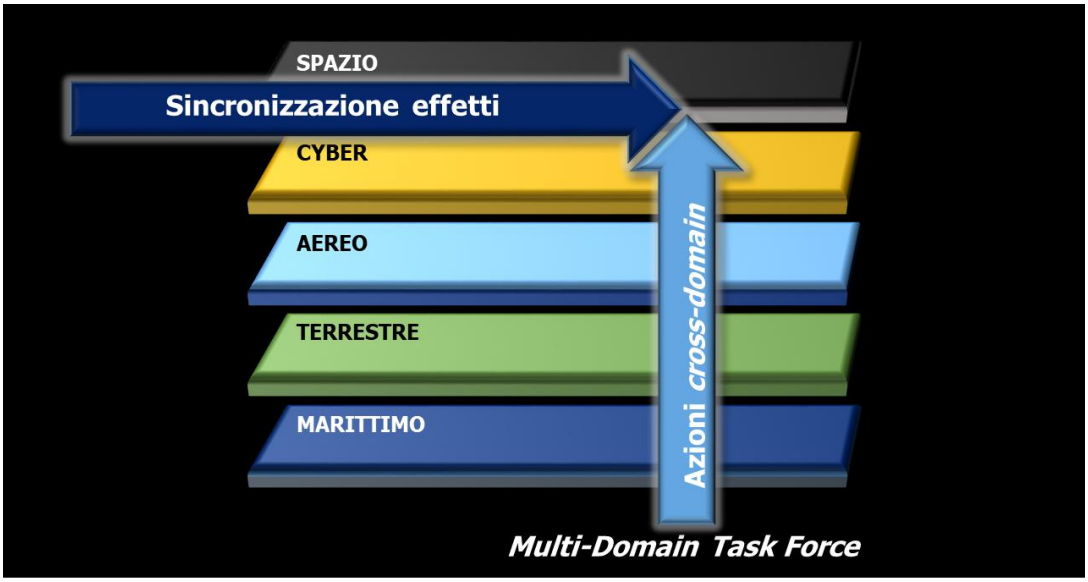
3.2.3 Le azioni *cross-domain* e la sincronizzazione degli effetti



Le azioni *cross-domain* rappresentano la combinazione integrata delle capacità (militari e non) nei diversi domini finalizzata a sfruttare una limitata finestra di superiorità e ingaggiare l'avversario nelle dimensioni fisica, cognitiva e/o virtuale.

Per garantire il raggiungimento degli obiettivi strategici, le azioni *cross-domain* presuppongono necessariamente la sincronizzazione degli effetti ai diversi livelli (strategico, operativo e tattico) e l'impiego sinergico delle capacità (cinetiche e non cinetiche) attraverso i vari domini e gli ambienti elettromagnetico e informativo. Pertanto, lo scopo delle azioni *cross-domain* è quello di creare effetti integrati nelle dimensioni fisica, virtuale e cognitiva, saturando l'avversario.

La sincronizzazione degli effetti riguarda invece l'integrazione di attività/eventi nel tempo al fine di raggiungere un *operational tempo*[26] favorevole rispetto a quanto sviluppato da un potenziale avversario. Pertanto, la sincronizzazione afferisce non solo al coordinamento delle attività militari a livello tattico, operativo e strategico, ma anche alla necessaria integrazione con le attività sottese agli altri strumenti del Potere nazionale in un dato intervallo di tempo.



In tale quadro, le azioni *cross-domain* devono quindi essere sviluppate a tutti i livelli (strategico, operativo e tattico), nell'ambito di un unico disegno strategico, da formazioni militari Multidominio per operare nel *continuum of competition*,

[26] Velocità e intensità delle azioni di una parte rispetto alla velocità e intensità degli altri eventi che avvengono nell'ambiente operativo.

modellare l'ambiente operativo, dissuadere gli avversari e – all'inasprirsi della competizione – intervenire per contrastare e/o neutralizzare la minaccia e tornare ad una situazione di vantaggio strategico.

La sincronizzazione degli effetti risale invece al livello strategico-militare che, attraverso una maggiore integrazione a livello governativo nazionale ed internazionale, possa configurare e, all'occorrenza, adeguare il disegno strategico della campagna in cui si sviluppano le operazioni *cross-domain* delle singole Forze Armate.

Pertanto, il processo di *Force Generation*[27] di una *Multi-Domain Task Force* dovrà necessariamente tenere conto della necessità di dotare le singole formazioni Multidominio di tutte le capacità necessarie ad operare in più domini e generare effetti in tutte le dimensioni. Particolare attenzione dovrà essere posta alle capacità afferenti ai domini *Cyber* e Spazio che, data la natura trasversale degli stessi e nel rispetto delle specifiche competenze di Forza Armata, dovranno essere attentamente "dosate" per:

- decentrare pacchetti di capacità alle singole formazioni Multidominio per garantire loro autonomia operativa e la possibilità di effettuare la propria azione *cross-domain*;
- accentrare le capacità strategiche, che dovranno essere mantenute sotto la direzione del COR e del COS, che ne disporranno e le impiegheranno in linea con il disegno strategico e le esigenze di sincronizzazione degli effetti.

In tal senso, occorre preliminarmente definire la catena di comando e controllo nazionale per le operazioni Multidominio (*Multi-Domain Command & Control* – MDC2) nella quale identificare le relazioni di comando e controllo e le deleghe necessarie per la condotta decentrata delle azioni *cross-domain* e la sincronizzazione degli effetti.

3.2.4 *Multi-Domain Command & Control* (MDC2)

L'estrema dinamicità e complessità con cui evolve la situazione richiede la disponibilità di dati di situazione quanto più aggiornati possibile e la capacità di velocizzare i processi decisionali per garantire la necessaria agilità e tempestività decisionale.

In tale contesto, acquista particolare rilevanza il potenziamento dell'attuale Sala Operativa del COVI, attraverso l'implementazione di una "regia" interforze (Progetto del ***Joint Operations Center* – JOC**)[28], che operi puntualmente nell'ambito di un approccio *whole of government* e che, con il ricorso a tecnologie, connettività e processi aggiornati in termini di s*ituational awareness* e di efficientamento dei processi di pianificazione e condotta, possa essere:

- il punto di convergenza di tutte le informazioni di valenza strategica, operativa e tattica provenienti dalle Aree di Operazioni in cui sono impiegati i Contingenti Militari nazionali;

---

[27] Processo di costituzione di un contingente militare attraverso la definizione delle capacità e degli assetti per la condotta di un'operazione militare. A livello multinazionale, tale processo avviene attraverso la condotta di *Force Generation Conferences* durante le quali le Nazioni offrono capacità ed assetti che si impegnano a rendere disponibili nell'ambito della coalizione.

[28] Inquadrato nell'ambito della revisione organico-funzionale del COI, c.d. *Functional Review*.

– l'elemento di raccordo con gli altri dicasteri e tutti gli attori coinvolti.

L'esigenza di un'evoluzione del COI in COVI è nata proprio dalla necessità di rafforzare in termini di unicità e rapidità la funzione operativa Comando e Controllo (C2), assicurando al Ca.SMD[29] uno strumento molto più puntuale per la pianificazione e la condotta delle operazioni in ottica *Joint*, interagenzia e/o Multidominio, anche in concorso alle Autorità Civili, nella misura in cui si ha la possibilità di disporre di una *situational awareness* aumentata relativa ai cinque domini (terrestre, marittimo, aereo, cibernetico e spaziale[30]) e all'*Information Environment* (*Multi-Domain Common Picture*).

In tal senso, il Progetto "JOC" è il perno su cui è incentrata la revisione funzionale del COVI, anche attraverso l'introduzione di nuove soluzioni tecnologiche afferenti a:

- *situational awareness* (ne è un esempio l'attuale *Joint Common Operational Picture* – JCOP[31]);
- efficientamento dei processi di pianificazione e condotta[32];
- nuove tecnologie per la gestione dei prodotti e dei documenti, e il monitoraggio di funzioni tipiche del Livello Operativo[33].

In particolare, l'evoluzione del JOC dovrà avvenire attraverso l'implementazione di prodotti già disponibili in ambito nazionale e NATO, per poi adeguarsi, con un processo su spire successive, al fine di realizzare una info-struttura che dovrà necessariamente caratterizzarsi per flessibilità e raccordo delle informazioni Multidominio e multi-livello, in linea con i più avanzati *standard* di sicurezza e in grado di dialogare con le reti NATO, UE e di Coalizione. Pertanto, le esigenze di standardizzazione dovranno assicurare:

– interoperabilità con i sistemi in dotazione alle diverse componenti della Difesa e in ambito Alleanza Atlantica, come pure alle strutture facenti capo agli altri dicasteri dello Stato, in particolare quelli di immediato riferimento per la gestione delle crisi in ambito nazionale e extra-nazionale (quindi *in primis* quelle facenti capo al Ministero dell'Interno e al Ministero degli Affari Esteri e della Cooperazione Internazionale);
– intercambiabilità dei sistemi in acquisizione o di nuova introduzione/ammodernati con quelli già nelle disponibilità delle Forze Armate.

Inoltre, in funzione dell'evolversi della situazione e dell'insorgere di eventuali situazioni di crisi o conflitto, il JOC dovrà poter assumere configurazioni differenti in funzione della situazione operativa.

---

[29] Come pure al Comandante del COI nelle funzioni di *Comandante Interforze* (COMINFOR) o *Comandante dell'Operazione Multinazionale* (COPER).

[30] Nella consapevolezza che quello *Cyber* e Spazio sono domini che richiedono necessariamente lo sviluppo e l'acquisizione di nuove capacità.

[31] Rappresentazione integrata e corrente delle operazioni in atto per tutte le componenti/domini (*Ground, Maritime, Air, Cyber, Space*), ad uso del Comandante Operativo e dei vari livelli decisionali, nonché di ciascuna delle aree funzionali (dal J1 al J9). Trattasi di informazioni associate a *layer* informativi definiti *Domain Pictures* (DPs).

[32] A titolo di esempio: strumenti *FAS (Functional Area Service), Core Services*, connettività aumentata, strumenti che consentano la valutazione e *l'assessment* (*Campaign-Operational-Tactical*) e l'esecuzione del processo di Pianificazione delle Operazioni Interforze (*Joint Operations Planning Process* – JOPP).

[33] Quali ad esempio: *Information Knowledge Management – IKM* e il cruscotto *info cloud*.

3.3 L'INTEGRAZIONE NAZIONALE NELLA GESTIONE DEI NUOVI DOMINI

La volontà di integrazione ed interoperabilità delle componenti militare/civile non è tuttavia supportata da un quadro giuridico internazionale condiviso con il conseguente rischio che alcuni *competitor* possano continuare a mantenere un atteggiamento aggressivo nei nuovi domini *Cyber* e Spazio ovvero nell'ambiente informativo, mantenendo, di proposito, la propria azione al di sotto della soglia di aperta aggressione e acquisendo una posizione di vantaggio strategico (asimmetria strategica) rispetto alle democrazie occidentali e, in particolare, al nostro Paese.

La capacità di "percepire" tempestivamente le variazioni che avvengono nel sistema e "comprendere" come queste possano essere collegate in un unico disegno di *Grand Strategy* necessita di un approccio comune e di una robusta condivisione delle informazioni sia a livello nazionale sia internazionale, con il coinvolgimento di tutti gli attori istituzionali, governativi, pubblici e privati che vi operano. Ciò consentirebbe, infatti, di svolgere anche una attenta valutazione delle vulnerabilità del sistema nazionale nel suo insieme e la possibilità di adottare le necessarie misure di mitigazione.

La crescente rilevanza della competizione nei nuovi domini *Cyber* e Spazio e negli ambienti informativo ed elettromagnetico evidenziano, infatti, potenzialità dirompenti che aprono spazi di opportunità, ma anche significativi rischi. In tal senso, occorre innanzitutto comprendere che, nonostante la costituzione del COR e del COS, lo sviluppo di capacità specifiche risiede all'interno delle singole Forze Armate e risulta ancora carente un'unicità di indirizzo strategico per lo sviluppo dei programmi e delle capacità afferenti a questi nuovi domini.

Pertanto, nella considerazione della loro rapida e crescente evoluzione (anche per la capacità intrinseca di generare effetti strategici), occorre innanzitutto comprendere che *Cyber* e Spazio assumeranno sempre più un ruolo determinante nella gestione della competizione anche militare, fino al punto di arrivare a eguagliare e, in talune occasioni, persino superare la rilevanza dei domini classici.

In tal senso, la recente approvazione del Decreto Legge 14 giugno 2021, n.82 che costituisce l'Agenzia di Cybersicurezza Nazionale (ACN) rappresenta una significativa opportunità di crescita per il sistema Paese nel dominio *Cyber*, nel quale dovranno tuttavia essere necessariamente innestate le esigenze della Difesa e il contributo dello strumento militare a tutela degli interessi nazionali. Al riguardo, diventa di primaria importanza una rivisitazione/integrazione del quadro normativo nazionale al fine di abbandonare l'attuale approccio reattivo "*Cyber Defence Centric*" verso un'efficace capacità di risposta proattiva, incentrata sull'efficacia degli Effetti Cibernetici Sovrani (SCEPVA[34]) e sulla condotta di Operazioni di Difesa Cibernetica (*Defensive Cyber Operation-DCO*) all'interno di una più ampia cornice Multidominio.

Parimenti, l'istituzione del "Comitato Interministeriale per le politiche relative allo Spazio e alla ricerca aerospaziale (COMINT)" rappresenta un importante passo avanti

[34] *Sovereign Cyber Effects Provided Voluntarily by Allies*: meccanismo dei Paesi dell'Allenza Atlantica che consente alla NATO di condurre operazioni (*offensive e defensive*) e produrre effetti nel e attraverso il dominio *Cyber* utilizzando le reti e i sistemi dell'Alleanza e/o gli altri autorizzati. – NATO AJP-3.20 "*Allied Joint Doctrine for Cyberspace Operations*".

per la crescita del sistema Paese in questo dominio. Il ruolo del COMINT deve essere infatti inteso sia quale *board* interministeriale in cui affrontare gli aspetti di sicurezza e difesa degli assetti nazionali, sia quale strumento di indirizzo per la *policy* e gli investimenti nel settore. Anche in tale contesto dovranno essere opportunamente veicolate e valorizzate le esigenze e il contributo che la Difesa potrà garantire nella tutela degli interessi nazionali.

L'attuale quadro giuridico nazionale, infine, impone significative limitazioni per la Difesa, in particolare al di sotto della soglia di aperta aggressione, nello sviluppo di capacità militari e nella condotta di operazioni nei domini *Cyber* e Spazio, così come nella gestione della competizione nell'ambiente informativo, a fronte di una sempre maggiore rilevanza negli scenari di competizione geostrategica.

Pertanto, al fine di garantire la propria funzione primaria di Difesa e la piena interoperabilità nell'ambito delle organizzazioni internazionali di riferimento, è necessario un approccio nazionale comune e condiviso, che consenta di effettuare investimenti e di definire *policy*, normative e procedure innovative ad ampio spettro che permettano alla Difesa di sviluppare capacità per operare efficacemente nelle nuove forme del confronto e contribuire a giocare un ruolo attivo nel *continuum of competition*.

MULTIDOMINIO: UN NUOVO PARADIGMA

Prepararsi ad affrontare le future sfide poste dall'evoluzione dello scenario internazionale in chiave Multidominio - realtà percepita da molti, ma compresa da pochi in termini di potenzialità e letalità capaci di colpire nel profondo il sistema Paese senza poter identificare chiaramente la provenienza della minaccia - necessita di un profondo cambio di paradigma concettuale, culturale e gestionale in grado di sviluppare una risposta spiccatamente multidimensionale attraverso la piena integrazione di una varietà di attori - civili e militari (c.d. *whole-of-government and whole-of- society approach*) - da sviluppare sui differenti livelli internazionale, nazionale, intergovernativo ed interagenzia.

Il nuovo paradigma delle operazioni Multidominio deve partire dall'elaborazione di una **visione strategica nazionale unitaria e condivisa** che delimiti inequivocabilmente il perimetro politico, economico e legale all'interno del quale tali operazioni possano essere condotte, identificando chiaramente le aree d'interesse nazionale da salvaguardare.

Si sente fortemente l'esigenza poi di **un organismo a livello governo centrale che definisca la Strategia Nazionale di Sicurezza** coordinando, integrando e sincronizzando gli strumenti del Potere nazionale (Diplomatico, Informativo, Militare ed Economico – DIME) per la gestione delle crisi e della competizione internazionale in un contesto Multidominio. A livello operativo, invece, appare senza dubbio necessario definire la configurazione ottimale di un **modello di Comando e Controllo** che superi le logiche delle competenze settoriali e che sia in grado di dare coerenza alle diverse informazioni fornite dai sensori periferici, consentendo l'integrazione delle diverse situazioni in un'unica, coerente ed aggiornata situazione generale – la *Multi-Domain Common Picture* – sulla base della quale verranno assunte le decisioni.

Un ulteriore elemento cardine delle operazioni Multidominio sarà la **ricerca continua dell'integrazione e dell'interoperabilità** tra sistemi, processi ed attori coinvolti nei diversi domini, sia a livello nazionale, sia a livello internazionale/sovranazionale.

In ultimo, sarà cruciale definire il nuovo ruolo della **dimensione umana** nell'evoluzione del suo rapporto con le tecnologie emergenti, con particolare riferimento all'Intelligenza Artificiale. In tal senso sarà strategico il rinnovamento del processo di scelta, formazione e crescita del capitale umano, che dovrà essere orientato sia allo sviluppo delle competenze a connotazione tecnico-specialistica, sia all'educazione dei *leader* a confrontarsi con realtà diverse e ad impiegare nuovi strumenti a disposizione.

In tale quadro di riferimento la Difesa si propone, pertanto, di promuovere un dibattito collettivo su quelle che possono essere le **linee di indirizzo generali** per consentire lo sviluppo di un approccio nazionale alle Operazioni Multidominio e, in maniera specifica, le **linee di indirizzo per la Difesa** in grado di delineare le principali esigenze di trasformazione ed innovazione dello Strumento Militare.

LINEE DI INDIRIZZO GENERALI

La definizione degli elementi che potranno risultare determinanti per lo sviluppo di un **approccio nazionale alle operazioni Multidominio** richiede necessariamente l'avvio di un dialogo intergovernativo nell'ambito del quale poter analizzare le potenziali vulnerabilità, individuare le migliori soluzioni ed adottare i necessari adeguamenti organizzativi, definendo le reciproche competenze. In questo senso sono state individuate le seguenti linee di indirizzo generali, ancorché non esaustive, volte a sviluppare capacità di consapevolezza (*awareness*) sulle nuove minacce, di analisi e sintesi, di rapidità decisionale proattiva piuttosto che reattiva:

- **Promozione della Cultura della Sicurezza nazionale**

  Il punto di partenza si colloca nella promozione di una Cultura della Sicurezza nazionale che formi ed informi i diversi livelli della società (dalla *leadership* al singolo cittadino) sulle possibili minacce in relazione agli interessi del Paese e, nel contempo, sui piani e le azioni definite nell'ambito di un'unica Strategia Nazionale di Sicurezza. In un sistema complesso in cui le nuove forme di minaccia possono arrivare a ingaggiare la sfera intima e privata delle persone, delle aziende, della società e delle istituzioni, la debolezza di un solo anello di questa complessa relazione ed interconnessione tra attori pubblici e privati può determinare un *vulnus* nell'ambito del più ampio perimetro di sicurezza nazionale.

  In tal senso, la distanza tra ambito governativo e società civile in Italia potrebbe rendere l'ambiente informativo un elemento di vulnerabilità della strategia difensiva italiana, soprattutto alla luce del livello di sofisticazione raggiunto in questo ambito dai *competitors*. Il controllo dell'ambiente informativo può risultare, infatti, particolarmente problematico per le democrazie occidentali e necessiterà di poter fare affidamento sulla popolazione tutta per riconoscere le minacce nell'ambiente informativo. In questo senso, il rinvigorimento della società nazionale, sfiduciata e poco coesa, e il rilancio del contratto sociale, anche attraverso l'elaborazione di strategie *ad hoc*, risultano fondamentali per assicurare la resilienza del sistema Paese.

E' importante, dunque, intervenire strutturalmente sui percorsi informativi e formativi ad ogni livello sui temi della Sicurezza e Difesa nazionale valorizzandoli come specifico settore disciplinare e sviluppando un linguaggio comune tra Istituzioni e Cittadino con un approccio di *soft power* volto a rafforzare il senso di appartenenza e l'identità nazionale.

Particolare attenzione in questo processo di crescita culturale deve poi essere posta nella formazione della *leadership* strategica nell'intento di adeguare il processo decisionale (*decision making*) in termini di velocità, completezza ed efficacia al nuovo contesto di confronto multidimensionale.

Questo nuovo approccio alla Sicurezza deve poi stimolare un dibattitto approfondito e coraggioso nella ridefinizione dell'attuale cornice etico-politica-giuridica che permetta di affrontare adeguatamente i nuovi scenari, con particolare riferimento a quello tecnologico, conferendo quella capacità di rispondere in tempi rapidi alle situazioni di crisi e di poter implementare strumenti e metodologie adeguate alle esigenze delle nuove sfide.

- **Sviluppo di una Sicurezza Multidominio integrata**

  L'estensione della competizione internazionale ai nuovi domini *Cyber* e Spazio comporta anche l'estensione del concetto di campo di battaglia (*battlespace*), evidenziando la necessità di una evoluzione del concetto di Sicurezza e Difesa che travalichi la sola dimensione fisica e/o geografica per concorrere alla tutela degli interessi nazionali (tangibili e intangibili, fisici e virtuali) ovunque essi si trovino, anche attraverso l'atteggiamento di una postura proattiva e preventiva. Ne consegue che la difesa degli assetti spaziali e quella delle reti risultano ulteriori funzioni critiche, che si aggiungono a quelle tradizionali, per garantire la continuità di servizi strategici essenziali e la tutela degli interessi nazionali. In tale contesto, la rapida evoluzione dei nuovi domini e la possibilità di una *escalation*, anche militare, della competizione necessitano di scelte innovative di *policy* in considerazione dell'esigenza di evitare inefficienze e ritardi sia in termini di frammentazione di competenze, sia di impiego delle risorse che, in termini economici, costituiscono un elemento significativo di cui necessariamente tenere conto. In tale contesto, risulta necessario sviluppare una Sicurezza Multidominio integrata nella quale prevedere, in particolare per i nuovi domini, una rivisitazione delle competenze assegnate ai diversi dicasteri e che garantisca unicità di indirizzo e continuità di finanziamento, attraverso l'impiego di risorse aggiuntive, per garantire lo sviluppo di capacità credibili. Parimenti, in funzione delle scelte che verranno adottate, risulterà necessario individuare, sia a livello nazionale che internazionale, livelli ed indicatori di soglia che, attraverso un sistema di deleghe predefinito, autorizzi la corrispondente reazione nazionale, nell'ambito di opzioni di risposta incrementali attraverso l'impiego di tutti i domini e gli strumenti del Potere nazionale (*Multi-Domain Escalation Management Options*).

- **Sviluppo di un approccio nazionale di deterrenza multidimensionale**

  Applicando l'attuale concetto di deterrenza - capacità di convincere un potenziale aggressore che le conseguenze della coercizione o del conflitto armato supererebbero

i potenziali guadagni attraverso il mantenimento di una capacità militare credibile e di una strategia con la chiara volontà politica di agire - all'evoluzione dello scenario geopolitico internazionale con un approccio Multidominio, risulta evidente la necessità di sviluppare un approccio nazionale di deterrenza basato su credibili capacità militari in tutti i domini, che vanno ad integrare le attuali capacità convenzionali tutt'ora determinanti. Nuove capacità militari per operare anche nei nuovi domini *Cyber* e Spazio, così come nell'ambiente informativo e in quello elettromagnetico. Inoltre, attraverso la definizione degli interessi nazionali ed il superamento del concetto di soglia che autorizza un intervento militare, sarà possibile sviluppare anche una strategia comunicativa orientata a sostenere un intervento preventivo con tutti gli strumenti del Potere nazionale, ivi incluso quello militare. L'efficacia di quanto detto non può prescindere da una *forma mentis* adeguata della *leadership*, che deve essere formata ed educata all'utilizzo di tutte le capacità a propria disposizione affinché l'approccio e la postura nazionale possano risultare coerenti.

- **Realizzazione di una dorsale digitale (*digital backbone*)**

  L'esigenza di percepire quanto avviene in tutti i domini (fisici e virtuali) necessita di una vasta rete di sensori che coprano anche gli ambienti elettromagnetico e informativo per comprendere il comportamento e l'atteggiamento di tutti gli attori in gioco. In tal senso, la capacità di raccogliere, analizzare, trasmettere, fondere e distribuire grandi quantità di dati necessita di una piattaforma di comunicazione distribuita, scalabile e ridondante, concepita e sviluppata *ab origine* per garantire la protezione dai potenziali attacchi o dalla possibile manipolazione dei dati, consentire la continuità dei servizi essenziali (quali, ad esempio, la radionavigazione satellitare PNT) e permettere la diffusione delle informazioni su differenti livelli di classifica (*multilevel security*). Inoltre, dovrà essere implementata attraverso l'impiego di soluzioni tecnologiche avanzate, per contribuire a generare una reale superiorità informativa e cognitiva, e l'utilizzo di protocolli standardizzati che consentano l'implementazione incrementale di nuovi sensori/attuatori (o la loro immediata sostituzione con soluzioni aggiornate allo stato dell'arte della tecnologia disponibile) e l'estensione della rete a un numero crescente di attori.

  La realizzazione di questa dorsale digitale, estesa ed integrata tra tutti gli strumenti del Potere nazionale, consentirà la piena condivisione delle informazioni, lo sviluppo di processi e procedure comuni ed il supporto al processo decisionale nazionale per garantire la sincronizzazione degli effetti. Nello specifico tale struttura risulta determinante per la Difesa nell'assicurare la funzione "percepire" e generare una piena e condivisa *Multi-Domain Common Picture*.

- **Accelerazione del processo di innovazione**

  Lo sviluppo e l'implementazione di nuove soluzioni tecnologiche rappresentano elementi abilitanti per la condotta di attività Multidominio. La spregiudicatezza con cui alcuni attori adottano nuove soluzioni tecnologiche per conseguire i propri precipui interessi sfruttando le lacune normative del diritto internazionale contribuisce ad acuire il possibile divario tecnologico a sfavore dei Paesi occidentali.

Per invertire tale tendenza risulta necessario avviare un processo di forte accelerazione dell'innovazione tecnologica, anche in ambito nazionale, attraverso lo sviluppo di nuovi modelli che possano consentire forme di collaborazione pubblico-privato più snelle, attraverso le quali sviluppare e implementare nuove soluzioni tecnologiche sulle quali modellare, qualora necessario, anche l'evoluzione del quadro normativo. Più in generale, si rende necessario promuovere una cultura dell'innovazione che permetta a tutti i livelli organizzativi e decisionali di cogliere appieno le sfide, ma soprattutto le opportunità offerte dalle tecnologie emergenti e dirompenti.

LINEE DI INDIRIZZO PER LA DIFESA

Il successo nelle operazioni Multidominio dipende dall'integrazione di tutti i fattori coinvolti (strumenti di potere, costante sviluppo tecnologico e capacità disponibili) e dall'attitudine ad intercettare gli indicatori della minaccia alla Sicurezza nazionale. Il concetto legato alle Operazioni Multidominio supera ed evolve, quindi, l'attuale dottrina militare delle Operazioni *Joint*, basandosi invece sull'effetto sinergico derivante dallo sviluppo coordinato di operazioni condotte nei domini convenzionali, in quelli *Cyber* e Spazio con estensione anche agli ambienti informativo ed elettromagnetico, e dalla capacità di produrre effetti in tutte e tre le dimensioni (fisica, virtuale e cognitiva). Questo nella consapevolezza che la perfetta integrazione di tutti gli elementi in campo è pressoché impossibile da ottenere a causa di diversi vincoli (politici, economici, operativi, tempistiche di utilizzo delle risorse, ecc.) così da impedire l'utilizzo simultaneo di tutte le risorse disponibili, accettando invece una sincronizzazione Multidominio per mantenere il vantaggio strategico e l'iniziativa sull'avversario.
Emerge quindi la necessità di dover evolvere l'attuale concetto di operazioni *Joint & Combined* verso un nuovo paradigma *cross domain* non lineare e non compartimentato, anche alla luce della straordinaria evoluzione delle tecnologie applicate ai processi decisionali, ai sensori ed ai sistemi d'arma.

Il primo obiettivo sarà quello di **formare ed educare la *leadership* militare**, attuale e futura, con una *forma mentis* idonea alla comprensione e alla gestione di tutti i domini attraverso una visione ed una volontà di agire basate su un approccio oggettivo, aperto e creativo per ottenere il risultato richiesto ad un costo accettabile, gestendo una situazione piena di interazioni e anticipazioni dinamiche che pongono problemi fondamentali per qualsiasi dottrina o teoria strategica.

Altrettanto cruciale ricopre lo sviluppo di **nuovi modelli di preparazione delle forze** che consentano di fronteggiare le sfide imposte dalle MDO. Attraverso l'addestramento del singolo e di tutte le unità ad ogni livello ordinativo da parte delle singole Forze Armate in prospettiva multidimensionale e la predisposizione a livello Interforze di scenari addestrativi simulati e di attività esercitative mirate sarà possibile assicurare quell'integrazione e quella interoperabilità tra sistemi e attori coinvolti (non solo militari) necessarie a preparare lo Strumento Militare ad operare efficacemente nel contesto Multidominio.

Il **modo di pianificare**, conseguire e misurare gli effetti dovrà necessariamente essere adattato, così come la definizione degli obiettivi che ad essi contribuiscono. Pertanto, il disegno concettuale delle operazioni (*Operation Design*) e quello esecutivo (*Plan*) avranno una forma diversa da quella attuale.

In tal senso, andrà sviluppato un **nuovo quadro normativo nazionale** che possa dare maggiore impulso alle attività descritte implementando l'integrazione a livello interforze, più di quanto non lo sia già, per consentire allo Strumento Militare di operare in modo sincrono su contesti fisici e virtuali diversi e con scarsi tempi di preavviso. Nell'ambito delle alleanze di cui il nostro Paese fa parte è, altresì, importante rendersi protagonisti di un processo evolutivo delle organizzazioni che portino verso un'unicità normativa e conseguentemente dottrinale, garantendo coerenza terminologica e unicità di intenti nel contrastare le minacce nel *continuum of competition*.

La risposta efficace alle minacce in ambito Multidominio necessita poi di una forte integrazione che consenta la sincronizzazione degli effetti attraverso la definizione di una **catena di Comando & Controllo sincronizzata** che garantisca sia l'unicità di comando, sia, laddove necessario, l'applicazione di deleghe ed un'ampia autonomia decisionale dei livelli inferiori. In tal senso, per la Difesa, l'evoluzione del Comando Operativo di Vertice Interforze (COVI) e l'implementazione del progetto del JOC consentiranno di garantire la capacità di sintesi necessaria a sviluppare una ***Multi-Domain Common Picture***, basata sulla condivisione dei concetti e sull'integrazione dei sistemi dei Comandi di Componente e delle rispettive Sale Operative. La sola *Multi-Domain Common Picture* risulta, tuttavia, poco significativa se non contestualizzata ed integrata anche nei processi di Comando e Controllo e nella gestione del *battlespace*, tanto che si dovrà creare una matrice di sincronizzazione che, con l'aiuto delle nuove tecnologie, possa mettere in relazione i domini, le capacità, le vulnerabilità e le opportunità da sfruttare in relazione al binomio costo-efficacia.

L'esigenza di prevenire e gestire l'*escalation* della competizione e influenzare l'ambiente e gli attori che vi operano necessita di un approccio nazionale che consenta un utilizzo integrato e, ove necessario, anche preventivo, di tutte quelle capacità che possono contribuire a generare effetti duraturi nella dimensione cognitiva. In tale contesto, le operazioni Multidominio seguono un andamento sinusoidale (con incremento e decremento della competizione) che si differenzia sostanzialmente dal modello lineare di *escalation*. Pertanto, la Difesa dovrà sviluppare un approccio che permetta di impiegare, in materia integrata, tutte **le proprie capacità (cinetiche e non cinetiche)** per assicurare il proprio contributo nell'ambito della strategia nazionale, anche attraverso un potenziamento delle proprie capacità non cinetiche per contribuire a generare effetti, anche attraverso l'ambiente informativo, nella dimensione cognitiva.

Le capacità sinora acquisite dalla Difesa risultano attestate alle singole FF.AA. e sono state sviluppate con un approccio *bottom-up* in cui le singole componenti si sono via via dotate di nuovi strumenti per garantire la propria autonomia operativa generando ridondanze ed una vera e propria competizione interna per l'acquisizione di ulteriori competenze e dei conseguenti programmi di finanziamento al fine di estendere il proprio raggio d'azione. Tuttavia, la specificità dei nuovi domini, l'entità delle risorse, anche

finanziarie, necessarie a sviluppare nuove capacità **richiedono un approccio *top-down*** che consenta una razionalizzazione della capacità, superando gli "*stovepipements*" di componente oggi esistenti e di definirne gli obiettivi e, conseguentemente, distribuire i mezzi necessari. Questo non comporterà, almeno nel breve termine, la costituzione di nuove forze dedicate, bensì lo sfruttamento delle eccellenze già esistenti per superare la logica *single service* e sviluppare capacità strategiche da integrare *ab origine* a livello interforze.

Nell'ambito dello **sviluppo tecnologico** anche la Difesa deve sviluppare un proprio acceleratore/incubatore di innovazione che, attraverso una stretta collaborazione pubblico-privato, possa avviare, sin dalla fase embrionale e concettuale, un processo di innovazione che, guardando al futuro, possa intercettare e indirizzare nuove e inedite traiettorie tecnologiche, ancor prima della successiva fase di ricerca e sviluppo. Basti pensare all'esigenza di disporre di una sempre maggiore quantità di sensori/attuatori distribuiti in tutti i domini che richiederà la necessità di dotarsi di *Robotic Autonomous System* (RAS) su larga scala da impiegare attraverso logiche e processi di robotica di sciame (*swarm intelligence*) o all'esigenza di operare efficacemente nell'ambiente elettromagnetico che richiederà lo sviluppo di capacità offensive (es. le c.d. *Directed energy weapons*) al fine di generare effetti (temporanei e/o permanenti) e interdirne l'utilizzo all'avversario per l'accesso ai domini.

La pervasività dell'elemento tecnologico non sostituirà, tuttavia, **la posizione preminente dell'uomo**, che manterrà la sua centralità anche se all'interno di nuovi paradigmi gestionali. La sempre maggiore rilevanza dei nuovi domini *Cyber* e Spazio e l'evoluzione della competizione sia nell'ambiente informativo, sia in quello elettromagnetico richiederanno maggiori investimenti in termini di risorse, anche umane che, attraverso lo sviluppo di percorsi formativi dedicati e di profili di impiego che mettano in risalto la competenza, acquisiscano *skills* differenti e diversificate, lasciando spazio a sistemi e piattaforme autonome nei settori convenzionali riducendo, così, la propria presenza.

Allegato A
VISIONE INTERNAZIONALE

GENERALITÀ

Il tema del Multidominio, e più nello specifico delle *Multi-Domain Operations* (MDO), è oggetto di un vivo dibattito internazionale. La concettualizzazione iniziale del modello statunitense, esercito centrica, prevedeva infatti l'inquadramento delle MDO nella sola risposta militare per penetrare eventuali strategie *Anti Access- Area Denial* (A2/AD) avversarie e sconfiggere un opponente di livello *peer/near peer competitor*. In tale ambito, le MDO sono intese come un'evoluzione delle *Joint Operations*, per garantire la convergenza delle capacità in tutti i domini. A questa visione, si sono poi accostate quelle che ricercano l'integrazione del *Military Instruments of Power* (MIoP) con gli altri *Instruments of Power* (IoP). Esempio è l'approccio inglese, con la propria *Joint Concept* "*Multi-Domain Integration*", che evidenzia l'esigenza di un'integrazione già dal livello governativo e nell'ambito dell'intero spettro della competizione a tutti i livelli delle operazioni militari (strategico, operativo e tattico).

LA VISIONE NATO

L'approccio Multidominio dell'Alleanza Atlantica è inteso ben oltre la semplice espansione dell'approccio *joint* con l'aggiunta dei domini Spazio e *Cyber*, attraverso un'integrazione che consenta di acquisire e mantenere l'iniziativa.

Tale approccio è volto a combinare le azioni in tutti e cinque i domini delle operazioni, orchestrando e amplificando le capacità disponibili al fine di sfruttare la sorpresa, la convergenza e il successo, tale da generare la libertà di manovra nello spazio di battaglia funzionale per creare effetti nella dimensione fisica, virtuale e cognitiva.

L'approccio Multidominio dell'Alleanza ottimizza l'intera gamma di capacità politiche, militari e civili e le integra attraverso i cinque domini per ottenere il massimo vantaggio[35].

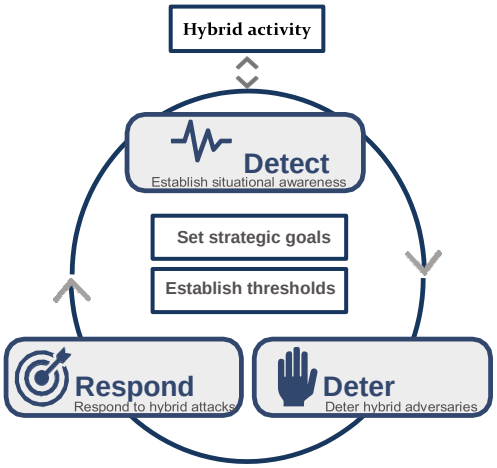
Va altresì osservato che l'*Allied Command for Transformation* (ACT) sostiene differenti iniziative di sviluppo concettuale sul tema nell'ambito della *Multinational Capability Development Campaign* (MCDC) con il progetto "*Multi-Domain – a multinational understanding*" e con il supporto del *Joint Air Power Competence Center* (NATO *Centre of Excellence* – CoE) per lo sviluppo di un progetto sulle "*Joint All Domains Operation* - JADO".

[35] AJP-01 Ed. F "*Allied Joint Doctrine"* (*draft*).

Di recente, inoltre, ACT ha inserito il proprio progetto sul tema del Multidominio nelle *Lines of Deliveries* e, ancor di più, nei *Warfare Development Imperatives* del NATO *Warfighting Capstone Concept* (NWCC)[36] quale esigenza prioritaria ed *enabler*, confermando la centralità del tema quale esigenza di operare attraverso tutti i domini nell'intero spettro delle operazioni.

UNIONE EUROPEA – *COUNTER HYBRID*

Seppur non strettamente legato al concetto di Multidominio *strictu sensu*, anche l'Unione Europea sta affrontando il tema del rapporto tra lo strumento militare e gli altri *Instruments of Power* nella gestione della competizione internazionale contro le minacce ibride. In particolare, attraverso l'elaborazione della propria "*EU Guidance on countering Hybrid threats during the planning phase of EU-led CSDP military operations and missions*" e partendo dal modello concettuale elaborato dal UE *Hybrid* CoE[37], l'UE intende fornire una guida per contrastare le forme di minaccia ibrida durante la fase di pianificazione delle operazioni militari nell'ambito della *Commons Security and Defence Policy* – CSDP.
Secondo la guida europea, il primo passo per contrastare le minacce ibride consiste nell'identificazione della minaccia per poi decidere la linea d'azione più idonea da intraprendere nella consapevolezza che il livello di ambizione non potrà essere lo stesso per tutti gli attori. In tale contesto, le forme di risposta dovranno uniformarsi alle scelte politiche variando in funzione dell'intensità della minaccia, delle decisioni politiche e della possibilità di risposta, dal semplice assorbimento degli attacchi, alla deterrenza aggressiva ed all'adozione di misure più assertive o di ritorsione per interrompere l'aggressione e prevenire ulteriori attacchi.

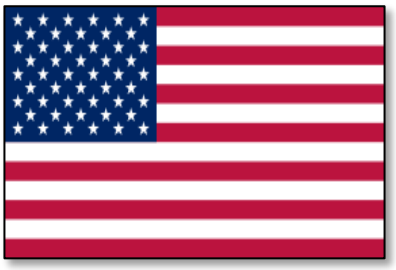


Il modello proposto dall'Unione Europea si basa sulla definizione di obiettivi strategici e soglie di risposta comuni e su un fra*mework* di riferimento su un ciclo di tre differenti funzioni: *Detect*, *Deter* e R*espond*, in cui la prima funzione è permanentemente attivata e le altre due vengono attivate in funzione delle soglie di risposta.
Infine, l'approccio UE tiene conto dell'*escalation* tra gli strumenti del potere, in cui un opponente può intensificare la propria azione verticalmente, aumentando l'intensità di

[36] Concetto a guida ACT per identificare le aree capacitive su cui far gravitare lo sviluppo dello strumento militare dei prossimi 20 anni sui criteri di multidominio, interoperabilità ed impiego di risorse tecnologicamente avanzate.
[37] *Centre of Excellence for Countering Hybrid Threats* (Hybrid CoE): istituito nel 2017 ad Helsinki da 9 Nazioni fondatrici (Finlandia, Francia, Germania, Lettonia, Lituania, Polonia, Svezia, Regno Unito e USA) con l'obiettivo di costituire un *forum* di discussione e cooperazione tra UE e NATO per contrastare le forme di minaccia ibrida. Hanno successivamente aderito altri 19 Paesi.

uno o più strumenti di potere, o orizzontalmente, sincronizzando più strumenti di potere per creare effetti maggiori rispetto alla sola *escalation* verticale.

USA – *JOINT ALL DOMAIN OPERATIONS*



L'origine del costrutto concettuale statunitense è legato all'identificazione di una soluzione efficace per competere con successo nell'ambiente operativo strategico con *peer/near peer competitor* (vds. Russia, Cina, Iran e Corea del Nord), sotto e sopra la soglia. Sotto la soglia emerge la centralità della deterrenza generale o su misura, intesa in tutte le sue declinazioni, dall'ammodernamento capacitivo al *capacity bulding*, al pre-posizionamento delle forze. In situazioni sopra la soglia viene invece posta particolare enfasi nella capacità di penetrare e disarticolare i sistemi A2/AD nemici.

In particolare, l'US *Air Force* ha recentemente pubblicato l'*Air Doctrine Publication* "*Department of The Air Force Role in Joint All-Domain Operations (JADO)*", in cui vengono declinate le implicazioni per l'impiego del potere aereo nelle operazioni Multidominio, mentre l'esercito statunitense ha avviato un progetto riassumibile in tre macro aree:

- consapevolezza concettuale e dottrinale, con l'elaborazione di una serie di documenti di natura concettuale, capacitiva e dottrinale (primariamente per l'impiego di *Brigade Combat Team*);
- creazione di unità dedicate, *multi-domain Task Force* – MDTF, che raccolgono sotto un unico comando capacità letali e non letali già esistenti, integrandole e sincronizzandole attraverso domini multipli al fine di sopraffare uno specifico obiettivo. Una MDTF con capacità cinetiche e non-cinetiche è già schierata nel teatro pacifico (INDOPAC) e un'altra sarà dislocata a Stoccarda (EUCOM/AFRICOM).
- avvio della sperimentazione, volta a testare la capacità di una formazione a livello Brigata di manovra (*Brigade Combat Team*) di concepire e condurre una operazione in contesto MDO, partendo dalla già citata idea cardine che tutte le formazioni devono essere in grado di combattere in modo *cross-domain.*

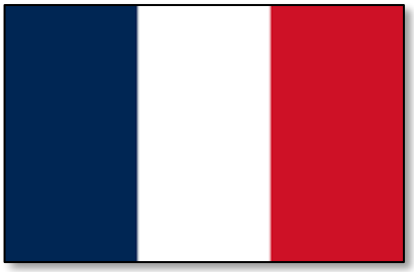
L'idea, immutata nella sua essenza, è stata riadattata in una visione denominata *Joint All-Domain Operation* (JADO), un modello che guiderà il processo di ammodernamento capacitivo nella prospettiva di medio-lungo termine (oltre il 2035).

REGNO UNITO – INTEGRAZIONE MULTIDOMINIO

A differenza dell'approccio statunitense, focalizzato sulla risoluzione di un problema militare con strumenti militari, l'approccio britannico è volto ad estendere il campo di interpretazione delle *Multi-Domain Operations* in chiave interministeriale, interagenzia e multinazionale al fine di aumentare il livello di "integrazione" delle capacità militari e civili, la

"sinergia" delle azioni e assicurare, dunque, la "sincronizzazione" degli effetti sui nodi critici multidimensionali dell'avversario.
Al momento, anche i britannici, sulla falsariga degli americani, stanno lavorando per federare capacità afferenti alle dimensioni cognitiva e virtuale.

FRANCIA – *MULTIMILIEUX ET MULTICHAMPS* (M2MC)



L'approccio francese si basa sul riconoscimento di una complessità dell'ambiente operativo incentrata sul riconoscimento dei 5 domini NATO (*milieux*) cui si aggiungono ulteriori due campi d'azione (*champs*), elettromagnetico e informativo, che consentono di operare per generare effetti. Tale complessità richiede un profondo cambio di paradigma nella gestione delle operazioni attraverso un rafforzamento della cooperazione tra componenti (*enhanced cooperation*). In particolare, l'approccio francese si fonda su una strategia nazionale consolidata in cui il contributo dello strumento militare è assicurato tramite il preposizionamento di forze nelle aree di interesse strategico, nell'ambito di una strategia nazionale di presenza avanzata.

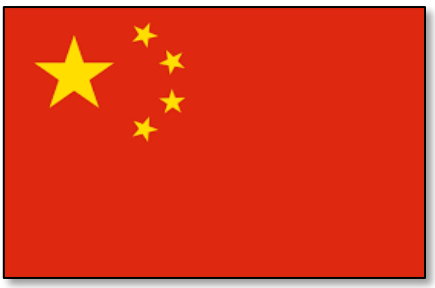
FEDERAZIONE RUSSA – CONTROLLO DELLA REAZIONE

La visione della Federazione russa può essere generalmente ricondotta al concetto di "controllo della reazione" (*reflexive control*). In particolare, sviluppatosi dal punto di vista storico attraverso differenti periodi del XX secolo, il controllo della reazione è il prodotto di un paradigma marxista-leninista, secondo cui "*la cognizione risulta dal riflesso del mondo materiale nella mente umana, che determina la coscienza sociale. L'intelligenza dell'uomo ed i processi cognitivi dipendono dalla sua conoscenza sensoriale del mondo esterno, che a sua volta determina il contenuto e le dimensioni della sua consapevolezza*" [38].
La strategia del "controllo della reazione", applicabile tanto contro i decisori umani quanto contro i sistemi informatici, è definita come un mezzo per indurre un collaboratore o un avversario a prendere volontariamente una decisione voluta dal promotore dell'azione, veicolandogli informazioni confezionate *ad hoc.* In tale contesto, le tecniche utilizzate nel *reflexive control* possono essere intimidazione, lusinghe, disinformazione, inganno, dissimulazione che mirano a scardinare il processo decisionale avversario ed a ridurre i tempi disponibili per l'adozione di efficaci correttivi. Ne consegue come per raggiungere la propria efficacia la strategia necessiti di uno studio approfondito della natura più "intima" dell'avversario e del suo pensiero e di un insieme di concetti, conoscenze, idee ed esperienze.

[38] "La dottrina Gerasimov e la filosofia della guerra non convenzionale nella strategia russa contemporanea", Libellula Edizioni - Nicola CRISTADORO, (2018).

In tale contesto, si innesta la dottrina Gerasimov, che prevede di attaccare l'avversario sul piano economico, cognitivo e fisico facendo largo ricorso a procedure non convenzionali, attraverso una correlazione di strumenti non militari e militari nel rapporto di 4 a 1. Gli strumenti non militari che la dottrina individua includono gli sforzi di condizionare le componenti politica, economica e sociale avversarie, attraverso la sovversione, lo spionaggio e la propaganda, combinati con attacchi cibernetici che con le loro capacità e gli strumenti sempre più sofisticati di cui dispongono, rappresentano l'avanguardia *dell'Information warfare*. Appartiene al dominio cibernetico, difatti, lo strumento della propaganda "bianca", "nera" o "grigia"[39], capace di colpire in modo devastante i centri nevralgici dell'economia, della società, della politica di uno Stato, attraverso la compromissione o la neutralizzazione di reti informatiche.
Con tale approccio, cresce il ruolo dei mezzi non militari per conseguire fini politici e strategici superando anche in efficacia la potenza della forza delle armi. La chiave dei metodi pratici di conflitto è mutata in direzione di un vasto utilizzo di misure politiche, economiche, mediatiche, umanitarie e di altre non appartenenti all'ambito militare, poste in atto in coordinazione con il potenziale malcontento popolare. L'uso manifesto della forza è riservato solo al conseguimento del successo finale nel conflitto.

CINA – DOTTRINA DELLE TRE GUERRE



L'obiettivo della grande strategia della Repubblica Popolare Cinese (RPC), di ampio respiro e spesso guardando a svariate decadi nel futuro, è quello di diventare un "paese socialista moderno" entro il 2049.[40] Per farlo, l'*establishment* cinese ritiene di dover trasformare l'Esercito Popolare di Liberazione (EPL) in una forza armata di "classe mondiale" entro la metà del XXI secolo. Nel decennio alle nostre spalle, la dottrina cinese ha sviluppato concetti importanti da questo punto di vista che offrono un'idea chiara della visione del conflitto, ma anche delle realistiche ambizioni e capacità militari cinesi. Il concetto di "difesa avanzata" per esempio, si riferisce non soltanto alla necessità di allontanare dal territorio nazionale la prima linea difensiva, ma anche al "supporto di un'espansione omni-direzionale degli interessi nazionali".[41] Con "spazio strategico" la dottrina militare demarca invece aree che "vorrebbe influenzare con lo strumento militare, ma non attraverso operazioni di combattimento".
Particolare rilevanza assume il concetto di "controllo efficace", espressione che rivela la consapevolezza della Cina di come le proprie "capacità" per azioni militari all'estero siano ancora limitate. Questo concetto si affianca al più conosciuto elemento di "difesa

[39] Classificazione in base alla fonte: la propaganda bianca arriva da una fonte chiaramente identificabile; la propaganda nera finge di arrivare da una fonte amica, ma in realtà è dell'avversario; la propaganda grigia pretende di arrivare da fonti neutrali, ma in realtà arriva dall'avversario.

[40] Xi Jinping, 2017. '*Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era*'. Relazione politica presentata in occasione del 19° congresso nazionale del Partito Comunista Cinese, 18 ottobre. http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf .

[41] Taylor Fravel, China's Changing Approach to Military Strategy: The Science of Military Strategy from 2001 and 2013. *MIT Political Science Department Research Paper*.

attiva" che si riferisce all'adesione ai principi di "difesa, autodifesa, attacco reattivo" e di "non attaccheremo a meno che non saremo attaccati, ma contrattaccheremo di sicuro qualora fossimo attaccati"[42]. Inoltre, il governo cinese ritiene che "strategie centrate sullo scontro cinetico" possano portare a "guerre "non-vinte"[43].

Questi elementi dottrinali hanno senso nel contesto di interessi cinesi che crescono a grande velocità rispetto all'arretratezza del EPL in alcuni settori. Perciò, da una parte "le minacce devono essere prevenute anche nelle menti di élite di paesi rivali che possano decidere di competere, contenere o attaccare la Cina"[44]. Dall'altra, la Cina vede il Multidominio emergere dalla "convergenza fra diverse capacità attraverso differenti domini su tutti i livelli di guerra al fine di compensare le debolezze relative in singoli domini e creare finestre di superiorità"[45]. In questo contesto dottrinale si inserisce la dottrina delle "Tre Guerre", che nasce anche sulla base dei principi delle antiche strategie cinesi di "guerra della percezione"[46] ed ha l'obiettivo di influenzare "narrazioni pubbliche internazionali, indebolire la volontà del nemico, plasmare narrazioni diplomatiche e politiche e promuovere gli interessi della RPC in tutte le fasi del conflitto"[47]. Il Pentagono americano fornisce i seguenti esempi per ognuna delle tre componenti:

- *Guerra psicologica*, utilizza la propaganda, l'inganno, le minacce e la coercizione per influenzare il processo decisionale dell'avversario, contrastando anche le operazioni psicologiche dell'avversario;
- *Guerra dell'opinione pubblica*, diffonde informazioni per il consumo pubblico per guidare e influenzare l'opinione pubblica ed ottenere il sostegno del pubblico nazionale e internazionale;
- *Guerra legale*, utilizza le leggi nazionali ed internazionali per ottenere il sostegno internazionale, gestire le ripercussioni politiche ed influenzare il pubblico di destinazione (*Lawfare*).

[42] *State Council 2015. China's Military Strategy*.
[43] Stefan Halper, 2013. China: *The Three Warfares. Office of the Secretary of Defense. Washington, D.C. May*.
[44] Peter Mattis, 2018. *China's 'Three Warfares' in perspective. War on the Rocks. January 30*.
[45] Derek Solen, 2020. *Chinese views of all-domain operations. China Aerospace Studies Institute*. Agosto.
[46] J. Garnaur, 2014. '*US unsettled by China's "three warfares" strategy: Pentagon report'. The Sydney Morning Herald. April 1*1.
[47] *Office of the Secretary of Defense, 2020. Military and Security Developments Involving the People's Republic of China 2020. August 21*.

Allegato B
GLOSSARIO

AMBIENTE
Contesto in cui si opera, compresi l'aria, le acque, il terreno, lo spazio, il c*yberspace*, le risorse naturali, la flora, la fauna, gli essere umani e le loro interazioni. Gli ambienti di riferimento per le operazioni militari sono: marittimo, terrestre, aereo, spaziale, cibernetico, a cui si aggiungono l'ambiente informativo e quello elettromagnetico.

ANTI-ACCESS (A2) E AREA-DENIAL (AD)
Le operazioni *Anti-Access* (A2) e *Area-Denial* (AD) includono una varietà di attività militari che possono essere condotte in tutti i domini delle operazioni (terrestre, navale, aereo, spaziale e cibernetico) volte a negare all'avversario la capacità di entrare in una determinata area e di manovrare liberamente nello spazio della battaglia. In particolare:
- *Anti-Access* tradizionalmente si riferisce alla capacità di creare un cordone intorno ad un'area e di controllarne l'accesso, di fatto negando all'avversario di entrare nell'area contesa;
- *Area-Denial* si riferisce alla capacità di diminuire, degradare o neutralizzare la libertà di azione dell'avversario nell'ambito di un'area contesa.

AZIONI *CROSS-DOMAIN*
La combinazione integrata delle capacità (militari e non) nei diversi domini finalizzata a sfruttare una limitata finestra di superiorità e ingaggiare l'avversario nelle dimensioni fisica, cognitiva e/o virtuale.

COGNITIVE WARFARE
Nuova modalità di confronto permanente che mira ad attaccare la sfera delle convinzioni e delle opinioni di una popolazione con lo scopo di destabilizzare la coesione, la sicurezza e la prosperità di una Nazione.

COMPRENDERE
Funzione delle Operazioni Multidominio assolta attraverso l'interpretazione delle informazioni raccolte durante la fase "percepire", allo scopo di inquadrare la situazione nel contesto di riferimento ed effettuare valutazioni e previsioni utili a supportare un processo decisionale rapido ed efficace.

DIMENSIONE degli effetti
Lo schema concettuale che permette di valutare gli effetti da conseguire con le operazioni militari nel campo di battaglia nelle tre dimensioni: fisica, virtuale e cognitiva.

DOMINIO delle operazioni

Un insieme di capacità e attività che vengono applicate al campo di battaglia, in un ambiente di riferimento (marittimo, terrestre, aereo, cibernetico e spaziale).

EFFETTO

Il risultato (*result/outcome*) o la conseguenza di una o più azioni che influenzeranno lo stato fisico o l'atteggiamento comportamentale di un sistema (o elemento di sistema), contribuendo così alla realizzazione di una o più "condizioni decisive"[48].

JOINT FUNCTIONS

Attività militari a carattere omogeneo che combinate tra loro consentono l'efficace sviluppo di un'operazione militare.

MULTI-DOMAIN ESCALATION MANAGEMENT OPTIONS

Costruzione di opzioni di risposta incrementale attraverso l'impiego di tutti i domini e gli strumenti del Potere nazionale.

OPERAZIONI MULTIDOMINIO

Attività condotte per generare effetti in più di un dominio, contemporaneamente e in modo integrato. (Definizione NATO – *draft*)

Attività militari condotte anche in più domini per percepire, comprendere e, successivamente, orchestrare effetti convergenti finalizzati a generare dilemmi multipli ad una velocità tale da superare la capacità decisionale avversaria. La condotta di tali attività avviene attraverso la sincronizzazione delle azioni militari con gli altri Strumenti del Potere nazionale e/o con alleati e partner, sotto una struttura di comando e controllo sincronizzata (*Multi-Domain Command & Control* - MDC2). (Definizione nazionale - *draft*)

ORCHESTRARE

Funzione delle Operazioni Multidominio che comprende l'insieme delle attività di pianificazione ed esecuzione integrata delle azioni e attività per raggiungere gli obiettivi prefissati. Tale funzione si basa sull'efficacia continua delle funzioni "percepire" e "comprendere" e permette di condurre in modo flessibile le operazioni Multidominio, tenendo conto degli effetti reali conseguiti, piuttosto che dei dati presunti o degli effetti desiderati.

PERCEPIRE

Funzione delle Operazioni Multidominio che include le attività di sorveglianza, scoperta, classificazione, riconoscimento, tracciamento e identificazione, raccolta dati utili per il ciclo *intelligence* e per contribuire a generare comprensione.

[48] AJP-01 (D), *Allied Joint Doctrine*.

RULES BASED INTERNATIONAL ORDER - RBIO

Impegno condiviso dei Paesi a condurre attività secondo regole condivise che evolvono nel tempo. Esse possono includere: diritto internazionale, accordi di sicurezza regionale, accordi commerciali, protocolli di immigrazione e accordi culturali, ecc.

SINCRONIZZAZIONE DEGLI EFFETTI

L'integrazione di attività/eventi nel tempo al fine di raggiungere un *operational tempo* favorevole rispetto a quanto sviluppato da un potenziale avversario. Afferisce non solo al coordinamento delle attività militari a livello tattico, operativo e strategico ma anche alla necessaria integrazione con le attività sottese agli altri strumenti del Potere nazionale in un dato intervallo di tempo.

SISTEMA

Insieme di elementi che, ordinatamente collegati tra loro, contribuiscono a un determinato oggetto. Un sistema tende ad essere un insieme di parti interconnesse e interdipendenti, che formano un insieme identificabile, organizzato, complesso e dinamico. Può comprendere elementi, attività, persone o idee.

SISTEMA DI SISTEMI

Insieme di sistemi orientati o dedicati che uniscono le loro risorse e capacità per creare un nuovo sistema più complesso.

Allegato C
METODOLOGIA DI LAVORO E BIBLIOGRAFIA

Il presente documento concettuale è stato elaborato nell'ambito delle attività del "Gruppo di Progetto per il Team degli Innovatori" denominato COMIND (Comitato per l'Innovazione della Difesa), costituito per proiettare lo Strumento Militare nel prossimo futuro, dando sviluppo ed integrazione innovativa al Concetto Strategico del Capo di Stato Maggiore della Difesa.

Abbracciando il paradigma dell'*Open Innovation* attraverso il coinvolgimento del *network* di esperti del mondo accademico, industriale e della ricerca attestato all'Ufficio Generale Innovazione Difesa-INNOV@DIFESA, è stato analizzato il tema del Multidominio, scrutinando molteplici idee e variegate prospettive provenienti da differenti ambienti, attraverso sessioni settimanali di incontro e confronto, intervallate da regolari momenti di sintesi e condivisione con le Forze Armate.

Dal punto di vista metodologico, applicando il metodo del *Concept Development & Experimentation* (CD&E), sono stati raccolti e resi disponibili i contributi specifici degli esperti, consultate le fonti internazionali sul tema e condivisi gli esiti della partecipazione ad attività internazionali NATO e EU.

Di seguito l'elenco degli esperti che hanno fornito continuo ed estensivo supporto allo sviluppo del Concetto, ai quali lo Stato Maggiore della Difesa esprime il proprio riconoscimento, e le citazioni bibliografiche.

ESPERTI

Area Industria

- Dott. Daniele FRISONI – LEONARDO, *Project Engineering Manager*
- Dott. Alessandro FIDENZI – RAIT 88, *Chief Global Strategist*
- Dott. Massimo AMOROSI – RAIT 88 CBRN e *Biothreats specialist*, già consulente presso il MAECI per le tematiche CBRN e presso il Senato della Repubblica per i temi della Difesa

Area Accademia

- Prof. Andrea UNGARI, Professore ordinario di Storia contemporanea presso Università Guglielmo Marconi e Luiss Guido-Carli
- Dott. Zeno LEONI, docente di Sicurezza internazionale presso il *King College London e Defence Accademy of the UK*
- Dott.ssa Cristina FONTANELLI, dottoranda in *Security and Strategic Studies* presso l'Università di Genova e collaboratrice presso il LAPS- Laboratorio Analisi Politiche e Sociali

Area Ricerca

- Ing. Alessandro ZACCHEI – membro del Comitato Tecnico Scientifico del CESMA (Centro Militare Studi Aeronautici "Giulio Douhet") per lo studio di applicazioni di *artificial intelligence dual use*; Ricercatore Ce.Mi.S.S.
- Dott. Pierluigi BARBERINI, CeSI - Centro Studi Internazionali, analista del *Desk* Difesa & Sicurezza
- Dott. Danilo MATTERA TRIMONTI, studente magistrale "Pace, guerra e Sicurezza" Università degli Studi Roma Tre; collaboratore Geopolitica.info e IARI – Istituto Analisi Relazioni Internazionali
- Dott.ssa Michela DI FRANCESCANTONIO, esperta in sicurezza economica, geopolitica ed *intelligence*

BIBLIOGRAFIA

Pubblicazioni Nazionali

- STATO MAGGIORE DIFESA, Il Concetto Strategico del Capo di Stato Maggiore della Difesa "Efficienza sistemica, rilevanza complessiva" (2020)
- STATO MAGGIORE DIFESA, Concetto Scenari Futuri (2021)
- STATO MAGGIORE ESERCITO, "*Multi-Domain Operations,* Approccio Concettuale" (2020)
- STATO MAGGIORE ESERCITO, Nota Dottrinale "Le Operazioni Multidominio" (2021)
- Ce.Mi.S.S., Ricerca AP-SMA-03 "Prospettive del ruolo del Potere Aereo e Spaziale sulle sfide poste dalle future operazioni multidominio", Ing. Alessandro ZACCHEI (2018)
- "La dottrina Gerasimov e la filosofia della guerra non convenzionale nella strategia russa contemporanea", Libellula Edizioni - Nicola CRISTADORO, (2018).

Pubblicazioni NATO

- NATO *Warfighting Capstone Concept* (NWCC), (2020)
- NATO *Allied Joint Publication* (AJP-01-F) "*Allied Joint Doctrine*" (*draft*).
- NATO INNOVATION HUB "*Cognitive Warfare*" (2020).
- NATO Cooperative *Cyber* Defence Centre of Excellence (CCDCOE), "*Cyber Threats to NATO from a Multi-Domain Perspective*" (2020)
- NATO *Joint Air Power Copetence Centr* (JAPCC) "*Shaping NATO for Multi-Domain Operations of the future*" (2019)
- NATO *Combined Joint Operations form the Sea Centre of Excellence* (CJOSCOE "*Study on Multi-Domain Operations in the Maritime Domain*" (2021)

Pubblicazioni UE

- UE *Hybrid Centre of Excellence* (CoE), "*The Landscape of Hybrid Threats: a concpetual model public version*" (2021)
- UE *European External Action Service* (EEAS), " *EU Guidance on countering Hybrid threats during the planning phase of EU-led CSDP military operations and missions*" (*draft*)

Pubblicazioni Estere

- *Multinational Capability Development Campaign* (MCDC) "*Countering Hybrid Warfare*" (2019)
- US *Army Training and Doctrine Command* (TRADOC), *Pamphlet* 525-3-1 "*The U.S. Army in Multi-Domain Operations* 2028" (2018)
- UK MoD, *Development, Concepts and Doctrine Centre*(DCDC) *Joint Concept Note 1/20 "Multi-Domain Integration"* (2020)
- UK MoD, *Development, Concepts and Doctrine Centre* (DCDC), *Joint Concept Note* 2/17 "*Future of Command and Control*" (2017)
- *French Joint Centre for Concepts, Doctrine and Experimentations* (CICDE), *Joint Concept* 0.1.1 "*Multimilieux et multichamps (M2MC), la vision française interarmées*" (2021)

Articoli accademici e sitografia

- http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf
- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2774761
- http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm
- https://cryptome.org/2014/06/prc-three-wars.pdf
- https://warontherocks.com/2018/01/chinas-three-warfares-perspective/
- https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/CASI%20Articles/2020-06-30%20Chinese%20Views%20of%20All-Domain%20Operations.pdf?ver=0gVa73tTs6oxBmMIQnTYxg%3D%3D
- https://www.smh.com.au/politics/federal/us-unsettled-by-chinas-three-warfares-strategy-pentagon-report-20140410-36g45.html
- https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF


VNA VIS