



CENTRO ALTI STUDI
PER LA DIFESA



ISTITUTO DI RICERCA E
ANALISI DELLA DIFESA

Pietro Batacchi

Potere Aerospaziale e Distributed Command and Control (C2): un nuovo approccio alle operazioni aeree nel contesto delle Multi Domain Operations (MDO)

(Codice AR-SMA-01)





ISTITUTO DI RICERCA E ANALISI DELLA DIFESA

L'Istituto di Ricerca e Analisi della Difesa (di seguito IRAD), per le esigenze del Ministero della Difesa, è responsabile di svolgere e coordinare attività di ricerca, alta formazione e analisi a carattere strategico sui fenomeni di natura politica, economica, sociale, culturale, militare e sull'effetto dell'introduzione di nuove tecnologie che determinano apprezzabili cambiamenti dello scenario di difesa e sicurezza, contribuendo allo sviluppo della cultura e della conoscenza a favore della collettività e dell'interesse nazionale.

L'IRAD, su indicazioni del Ministro della Difesa, svolge attività di ricerca in accordo con la disciplina di Valutazione della Qualità della Ricerca e sulla base della Programma nazionale per la ricerca, sviluppandone le tematiche in coordinamento con la Direzione di Alta Formazione e Ricerca del CASD.

L'Istituto provvede all'attivazione e al supporto di dottorati di ricerca e contribuisce alle attività di Alta Formazione del CASD nelle materie d'interesse relative alle aree: Sviluppo Organizzativo; Strategia globale e sicurezza/Scienze Strategiche; Innovazione, dimensione digitale, tecnologie e cyber security; Giuridica.

L'Istituto opera in coordinamento con altri organismi della Difesa e in consorzio con Università, imprese e industria del settore difesa e sicurezza; inoltre, agisce in sinergia con le realtà pubbliche e private, in Italia e all'estero, che operano nel campo della ricerca scientifica, dell'analisi e dello studio.

L'Istituto, avvalendosi del supporto consultivo del Comitato scientifico, è responsabile della programmazione, consulenza e supervisione scientifica delle attività accademiche, di ricerca e pubblicistiche.

L'IRAD si avvale altresì per le attività d'istituto di personale qualificato "ricercatore della Difesa, oltre a ricercatori a contratto e assistenti di ricerca, dottorandi e ricercatori post-dottorato.

L'IRAD, situato presso Palazzo Salviati a Roma, è posto alle dipendenze del Presidente del CASD ed è retto da un Ufficiale Generale di Brigata o grado equivalente che svolge il ruolo di Direttore.

Il Ministro della Difesa, sentiti il Capo di Stato Maggiore della Difesa, d'intesa con il Segretario Generale della Difesa/Direttore Nazionale degli Armamenti, per gli argomenti di rispettivo interesse, emana le direttive in merito alle attività di ricerca strategica, stabilendo le linee guida per l'attività di analisi e di collaborazione con le istituzioni omologhe e definendo i temi di studio da assegnare all'IRAD.

I ricercatori sono lasciati liberi di esprimere il proprio pensiero sugli argomenti trattati: il contenuto degli studi pubblicati riflette quindi esclusivamente il pensiero dei singoli autori e non quello del Ministero della Difesa né delle eventuali Istituzioni militari e/o civili alle quali i Ricercatori stessi appartengono.



**CENTRO ALTI STUDI
PER LA DIFESA**



**ISTITUTO DI RICERCA E
ANALISI DELLA DIFESA**

Pietro Batacchi

Potere Aerospaziale e Distributed Command and Control (C2): un nuovo approccio alle operazioni aeree nel contesto delle Multi Domain Operations (MDO)

(Codice AR-SMA-01)

“Potere Aerospaziale e Distributed Command and Control (C2): un nuovo approccio alle operazioni aeree nel contesto delle Multi Domain Operations (MDO)”



NOTA DI SALVAGUARDIA

Quanto contenuto in questo volume riflette esclusivamente il pensiero dell'autore, e non quello del Ministero della Difesa né delle eventuali Istituzioni militari e/o civili alle quali l'autore stesso appartiene.

NOTE

Le analisi sono sviluppate utilizzando informazioni disponibili su fonti aperte.

Questo volume è stato curato dall'**Ufficio Studi, Analisi e Innovazione dell'IRAD.**

Direttore

Col. c. (li) s. SM Gualtiero Iacono

Capo dell'Ufficio Studi, Analisi e Innovazione

Col. AArn Pil. Loris Tabacchi

Progetto grafico

**1° Mar. Massimo Lanfranco – C° 2ª cl. Gianluca Bisanti – Serg. Manuel Santaniello -
Ass. Amm. Massimo Bilotta**

Revisione e coordinamento

**Ten. Col. Luigi Bruschi – S.Ten. Elena Picchi – Funz. Amm. Aurora Buttinelli - Ass.
Amm. Anna Rita Marra**

Autore

Pietro Batacchi

Stampato dalla Tipografia del **Centro Alti Studi per la Difesa**

Istituto di Ricerca e Analisi della Difesa

Ufficio Studi, Analisi e Innovazione

Palazzo Salviati

Piazza della Rovere, 83 - 00165 – Roma

tel. 06 4691 3205

e-mail: irad.usai.capo@casd.difesa.it

chiusa a ottobre 2022

ISBN 979-12-5515-038-1

INDICE

SOMMARIO	6
ABSTRACT	8
CAPITOLO 1	10
Lo scenario politico-strategico di riferimento	10
CAPITOLO 2	19
Analisi ed evoluzione dottrinale del Comando e Controllo (C2)	19
CAPITOLO 3	32
Verso un nuovo C2 distribuito	32
CAPITOLO 4	45
La rilevanza strategica della componente aerospaziale nelle multi-domain operations	45
CAPITOLO 5	60
Nuove tecnologie e sensori di 5 ^a Generazione nel C2 distribuito	60
CONCLUSIONI	73
BIBLIOGRAFIA	75
Nota sull'IRAD e Nota sull'Autore	79

SOMMARIO

Il presente studio ha lo scopo di analizzare e valutare i possibili nuovi approcci alle operazioni aeree ed al comando e controllo nel contesto delle *multi-domain operations*.

Siamo partiti, dunque, con un esame approfondito degli scenari internazionali e, in particolare, di quello che abbiamo chiamato “scenario multipolare plurilivello”. Si tratta di uno scenario caratterizzato dalla presenza di un numero sempre maggiore di attori rilevanti, ovvero di attori, statuali e non statuali, capaci di incidere in maniera empiricamente apprezzabile sulle dinamiche internazionali, e dalla presenza di dimensioni di interazione che si intersecano a diversi livelli. Il risultato è un sistema molto complesso e super-competitivo, perfettamente descritto dal concetto del *continuum* competizione-crisi-guerra. Nel Cap.2, si è passati all’analisi dell’evoluzione dottrinale del comando e controllo, partendo dal generale concetto di C2 nelle operazioni militari nella sua definizione più elementare, ovvero di C2 inteso come esercizio del comando e della direzione delle truppe da parte di un Comandante designato. Sulla base di ciò abbiamo poi cercato di delineare l’evoluzione del C2 a partire dalla Rivoluzione negli Affari Militari proseguendo poi fino ai nostri giorni, contraddistinti dalla nuova dottrina delle operazioni multi-dominio, e soffermandoci sul comando e controllo nelle operazioni aeree. In particolare, già a partire da questo capitolo, abbiamo fissato il concetto di un C2 nel cui ambito diventa indispensabile avere la capacità di elaborare ed analizzare un’enorme mole di informazioni e delegare maggiori responsabilità ai livelli subordinati, affidandosi all’autonomia delle pedine sul campo e dando anche alle unità più elementari responsabilità e capacità prima impensabili.

Questo concetto è stato “esploso” nel Cap.3 dove l’analisi si è focalizzata sulla descrizione di un nuovo modello di comando e controllo basato sul principio del controllo distribuito e dell’esecuzione decentrata/periferica, e da un punto di vista organizzativo su una struttura orizzontale dinamica e adattiva, tenuta assieme da un livello intermedio dotato di un’intelligenza e di una consapevolezza informativa senza precedenti. Il capitolo viene concluso da un esame dettagliato riguardante l’esperienza americana ed i programmi ABMS e SKYBORG.

Il Cap.4 è invece dedicato all’approfondimento del concetto di operazione multi-dominio ed alla rilevanza che all’interno di essa riveste la componente aerea. In quest’ottica abbiamo preso in esame tre casi di studio: il primo, dedicato all’F-35 come *battle manager*, il secondo, dedicato al programma NATO AFSC, ed il terzo, ai programmi per i sistemi di combattimento aereo del futuro basati sui caccia di sesta generazione.

Infine, nel Cap.5 abbiamo affrontato la grande questione degli abilitanti tecnologici che devono garantire che le nuove dottrine e i nuovi concetti operativi si traducano in pratica. Ci siamo, dunque, soffermati su intelligenza artificiale, super calcolo, ecc., cercando di delinearne lo stato dell'arte attuale e le prospettive in campo militare.

ABSTRACT

This study aims to evaluate possible new approaches to air operations and command and control in the context of multi-domain operations. We started, therefore, with an in-depth overview of international scenarios and, in particular, of what we have called the multi-polar/multi-domain scenario. This is a scenario characterized by the presence of an increasing number of relevant actors - i.e. actors, both state and non-state - capable of affecting international dynamics in an empirically appreciable manner, and by the presence of intersecting dimensions of interaction at different levels. The result is a highly complex and super-competitive system, perfectly described by the concept of the competition-crisis-war continuum.

In Chapter 2, we moved on to an analysis of the doctrinal evolution of command and control, starting with the general concept of C2 in military operations in its most basic definition: C2 as the exercise of command and direction of troops by a designated commander. Based on that, we then tried to outline the evolution of C2 starting with the Revolution in Military Affairs and continuing to the present day, marked by the new doctrine of multi-domain operations, and focusing on command and control in air operations. In particular, already in this chapter, we have “fixed” the concept of a C2 within it becomes essential to have the capacity to process and analyze a huge amount of information and delegate more responsibility to subordinate levels, relying on the autonomy of the units in the field and giving even the most basic of them previously unthinkable responsibilities and capabilities.

This concept was detailed and deepened in Chapter 3, where the analysis was focused on the description of a new command and control model based on the principle of distributed control and decentralized/peripheral execution, and, from an organizational point of view, on a dynamic and adaptive horizontal structure, held together by a middle level endowed with unprecedented intelligence and information awareness.

The chapter ends with a detailed examination of the American experience and the ABMS and SKYBORG programs.

Chapter 4 deals with an in-depth examination of the concept of multi-domain operations and, within it, the relevance of the air component. With this in mind, we have made three case studies: the first, concerning the F-35 as battle manager, the second, concerning the NATO AFSC program, and the third, concerning the future air combat systems based on sixth-generation fighters.

Finally, in Chapter 5, we addressed the technological enablers that have to allow the new doctrines and operational concepts to translate into practice. We therefore dwelt on artificial intelligence, supercomputing, etc., trying to outline their current state and prospects in the military field.

CAPITOLO 1

Lo scenario politico-strategico di riferimento

1.1 Il ritorno della logica di potenza

Il nuovo scenario geopolitico globale è caratterizzato da una configurazione che definiremmo multipolare plurilivello, con poli rilevanti non tutti della stessa natura. Vedremo poi se l'esito della Guerra in Ucraina – guerra destinata ad incidere profondamente sull'ordine internazionale – accentuerà o meno tale caratterizzazione. Secondo autorevoli analisi, infatti, i costi dell'invasione della Guerra in Ucraina nel complesso saranno talmente alti, che, qualunque sia il suo esito, la Russia ne uscirà talmente indebolita da farla retrocedere dal rango attuale, quello di superpotenza, al rango di potenza regionale. Non solo, ma l'allargamento della NATO, con la relativa crescita dell'influenza americana – conseguenze “non volute” della scelta fatta da Putin il 24 febbraio 2022 – sempre secondo il medesimo filone di pensiero, sarebbe un'altra delle cause che potrebbe accentuare il processo di “declassamento” della Russia e quindi una variazione sistemica rilevante.

Secondo un'altra scuola di pensiero – di cui fa parte lo Scrivente – è ancor un po' troppo presto per capire quali potranno essere le conseguenze sulla Russia del suo sforzo bellico in Ucraina e se, veramente, per effetto di questo, nei prossimi anni assisteremo ad un processo di declassamento sistemico di Mosca. Certamente, nell'equazione vanno inseriti anche quei fondamentali che da sempre caratterizzano la Russia - la disponibilità di materie prime e risorse naturali, la profondità strategica, un'industria militare sostanzialmente autonoma e così via – e che continueranno a caratterizzarla nel prossimo futuro. Basti pensare che la Guerra, che incide indirettamente sull'economia russa attraverso le sanzioni, non scalfisce l'industria militare di Mosca, sostanzialmente autonoma da Europa e Occidente, né intacca più di tanto le materie prime, per le quali sono stati prontamente individuati nuovi mercati di sbocco¹, in alternativa a quello europeo.

Ciò detto, partiamo con il nostro esame dal primo livello di questo nuovo sistema multipolare, ovvero quello delle tre super-potenze: USA, Cina e Russia.

Gli USA mantengono la loro posizione predominante, una sorta di *primus inter pares*, in particolare in campo militare con un *budget* per la Difesa che ha raggiunto gli 800 miliardi di dollari - e che potrebbe crescere ancora sull'onda della Guerra in Ucraina e delle sue conseguenze - ovvero una cifra quasi 4 volte superiore a quella del *budget* cinese e 8-10 volte superiore a quella del *budget* russo. Dentro questi numeri c'è poi l'incontrastata

1 Peraltro con gli alti prezzi di petrolio e gas, Mosca finanzia tranquillamente il proprio sforzo bellico in Ucraina.

leadership in alcuni settori strategici - bassa rilevabilità, elettronica/avionica, portaerei, ecc. - che ne qualificano un primato inarrivabile per i Russi ed ancora molto distante per i Cinesi. A ciò bisogna aggiungere una rete globale di influenza e *partnership*, con un posizionamento strategico con il quale poter garantire una capacità di risposta immediata e di proiezione praticamente in ogni scacchiere del globo, prevenendo o rispondendo rapidamente ad ogni possibile contingenza. Per quanto riguarda la Cina, stiamo parlando del vero concorrente dell'America sul piano globale e di un Paese che nell'ultimo ventennio ha sperimentato uno straordinario, quanto unico, processo di crescita economica e industriale – basato su un modello articolato su un *mix* tra iniziativa privata individuale, grande capitale pubblico e privato, e ferreo monopolio sul piano politico del Partito Comunista Cinese – accompagnato da un altrettanto straordinario processo di ammodernamento dello strumento militare. La modernizzazione delle Forze Armate cinesi non ha trascurato nessun settore, ma ha riguardato soprattutto il comparto strategico-missilistico, aeronautico e navale. In campo navale, per esempio, sono assolutamente da rimarcare i progressi compiuti nel settore delle grandi unità di superficie (DDG Type 52C e Type 52D, e incrociatori Type 55), con numeri in termini di acquisizione superiori addirittura a quelli americani, e nel settore dello strumento portaerei, creato letteralmente da zero in 15 anni, e basato oggi sulle prime due portaerei STOBAR, LIAONING e SHANDONG, a cui si aggiunge la prima unità di concezione interamente nazionale di tipo CATOBAR con catapulte elettromagnetiche, la Type 003 Fujian. Ma non dimentichiamo neppure la corsa in campo subacqueo che oggi ha portato la Marina Cinese ad avere in servizio più di 100 tra sottomarini a propulsione nucleare e convenzionale. In campo missilistico come non citare i progressi compiuti nell'ipersonico con lo sviluppo e la realizzazione di sistemi come il DF-17 o nel campo dei missili da crociera e antinave – prodotti in migliaia di esemplari – con le ultime evoluzioni quali, per esempio, il supersonico pesante YJ-12. Pechino ha dunque compiuto progressi notevoli, mentre l'industria militare è andata accentuando la sua indipendenza rispetto alla tradizionale assistenza russa, con un'ulteriore accelerazione negli ultimi 5 anni dovuta ai grandi investimenti in tecnologie disruptive quali il super calcolo, l'intelligenza artificiale, i sistemi di comunicazione, l'ISR e così via.

Venendo alla Russia, buona parte del suo percorso futuro come si diceva dipenderà dall'esito della Guerra in Ucraina, ma è chiaro che si tratta di un Paese che, dopo la grave crisi degli anni '90, ha lentamente recuperato una parte del suo peso e della sua influenza sulla scena internazionale tanto nel cosiddetto "estero vicino"² quanto in altri scacchieri, a cominciare dal Medioriente dove, grazie all'intervento in Siria iniziato nel 2015 ed

2 L'Ucraina è per l'appunto centrale in questo estero vicino.

all'impegno in Libia, Mosca è tornata protagonista. A ciò bisogna aggiungere la sempre più evidente penetrazione strategica in Africa con gli accordi per l'apertura di una base navale in Sudan, l'utilizzo di consiglieri e *contractors* in Repubblica Centrafricana, ma anche in altri Paesi (Mozambico, Madagascar), senza dimenticare il Mali, dove Mosca si è in pratica sostituita a Parigi come tradizionale punto di riferimento.

In campo militare, la Russia, pur essendo condizionata da evidenti vincoli di bilancio, in parte alla base della *performance* certo non esaltante dello strumento convenzionale in Ucraina, ha mantenuto una sostanziale parità strategica con gli USA. E questo spiega – unitamente alla disponibilità di risorse strategiche, alla capacità di condizionare economie e mercati, ad una profondità strategica senza eguali ed alla *membership* permanente in Consiglio di Sicurezza dell'ONU - perché la si può considerare ancora oggi una superpotenza.

Più di ogni altra cosa, Mosca ha saputo sviluppare e perseguire una strategia chiara e coerente, che ha nella cosiddetta zona grigia il suo campo di espressione di elezione, ma che, come nel caso dell'Ucraina, può esprimersi pure mediante il ricorso diretto alla forza quando sono in gioco interessi ritenuti vitali.

Il secondo livello del sistema è composto da grandi potenze globali, ad oggi rappresentate essenzialmente dal Regno Unito, a maggior ragione alla luce della formulazione della strategia della Global Britain, e dalla Francia. Questi attori sono più o meno caratterizzati dai seguenti fondamentali di potenza: 1. Un'economia sofisticata 2. Il deterrente nucleare 3. La *membership* permanente nel Consiglio di Sicurezza dell'ONU 4. Una tradizione imperiale e coloniale, dunque un'abitudine a pensare e comportarsi in un certo modo 5. La *membership* nel G7.

Il terzo livello è composto da un novero di medie potenze globali. Si tratta di Paesi – Italia, Germania, Giappone - con economie sofisticate e proiezione commerciale globale, membri del G7 - ma anche di Paesi come Israele, dotati dell'arma nucleare e di un'enorme capacità di condizionamento delle politiche di difesa e sicurezza di altri soggetti, a cominciare dagli Stati Uniti.

Un quarto livello è composto da medie potenze regionali nucleari, ovvero da Paesi quali India, Pakistan e Corea del Nord. Quest'ultima ha ormai uno *status* nucleare acquisito - con un numero di testate stimabile in 20-30 esemplari, a cui si aggiunge una collaudata *expertise* in campo balistico³. Nel caso di India e Pakistan lo *status* nucleare, acquisto tra gli anni ottanta e novanta, è oggi maturato fino ad abbracciare una capacità di *second strike* basata su armi nucleari (balistiche e da crociera) lanciabili da sottomarini. In sostanza, si tratta di

3 Capacità, peraltro, esportata in Siria e Pakistan, e che sta giungendo a maturazione pure nel settore dei missili a raggio intermedio e intercontinentali.

Paesi che hanno la possibilità di sostenere le loro politiche regionali con la minaccia di uso o con l'uso dell'arsenale nucleare: possiamo dunque considerarle anche come potenze regionali "rafforzate". Un quinto livello, infine, comprende le potenze regionali *tout-court*, ovvero Paesi capaci di incidere sulle dinamiche internazionali al loro livello (appunto, quello regionale) esercitando influenza e capacità di interdizione/condizionamento. Tale categoria annovera attori quali Iran, Brasile, Sudafrica, Arabia Saudita, Corea del Sud, Turchia, Egitto, ma pure, aggiungiamo, gli Emirati Arabi Uniti. Il caso degli EAU può essere considerato di scuola visto che stiamo parlando di un Paese che 40 anni "non esisteva", o quasi, e che, invece, negli ultimi anni è stato capace di proiettare la propria influenza in tutto il "grande Medioriente" – dalla Libia, allo Yemen passando per la Siria – capitalizzando le proprie enormi risorse economiche e mettendole a sistema con rapporti internazionali trasversali. Un attivismo culminato con gli Accordi Abramo con Israele che hanno portato alla formalizzazione di una *partnership* – che sotto banco andava avanti da anni – che ha profonde implicazioni sul piano tanto commerciale quanto strategico-militare. E poi, quando si parla di medie potenze regionali, non si possono non dedicare due parole di approfondimento ad Iran e Turchia. Il primo ha creato negli ultimi anni uno spazio geopolitico sotto la propria influenza che parte da Teheran e arriva fino al Mediterraneo Orientale ed al Libano, passando per Iraq e Siria senza soluzione di continuità – la cosiddetta "mezzaluna sciita" – e che ha una propaggine pure più a sud fino allo Yemen ed al Corno d'Africa. In quest'area, Teheran è in grado di condizionare governi, muovere *lobby* e gruppi politici, ma, soprattutto, di manovrare - finanziando, inquadrando, armando e supportando – una galassia di proxy che comprende gli Hezbollah libanesi, le milizie sciite siro-irachene, i ribelli Houthi in Yemen, ecc. L'utilizzo del proxy è centrale nella strategia ibrida iraniana e Theran ha investito molto negli ultimi 10-15 anni in questa direzione fornendo ai propri clienti non solo equipaggiamento militare, addestramento, inquadramento e supporto finanziario, ma pure la capacità di produrre *in house* certi sistemi d'arma – razzi, droni, ecc.

La Turchia ha dal canto suo abbracciato una politica sempre più autonoma ed assertiva basata sull'appoggio a tutte le realtà ed i gruppi che in Medioriente si ispirano alla Fratellanza Musulmana, sulla creazione di aree di influenza/cuscinetto in Siria, sul raggiungimento dell'autosufficienza energetica, sulla proiezione di potenza nel Mediterraneo Centrale e in Libia, così come in Asia Centrale, ecc. L'obiettivo di fondo di Ankara è creare/consolidare uno spazio geopolitico sotto la propria influenza guadagnando profondità strategica e spazi di azione autonomi, fuori dalla tradizionale appartenenza ad organizzazioni quali la NATO.

Questi 5 livelli, imperniati sulla dimensione e sul ruolo quali attori centrali degli Stati, sono intersecati da un'ulteriore dimensione, ovvero dalla dimensione che attiene agli attori non statuali. In questa categoria rientrano organizzazioni che impiegano per i loro fini - di carattere politico/simbolico o economico/personalistico – risorse coercitive (militari e non) non legittime⁴: gruppi terroristici, criminal/mafiosi, organizzazioni guerrigliere, ecc. Prendiamo, per esempio, i grandi cartelli della droga o organizzazioni malavitose straordinariamente potenti come la 'Ndrangheta, capaci di condizionare amministrazioni locali e governi e di farlo utilizzando sia metodi violenti e coercitivi, sia mezzi più subdoli arrivando a mescolarsi/identificarsi con gli stessi apparati legittimi⁵. Il dato, se vogliamo nuovo, è che si tratta di realtà sempre più forti e dotate di risorse economiche e militari significative, in alcuni casi superiori persino a quelle degli Stati, in grado di incidere in maniera empiricamente apprezzabile sulle dinamiche internazionali. Questi gruppi traggono vantaggio da tutta una serie di fattori, che riassumiamo di seguito:

1. La progressiva erosione della statualità in diverse aree del pianeta - soprattutto in Medio Oriente e Africa – dove il numero di Stati falliti, in via di fallimento o di Stati semplicemente incapaci di esercitare le proprie prerogative sui rispettivi territori sta osservando un *trend* di crescita.
2. I processi di diffusione orizzontale di determinate tecnologie. Tale processo fa sì che alcune tecnologie, in particolar modo militari, prima disponibili solo per le organizzazioni statali oggi lo siano anche per gruppi e realtà irregolari. Si pensi ai droni, a razzi e missili sempre più sofisticati, a sistemi di guerra elettronica e così via.
3. Il sempre più diffuso utilizzo di strategie ibride/grigie da parte degli Stati che, dunque, hanno tutto l'interesse a far crescere e potenziare per i loro usi proxi e realtà non statuali.

1.2 Il *continuum* competizione, zona grigia, guerra

Come appare evidente da quanto esaminato nel precedente paragrafo, rispetto anche solo a 20 anni fa, il numero di attori in grado di incidere sulle dinamiche internazionali è cresciuto notevolmente. Questo ha inevitabilmente portato ad un radicale cambiamento nella distribuzione del potere a livello internazionale ed alla creazione di un sistema internazionale con una struttura sostanzialmente piramidale. A ciò bisogna aggiungere la

4 Nella prima categoria rientrano organizzazioni che mirano al raggiungimento di obiettivi a carattere politico, definiti nell'ambito di piattaforme ideologiche, etniche o religiose, e questo le differenzia dalle organizzazioni della seconda categoria, ovvero da organizzazioni criminali e/o malavitose che si muovono senza alcun rimando ad ideologie, sistemi di valori o a professioni religiose e che perseguono interessi particolari di carattere economico-criminale e personalistico.

5 Non a caso si parla di 'Ndrangheta dei colletti bianchi.

decisa crescita della popolazione mondiale negli ultimi 40-50 anni. Un *trend* che ha significato contestualmente pure la crescita del numero di persone con bisogni strutturati. Allo stesso tempo, le risorse per soddisfare una maggiore richiesta di benessere, servizi e assistenza sono sempre più o meno le stesse. Certo, grazie a sintetizzazione chimica e energie rinnovabili, una parte dei nuovi bisogni potrà essere soddisfatta, ma nel complesso ci troviamo in una situazione in cui l'equilibrio tra domanda e offerta è sempre più precario, e questo non fa che aumentare la competizione e le potenziali fonti di conflitto. Lo abbiamo visto, di recente, con la competizione per le risorse energetiche nel Mediterraneo Orientale o in Asia-Pacifico, senza dimenticare ciò che sta accadendo in Africa con la rincorsa alle terre rare.

L'intersecarsi di tutte queste dimensioni, dunque, porta ad un sistema internazionale sempre più e sempre meglio descritto dall'immagine di un *continuum* conflittuale tra una fase di assenza di guerra, ma di super-competizione, una fase di crisi – o grigia – e una fase di conflitto aperto/guerra.

La prima fase rappresenta oggi la normalità della vita internazionale. Un *new normal* contraddistinto da assenza di conflittualità, certo, ma da una super competizione che spazia dal campo economico-finanziario a quello tecnologico, per finire al settore dell'immagine e della comunicazione. In questa competizione ci si affronta a colpi di embarghi, dazi, *dumping*, manipolazione dei debiti sovrani, ecc., senza dimenticare lo sfruttamento sfrenato delle risorse del mare e della terra⁶. E poi c'è la competizione tecnologica che avviene tramite spionaggio industriale, concorrenza sleale ed alti investimenti in ricerca e sviluppo in settori disruptive: intelligenza artificiale e *machine learning*, *block chain*, realtà aumentata, comunicazioni di nuova generazione, robotica e sistemi autonomi, *cloud*, super calcolo, ecc. Probabilmente, ad oggi e presumibilmente ancor di più nel prossimo decennio, la competizione tecnologica sarà cruciale per capire quali saranno gli attori che avranno successo e che saranno capaci di mantenere la loro posizione nella piramide o accrescerla o, al contrario, perderla per mancanza di una strategia sistemica orientata alla vittoria.

Infine, la competizione sulle "immagini" e la loro manipolazione, con la creazione di narrazioni, la conduzione di campagne di disinformazione, la manipolazione del Web, l'utilizzo dei *social media* e così via.

In definitiva, per ogni attore nella super-competizione, l'obiettivo principale è migliorare, o mantenere, il proprio posizionamento relativo e il proprio vantaggio competitivo sia verso gli avversari sia verso gli alleati. In un mondo sempre più dinamico, complesso e insicuro, difatti, essere più competitivi significa poter rispondere in maniera adeguata a bisogni

6 Gas naturale e terre rare soprattutto.

strutturati crescenti, estraendo le risorse dal sistema, trasformandole e distribuendole ad una platea sempre più ampia di utenti/cittadini, negoziando da posizioni di vantaggio nei grandi accordi internazionali (dal clima, al cibo, passando per l'energia o il disarmo), ecc., ma pure posizionandosi meglio in vista di crisi e conflitti.

In questo contesto lo strumento militare assume una rinnovata rilevanza come strumento deterrente. Anzi, possiamo senz'altro dire che proprio con il mondo super-competitivo la deterrenza è tornata di attualità trovando una nuova centralità nel "discorso" strategico. E questo banalmente perché, a fronte di nuove e più sofisticate minacce, di una complessiva incertezza e insicurezza di fondo, è necessario avere la forza per dissuadere eventuali iniziative ostili da parte dell'avversario, sia che queste abbiano la forma dell'aggressione diretta sia che queste vengano condotte in quell'area grigia di cui parleremo a breve, e per evitare che dalla competizione si passi alla crisi o al confronto aperto su iniziativa dell'avversario⁷. Non solo la deterrenza torna centrale, ma si amplia anche il suo campo di applicazione secondo il concetto di deterrenza estesa, ovvero di una deterrenza estesa a contesti locali/periferici e capace di dissuadere iniziative "grigie" o di fatto compiuto o, ancora, aggressioni regionali su larga scala.

I cardini di questo concetto di deterrenza estesa sono due: l'uso del nucleare tattico ed il concetto di posizionamento avanzato e agile. Per quanto riguarda il primo aspetto, gli Americani, a partire dalla Nuclear Posture Review 2018, hanno rilanciato il concetto di deterrenza flessibile, ovvero di deterrenza capace di aumentare il *range* delle opzioni a disposizione. Gli obiettivi apertamente dichiarati di questa revisione del concetto di deterrenza da parte USA sono due: dissuadere un possibile impiego limitato di armi nucleari da parte degli avversari e dissuadere un'aggressione regionale. Per rendere credibile questa postura hanno installato sui missili balistici intercontinentali lanciabili da sottomarini la nuova testata a bassissimo potenziale (attorno ai 5 Kiloton) W-76-2. La testata è già operativa⁸. Pertanto, un sottomarino strategico classe Ohio potrà avere, caricate sui missili Trident II D5, oltre che le "normali" testate ad alto potenziale W-88 o W-76, anche la citata W-76-2. Dal canto loro, i Russi teorizzano apertamente l'uso dell'atomica tattica per arrestare un'eventuale penetrazione strategica avversaria con forze convenzionali: un modo per ri/equilibrare con l'arma atomica la schiacciante superiorità convenzionale NATO, dimostrata, non ultimo, anche dal conflitto in Ucraina.

7 Nello scenario attuale la scelta di quando iniziare un conflitto deve essere "nostra", perché ciò costituisce un vantaggio, ancor più importante che nella conflittualità classica.

8 La NPR dell'Amministrazione Biden, invece, ha cancellato la decisione della NPR 2018, ovvero dell'Amministrazione Trump, di sviluppare un nuovo missile da crociera lanciabile da sottomarini a testata nucleare.

Per quanto riguarda il secondo aspetto, con posizionamento avanzato delle forze intendiamo il posizionamento dinamico nei pressi di aree sensibili di contingenti piccoli, ovvero meno tracciabili/rilevabili, ma altamente letali e capacitivi. Gli Americani hanno coniato in tal senso il concetto di Forza Stand In e di ACE (Agile Combat Employment). Nel primo caso, si tratta di una forza, soprattutto dei Marines, dispiegata a contatto o dentro la WEZ (Weapon Engagement Zone) avversaria e dotata di capacità altamente letali (missili da crociera antinave, Naval Strike Missile, e dual capable, Tomahawk Block V, loitering munitions, missili a lungo raggio con capacità anche antinave⁹, ecc.). Il compito delle Stand In Force è segnalare l'indisponibilità ad accettare iniziative grigie/sotto soglia o di fatto compiuto, assicurare gli alleati più esposti, rispondere rapidamente all'iniziativa ostile, ecc. Nel secondo caso, invece, siamo di fronte ad un concetto coniato dall'USAF per un impiego flessibile delle forze - appunto, agile – teso a non dare riferimenti all'avversario e a ridurre tracciabilità e vulnerabilità. Funzionale a questo concetto, c'è un comando e controllo dinamico e scalabile verso il basso, ma pure la capacità e la possibilità di operare da siti e basi austere/improvvisate, aeroporti alternativi, con minima aderenza logistica e rotazioni brevi, continue e sistematiche. Insomma, un modo per aumentare i dilemmi dell'avversario e complicarne il ciclo di *targeting*.

Passiamo a questo punto all'esame della fase intermedia del *continuum*, dove troviamo almeno tre tipologie: diplomazia coercitiva, guerra ibrida e fatto compiuto.

Per "diplomazia coercitiva" si intende quella fattispecie in cui l'azione diplomatica è accompagnata, o meglio rafforzata, dalla minaccia di utilizzo della forza o dall'adozione di un limitato quantitativo di forza per costringere l'avversario ad attuare una condotta politica non desiderata. A volte la minaccia da sola può obbligare la controparte a modificare il proprio comportamento. In altri casi, invece, la minaccia non basta: bisogna allora utilizzare la forza, mantenendone l'applicazione ad un basso livello. Poca forza, infatti, significa anche maggiore forza a venire, in caso di mancata accondiscendenza, ovvero potere di arrecare un danno ulteriore: un messaggio all'avversario che in futuro potrebbe riservare costi ancor più alti di quelli già pagati. Vale la pena sottolineare – in particolare nell'ottica del presente studio - che il potere aereo è quello che fa maggiormente al caso della diplomazia coercitiva: è intrinsecamente più flessibile, più rapidamente dispiegabile e, dunque, quello maggiormente in grado di dare corso immediato alla minaccia graduando nel contempo l'intensità dell'azione di coercizione¹⁰.

9 In particolare il Precision Strike Missile dell'US Army, per il quale è in sviluppo anche una variante con seeker antinave.

10 Non solo, ma la minaccia risulta credibile soltanto se esiste uno strumento militare in grado di implementarla rapidamente. Sarebbe sostanzialmente inutile minacciare di utilizzare la forza se poi da un punto di vista logistico

La seconda tipologia, “guerra ibrida o sotto soglia”, può essere considerata un complesso di azioni – militari e non militari – il cui obiettivo è raggiungere lo scopo mascherando la propria responsabilità diretta dietro quel complesso di azioni ed evitare così la reazione sopra soglia dell’avversario o di una terza parte. In questi casi una potenza ostile si muove in un’area grigia – tra pace e guerra – ricorrendo ad azioni limitate che mantengono la pressione e puntano all’obiettivo senza sfociare in guerra aperta: azioni terroristiche, attacchi *cyber*, utilizzo di campagne di informazione/disinformazione, guerra elettronica, sabotaggi, ecc., ma pure utilizzo di *proxi*. I Russi hanno ampiamente utilizzato la guerra ibrida, con risultati rilevanti, tanto in Crimea quanto nel Donbass tra il 2014 ed il 2015.

Con “fatto compiuto”, invece, intendiamo un’azione militare diretta di entità circoscritta sotto la soglia del conflitto militare aperto. In questi casi non si vuole celare la propria responsabilità dietro l’azione, ma si vuole ottenere l’obiettivo con un’azione militare diretta estremamente rapida. Un’azione, cioè, che metta tutti di fronte ad un fatto compiuto sul terreno, reversibile solo al prezzo di un’*escalation* e di una guerra maggiore. In pratica chi utilizza il fatto compiuto punta tutto su velocità e tempistica, e sulla percezione che la reazione innescherebbe un conflitto più ampio, ovvero che il ristabilimento dello *status quo* avrebbe un costo di gran lunga superiore al beneficio¹¹.

La terza fase del *continuum* è quella della guerra aperta nell’ambito di uno scenario cosiddetto *peer-to-peer* o *near-peer*. Si tratta di conflitti armati su larga scala o di tipo regionale caratterizzati dai seguenti elementi:

- alta intensità;
- preponderanza dell’elemento tecnologico;
- operazioni multi-dominio;
- inquinamento informativo, *cyber* ed EW;
- possibilità di utilizzo dell’arma nucleare.

ed operativo i tempi di attuazione della minaccia fossero eccessivamente lunghi e condizionati dalla mobilitazione/dislocamento di grandi unità terrestri.

11 Questo potrebbe essere un paradigma per i prossimi anni, soprattutto in quei contesti, a cominciare dall’Asia-Pacifico, dove esistono miriadi di dispute per rivendicazioni territoriali o per diritti di sfruttamento energetici e dove ad un certo punto nella deterrenza estesa si potrebbero aprire dei gap sfruttabili con un’azione rapida e risolutiva. Insomma, è il mix tra super-competitività del sistema e territorializzazione/parcellizzazione delle risorse che potrebbe indurre in alcuni attori, che percepiscono lo status quo come svantaggioso, a rischiare il *fait accompli*.

CAPITOLO 2

Analisi ed evoluzione dottrinale del Comando e Controllo (C2)

2.1 Il comando e controllo nelle operazioni militari

Nella sua definizione più elementare, il C2 è l'esercizio del comando e della direzione sulle truppe assegnate ad un Comandante designato. Naturalmente la questione è molto più ampia e complessa: il primo e più importante elemento del C2 è proprio il personale. Uomini e donne che raccolgono informazioni, prendono decisioni, comunicano e cooperano per il raggiungimento di un obiettivo comune. Sono le persone che mandano avanti il C2 e che determinano il corso degli eventi, e il resto del "sistema" esiste soltanto per agevolare il loro lavoro.

In effetti tutta la guerra si riduce ad uno scontro fra le volontà contrapposte, e il concetto di C2 deve sempre tenere conto di questa fondamentale realtà: tutto il C2 serve non a diminuire il ruolo dell'uomo, ma proprio a consentire al personale di ottenere i maggiori risultati possibili. A tutti i livelli gerarchici, il comando e controllo esiste per sgretolare non solo e forse non tanto le possibilità materiali dell'avversario di continuare a lottare, ma la sua volontà di farlo.

Il comando e controllo non può quindi mai scindersi dalla *leadership*, dall'abilità di ispirare e spronare le forze amiche e trarre da ogni soldato il meglio che la sua personale natura può esprimere. Ovviamente ne consegue che ogni Comandante deve tener conto degli effetti della paura, delle privazioni, della fatica, di tutte le qualità intangibili e non misurabili meccanicamente che determinano la tenuta e le prestazioni dei reparti.

L'altro elemento chiave nel comando e controllo è rappresentato dalle informazioni: i Comandanti devono poter disporre di un'accurata rappresentazione della realtà sul campo, che deve poi essere analizzata e giudicata fino alla presa di decisioni che devono poi essere disseminate.

Indissolubilmente legato alle informazioni è il tempo: in battaglia, ogni informazione è solo un'immagine che descrive un periodo di tempo sfuggente. Un'informazione può essere preziosa in un momento ed inutile, o addirittura dannosa, in un altro.

Le informazioni sono essenziali per consentire ai Comandanti di prendere decisioni e sono altrettanto importanti nel consentire il coordinamento e la direzione delle operazioni una volta avviate.

Un piano ben congegnato si fonda sulle informazioni in entrambe le direzioni, poiché è importante che alle unità sotto-ordinate venga fornito un quadro situazionale, un'idea chiara

degli obiettivi contingenti e dell'immediato futuro, così che ai livelli più bassi ci si possa adattare all'evolvere della situazione locale senza allontanarsi dall'intento generale.

Il concetto di "informazione" è ampio e include ogni cosa: dai dati grezzi, come segnali intercettati e non processati, fino alla vera conoscenza che risulta dalla valutazione, elaborazione ed integrazione di dati utili.

Il Comandante fornisce informazioni ai sottoposti in allegato ai suoi ordini, e riceve *intelligence* sullo stato dell'avversario, rapporti sulla situazione delle forze amiche, dati sulla coordinazione fra vari reparti. Senza ricevere queste informazioni, nessun Comandante, quali che siano le proprie abilità personali, può dirigere efficacemente le operazioni. Allo stesso modo, uno *staff* di comando che non riesca a comunicare alle unità sul campo il concetto e l'intento dell'operazione non mette i suoi reparti nelle condizioni di agire efficacemente.

Moltissime informazioni che transitano da un posto di comando non sono importanti, e a volte neppure rilevanti. Molte non sono utilizzabili per limiti temporali. Molte sono inaccurate se non addirittura ingannevoli. Con l'aumentare del numero e della qualità dei sensori e dei sistemi di comunicazione che mettono, in teoria, anche il singolo soldato in prima linea in connessione diretta con comandi di alto livello, la quantità di dati e informazioni raccolta può diventare un'arma a doppio taglio, subissando i Comandanti con "rumore" che ne rallenta la capacità di decidere.

Serve quindi una struttura di supporto, ed una base tecnologica, che aiuti lo *staff* che crea, usa e ritrasmette informazioni. Le fondamenta del C2 sono l'organizzazione, le procedure, la dottrina, l'addestramento e soltanto in seguito "l'hardware".

Questo non significa che l'equipaggiamento non sia cruciale, tutt'altro. Lo è, inevitabilmente, in misura sempre maggiore, poiché i decisori hanno la necessità di accedere tempestivamente ad una moltitudine di informazioni diverse, provenienti da una vasta gamma di sensori e fonti. Dunque, essi hanno bisogno di sistemi di comunicazione capaci di operare anche in presenza di disturbi e attacchi *cyber*, e (sempre più) di computer e sistemi di analisi che li aiutino a processare e scremare l'enorme mole di dati in arrivo, comprimendo i tempi di reazione.

Proprio da questo requisito discende il sempre crescente interesse per l'intelligenza artificiale (AI), affiancata dal supercalcolo e da tecnologie quantistiche (concetti che verranno approfonditi in dettaglio nel Cap.5, e non è un caso che molteplici progetti in corso

vertano sullo sviluppo di sistemi a base AI che possano assistere gli umani nell'analisi dati e nel processo decisionale¹².

In tale contesto, meritano di essere segnalati i progressi significativi compiuti soprattutto in ambito navale, dove il principale *driver* di sviluppo è la minaccia rappresentata dai missili antinave super e ora anche iper-sonici, che lasciano alle unità tempi sempre più ridotti per la reazione. Nei Combat Management Systems di US Navy e Royal Navy stanno quindi trovando posto i primi cervelli artificiali capaci, in maniera *intelligence* e in tempo reale, di predire scenari strategici e tattici, fondendo e correlando informazioni provenienti da tutti i sensori imbarcati e da quelli esterni all'unità. Questi strumenti sfruttano l'istantanea multi-sensore della situazione per valutare la natura delle minacce e suggerire in tempi rapidissimi la miglior reazione e il miglior effetto da attivare, supportando quindi le decisioni degli ufficiali in comando.

L'US Navy sta quindi integrando algoritmi AI nell'architettura CANES (Consolidated Afloat Networks and Enterprise Services, già in servizio) per razionalizzare e discriminare le informazioni in ingresso, identificare e scremare "anomalie" (falsi segnali, disturbi, esche, ecc.) e assistere gli operatori nell'assunzione di decisioni cruciali, nonché proteggere meglio il tutto dalle minacce cibernetiche e potenziare il collegamento fra i CMS di unità navali di superficie e subacquee con comandi basati a terra e altri nodi tattici.

La Royal Navy ha testato, nel corso della FORMIDABLE SHIELD 2021, le architetture AI denominate STARTLE e SYCOIEA. STARTLE è un "operatore artificiale" che valuta continuamente la "picture" generata dai sensori di bordo, fornendo allerta precoce e suggerimenti tattici. STARTLE è in grado di riconoscere gli schemi comportamentali sfruttando processi di *deep learning* e consentendo agli utenti di migliorare la Maritime Domain Awareness per identificare, tracciare e ingaggiare i bersagli più subdoli¹³. SYCOIEA opera specificamente valutando le minacce e pianificando la reazione più appropriata con armi difensive, contromisure ed esche.

I CMS capaci di "apprendere" costantemente dai *feedback* ricevuti dall'ambiente circostante grazie all'AI possono anche assistere nella gestione della piattaforma e nella manutenzione preventiva. In diversi Paesi si sta dunque lavorando per integrare sistemi AI anche negli

12 Dai CMS di nuova generazione per unità di superficie e subacquee, ai sistemi di combattimento aereo del futuro basati sui caccia madre di sesta generazione.

13 Anche in Italia si sta lavorando alacremente in tale direzione. Per esempio, già oggi il CMS ATHENA per unità navali di superficie di Leonardo ATHENA si caratterizza innanzitutto per l'altissima velocità di calcolo e di distribuzione dati: oltre 30.000 transazioni al secondo, 5-6 volte in più dei sistemi concorrenti. Tuttavia, l'arrivo di nuove tecnologie come il supercalcolo e l'intelligenza artificiale (AI) comporteranno una crescita ulteriore, ma il sistema è già predisposto sin d'ora per ricevere ed ottimizzare queste rivoluzionarie capacità. ATHENA è infatti stato pensato fin dalla fase progettuale come scalabile verso l'alto, permettendo un ampliamento delle capacità ai fini dell'adattamento ad unità navali ancora più complesse o a tecnologie più disruptive. Giusto per fare un esempio, sarà possibile pure integrare una parte di software ad hoc per le operazioni multi-dominio.

IPMS, Integrated Platform Management System, come nel caso del progetto “Intelligent Ship” portato avanti dal Defence Science and Technology Laboratory britannico.

La quantità di dati che l’AI può valutare, in tempo reale, va molto al di là di quanto possa fare una mente umana. Il Comandante porta in dote creatività e flessibilità, ma l’AI è imbattibile nel calcolo e nella valutazione di una miriade di fattori tecnici. La manutenzione predittiva, applicata ai vettori nemici, può consentire all’AI di discriminare vari contatti e, magari, determinare che, per tipo e probabile *fuel fraction*, un drone identificato a maggiore distanza di un altro rappresenta, contro-intuitivamente, una maggiore minaccia.

In ambito aeronautico la capacità di autodiagnostica è ovviamente da molto tempo al centro dell’attenzione. Malgrado alcune delle capacità un tempo immaginate siano state rinviate per le difficoltà tecniche incontrate nello sviluppo, merita comunque menzione il livello di autodiagnostica e manutenzione predittiva che il sistema F-35 si ripropone di raggiungere, con velivoli che, ancora prima di atterrare, sono capaci di comunicare il loro stato allertando gli operatori sulle componenti da controllare o gli interventi da effettuare.

2.2 Dalla RMA alle operazioni multi-dominio

Nello studiare l’evoluzione delle tecniche belliche, i teorici individuano alcuni momenti chiave in cui nuove tecnologie, unite a innovativi concetti operativi e a nuove strutture organizzative, generano un radicale cambiamento nel modo di combattere una guerra. Possiamo facilmente identificare alcune di queste “Revolution in Military Affairs” (RMA), per esempio nell’avvento della meccanizzazione durante la Grande Guerra o nell’avvento degli armamenti nucleari e dei missili balistici, che hanno portato all’affermarsi dell’equazione della deterrenza, ovvero “non ti attacco perché la tua rappresaglia avrebbe un costo sproporzionato rispetto al beneficio ottenibile con il mio attacco”¹⁴. Dagli anni ‘70 in poi abbiamo assistito ad una rivoluzione più o meno strisciante con l’avvento dell’informatica e l’aumento delle capacità di calcolo dei computer, e con l’affermarsi progressivo delle armi “intelligenti” consacrate dalle operazioni contro l’Iraq nel 1991 e, ancora di più, nel 2003.

Prima però di alcune considerazioni sulle succitate operazioni in Iraq, conviene soffermarsi un attimo sul concetto di RMA. Quest’ultima la si può intendere come una trasformazione che consiste non solo nella disponibilità di mezzi e sistemi d’arma rivoluzionari, grazie all’utilizzo di tecnologie nuove, ma anche nell’adozione di strutture ordinarie e di dottrine operative che ottimizzino lo sfruttamento di tali nuove tecnologie, determinando capacità operative e strategiche qualitativamente diverse. Si può, dunque, considerare la Rivoluzione

14 In questo caso si parla di “deterrence by punishment”, mentre in altri di “deterrence by defence”, ovvero “non ti attacco perché la tua difesa mi imporrebbe un costo troppo alto o comunque superiore al beneficio ottenibile con l’attacco”.

negli Affari Militari, fermo restando l'orientamento dottrinale che deve garantire l'ottimizzazione delle nuove tecnologie, un nuovo modo di combattere contraddistinto dall'adozione sistematica, appunto dottrinariamente orientata, di tre grandi categorie di sistemi: i sistemi di *intelligence*, di comando e controllo e di ingaggio di precisione. Nella prima categoria rientrano i sistemi di *intelligence*, *surveillance* e *reconnaissance*, con i quali è possibile acquisire e mantenere una comprensione *near real-time* e ogni-tempo in un area geografica molto estesa e raggiungere il dominio nella conoscenza dello spazio di battaglia. Il secondo filone riguarda gli avanzati sistemi C4I (Command, Control, Communications, Computers e Intelligence), attraverso i quali la comprensione del campo di battaglia si traduce nella pianificazione delle missioni e nella successiva assegnazione al tipo di unità più adatta. L'ultimo aspetto riguarda il *precision-strike*, ovvero la capacità di localizzare bersagli mobili o fissi e distruggerli con un alto grado di confidenza, riducendo e contenendo i tempi di tutto il ciclo localizzazione-attacco. Queste tre componenti, precedentemente considerate e organizzate come autonome e indipendenti tra di loro, nella RMA tendono invece ad essere integrate al fine di rendere praticabili operazioni simultanee e sincronizzate su tutta la profondità del teatro di operazioni. Fin dall'inizio delle ostilità, l'obiettivo è per l'appunto coinvolgere il campo di battaglia in ogni singola parte della sua estensione.

L'operazione Enduring Freedom del 2003 contro l'Iraq di Saddam Hussein dimostrò definitivamente quanto l'arte della guerra sia stata cambiata dall'adozione di un modello operativo basato sull'altissima sincronizzazione delle operazioni, da un comando e controllo capace di garantire tale sincronizzazione a partire da pedine diffuse e distribuite su tutta la profondità del teatro e da un impiego di armamento di precisione senza precedenti. L'impatto delle armi guidate aveva in realtà iniziato a manifestarsi già molti anni prima, per esempio con la distruzione del famigerato ponte Dragon's Jaw di Thanh Hoa in Vietnam il 13 maggio 1972, quando 26 bombe a guida laser sganciate da un gruppo di F-4 PHANTOM portarono a termine quanto era stato impossibile ottenere negli anni precedenti: l'USAF e l'US Navy cercavano infatti di abbattere quel ponte fin dal 1965, ma 871 sortite e 11 aerei abbattuti non erano stati sufficienti.

In Desert Storm, nel 1991, l'impiego di armamenti guidati fu immediato, massiccio e decisivo, ma rappresentò ancora una percentuale molto bassa sul totale delle armi aereo-lanciate impiegate: 15.500 armi, per complessive 7.400 tonnellate, su un totale di 210.800 armi per 88.500 tonnellate totali, ovvero un misero 8,5%. Le analisi post-belliche ridimensionarono sensibilmente alcune dichiarazioni chiaramente propagandistiche che dipingevano le bombe a guida laser come una soluzione infallibile, *one-shot, one-kill*, anche

perché i designatori dell'epoca subivano ancora grosse limitazioni dovute alle condizioni meteo, ma i risultati complessivamente furono storici. La letalità del potere aereo, e degli *strike* a lungo raggio con missili cruise Tomahawk, si dimostrò efficace a livelli senza precedenti e consentì di contenere le perdite a livelli bassissimi: una media di 1,7 aerei persi o danneggiati ogni 1.000 attacchi. Desert Storm fu anche il debutto operativo della tecnologia *stealth* con l'impiego degli F-117, e la combinazione di precisione, furtività e sopravvivenza, garantita dalla capacità di ingaggio di precisione da quote medio-alte, ha segnato senza dubbio uno spartiacque nella storia della guerra.

Nel 2003, Iraqi Freedom non fece che confermare quelle lezioni, rincarando la dose: la percentuale di armi guidate impiegate salì al 68%, con 19.948 munizioni "intelligenti" impiegate contro 9.251 "stupide". L'operazione vide anche l'affermazione delle bombe a guida GPS JDAM, sviluppate proprio dopo l'esperienza del 1991. Pur non superando le affermate armi laser, le JDAM vi si avvicinarono a grandi passi, con 6.542 ordigni impiegati contro 8.618.

L'uso delle armi guidate è diventato sempre più centrale negli anni successivi, sia perché l'efficienza crescente lo rende vantaggioso, sia perché la precisione consente di ridurre i danni collaterali. Poche armi non guidate rimangono di uso comune oggi. La Royal Air Force britannica, per esempio, ha impiegato un'arma non guidata operativamente per l'ultima volta nel 2009 in Afghanistan, nonostante il suo impegno in operazioni reali sia proseguito ininterrottamente in tutti gli anni successivi.

La combinazione di *strike* aerei e di lanci di missili Tomahawk da navi e sottomarini, o da bombardieri¹⁵, è diventata il cuore della cosiddetta "american way of war", e con essa il corollario di capacità strategiche che la rendono possibile: dall'indispensabile segnale di localizzazione GPS al massiccio uso di piattaforme aeree per l'ISR e per l'aerorifornimento dei pacchetti d'attacco.

La storia insegna che le rivoluzioni stimolano contro-rivoluzioni, e la reazione ai successi dell'"american way of war" ha generato gli approcci che vengono collettivamente identificati come Anti Access, Area Denial (A2AD). Con l'approccio A2AD, gli avversari puntano ad impedire alle forze occidentali, americane *in primis*, di sfruttare il proprio vantaggio in termini di aviazione ed armamenti di precisione, creando invalicabili distanze sia fisiche sia politiche. Alla combinazione di sofisticate difese aeree stratificate e missili balistici ed ipersonici a lungo raggio si affiancano infatti guerra elettronica, attacchi *cyber* e disinformazione per sgretolare la volontà delle democrazie occidentali di combattere, e per

15 Da rimarcare in proposito anche il massiccio utilizzo di cruise Kalibr, lanciati da navi e sottomarini, e di cruise Kh-505/101, lanciati da bombardieri, da parte dei russi nella Guerra in Ucraina.

minarne la coesione, creando separazioni politiche in grado di rallentare o impedire il dispiegamento di forze in tempi brevi.

Assistiamo quindi ai grandi sforzi profusi da Russia e Cina per creare bastioni avanzati basati su armi a lungo e lunghissimo raggio con cui isolare intere regioni per impedire l'accesso agli americani ed ai loro alleati. Che si parli dell'armatissima enclave di Kaliningrad come "bolla" A2AD per isolare i Paesi baltici o delle isole artificiali cinesi, questi bastioni missilistici, insieme alla delegittimazione e alla disinformazione, sono pensati per tenere gli avversari a distanza almeno tanto a lungo da porli di fronte ad un *fait accompli*, ad un nuovo *status quo* difficilmente reversibile se non ad un prezzo molto alto, ovvero al prezzo di una guerra di teatro maggiore.

La risposta occidentale a questa sfida è il ricorso ad un nuovo modello, basato su un esercizio operativo che si sviluppa a partire da tutti i domini operativi - da quello informatico fino allo Spazio¹⁶ - e da complessi e sofisticati *network* informativi distribuiti, a cui è sempre più facile accedere. Si tratta di una fase ulteriore della RMA che ha un impatto enorme anche nel nostro quotidiano, con l'accesso ad internet sempre disponibile e con comodi *devices* multifunzionali nelle nostre mani capaci di scambiare grandi quantità di dati, immagini, video. Lo viviamo nella domotica e nel fatto che ormai possiamo "parlare" ai nostri elettrodomestici e collegarli alla rete affinché "collaborino". Lo sperimentiamo nel sempre maggiore incremento delle capacità di conservare e condividere dati, fra *cloud* e supporti di memoria fisici sempre più grandi ed economici. Stiamo parlando, insomma, dell'Internet Of Things (IoT) che, applicato all'ambito bellico, promette di consentire una continua e onnipresente raccolta di informazioni da ogni angolo del campo di battaglia, con il supporto di memorie d'archiviazione virtualmente illimitate, di sistemi di comunicazioni globali in grado di rendere il tutto disponibile ai vari gradi di comando e con l'assistenza di avanzati sistemi di analisi e intelligenze artificiali capaci di setacciare l'enorme quantità di dati grezzi. Insomma, con l'IoT e il multi-dominio siamo probabilmente all'ultimo stadio della RMA.

16 In realtà prima dell'avvento del multi-dominio, bisogna parlare di uno stadio "intermedio" rappresentato dalla cosiddetta Network Centric Warfare. La NCW la si può considerare come un ulteriore stadio della Rivoluzione negli Affari Militari reso possibile dal pieno sfruttamento delle tecnologie dell'informazione. Per cui, con la NCW il centro di tutto diventa l'infrastruttura informativa, senza la quale il dispiegamento di tutte le potenzialità della RMA, nel frattempo divenuta NCW, può avere luogo. L'approccio Network Centric Warfare, come dice il nome stesso, pone al centro di tutto la rete. Le piattaforme, i sistemi e perfino i concetti operativi devono essere pensati e realizzati in funzione della rete e della qualità e quantità di informazione che essa mette a disposizione di tutti gli operatori e gli utilizzatori. Funzionale al concetto di RMA e NCW è il concetto di sistema dei sistemi, da intendersi come un insieme di nodi che interagiscono fra loro attraverso una rete di collegamento dati al fine di svolgere "operazioni netcentriche" (definite da concetti operativi e dottrina).

Questa rivoluzione tecnologica rappresenta allo stesso tempo un'opportunità e una minaccia. La soglia finanziaria e tecnologica per accedere a tecnologie militarmente rilevanti come droni, visione notturna, comunicazioni satellitari e raccolta immagini dallo Spazio si è enormemente abbassata, tanto che anche avversari tradizionalmente non organizzati hanno ora accesso a capacità belliche che anni fa non sarebbero state pensabili. Attraverso i droni, per esempio, le forze di superficie occidentali sono, per la prima volta in diversi decenni, nuovamente esposte ad un reale rischio di attacco dal cielo, anche in scenari asimmetrici e contro avversari non-statali privi di una vera Aeronautica.

L'avvento dei *social media* e la sempre maggiore digitalizzazione hanno inoltre aperto nuovi fronti di vulnerabilità che possono essere sfruttati sia con attacchi *cyber* veri e propri contro infrastrutture e servizi chiave, sia attraverso una subdola e costante opera di disinformazione e propaganda per erodere la coesione sociale e politica di un Paese. Lo abbiamo visto ed esaminato nel Cp.1.

Dall'altro lato è evidente che l'Internet of Things, applicato ai sistemi militari, consente di comprimere enormemente i tempi di reazione ed ottimizzare l'impiego dei sistemi d'arma. Nell'odierna, estrema, evoluzione del concetto di guerra *network*-centrica, i sensori appartenenti a ciascuna Arma, dispiegati e operativi in uno qualunque dei vari Domini (terra, mare, aria, spazio e *cyber*), possono operare congiuntamente e scambiare dati in tempo reale per schermare ogni vulnerabilità.

Per questo gli sforzi occidentali si rivolgono ora verso il concetto di operazioni multi-dominio, che l'U.S. Army Training and Doctrine Command così descrive nel documento "Multi-Domain Battle: Evolution of Combined Arms for the 21st Century, 2025-2040": *"Un nuovo approccio olistico per mettere a fattor comune le capacità delle forze amiche attraverso domini, ambienti e funzioni, attraverso il tempo e lo spazio fisico, per ottenere specifici risultati sia in combattimento, sia prima e dopo il conflitto nella competizione fra Stati"*. Sulle definizioni e sul concetto di operazioni multi-dominio, in particolare quando applicati alle operazioni aeree. Parleremo dettagliatamente nel Cap.4.

Per il momento, ci basta osservare che l'impiego simultaneo ed integrato di capacità multi-dominio è pensato per sovraccaricare le capacità nemiche di comando e controllo ponendolo di fronte ad una moltitudine di "dilemmi". In pratica, il fronte avversario viene soverchiato attraverso la generazione di una moltitudine di minacce complementari, nessuna delle quali può essere ignorata. Il nemico è così costretto a dividere i suoi sforzi e ad aprire finestre di opportunità che possono essere sfruttate per distruggere elementi cruciali delle sue capacità A2AD.

Questo, per esempio, comporta un cambiamento concettuale sostanziale per le formazioni di terra, chiamate ora ad essere molto più proattive di quanto non lo siano state nel passato recente. Invece di manovrare soltanto dopo il completamento di attente campagne di *intelligence* e con il supporto decisivo degli attacchi aerei, le forze di terra dovranno ora manovrare in funzione della ricognizione, combattendo per raccogliere informazioni, e creare le condizioni perché le forze aeree possano lanciare *strike* in profondità. Mentre in passato le capacità aeronavali degli Stati Uniti erano viste come i fondamentali “enablers” strategici che consentivano alle forze di terra di entrare in teatro e vincere la battaglia, nel nuovo concetto è possibile che siano le forze di terra a dover creare le condizioni necessarie perché Marina e Aeronautica possano penetrare le difese avversarie e conseguire obiettivi strategici in profondità.

Alla base delle operazioni multi-dominio c'è la sostenibilità di un tempo di operazioni estremamente denso, che richiede ai Comandanti ed al C2 la capacità di aver accesso a tutte le informazioni necessarie, senza al contempo essere sepolti da dati d'importanza secondaria. Diventa indispensabile delegare maggiori responsabilità ai livelli subordinati e affidarsi all'autonomia degli Ufficiali sul campo, dando anche a piccoli gruppi di combattimento responsabilità e capacità prima impensabili. Non è più possibile concepire operazioni sincronizzate al secondo ed organizzate in rigide fasi con separazioni temporali e spaziali, né si possono prevedere pause fra un'operazione e l'altra. I piani devono essere formulati in continuazione, con agilità e capacità d'improvvisazione, secondo una direzione tattica decisa sul breve termine (indicativamente 24 ore) e una serie di idee di massima per i giorni successivi.

La raccolta e la disseminazione di informazioni utili al processo di Targeting del dispositivo avversario, a cominciare dall'artiglieria e dalle difese contraeree, è ovviamente un fattore assolutamente cruciale. Altrettanto ovvio è il fatto che in ogni scenario *peer* o *near peer* bisogna attendersi una feroce battaglia anche nel Cyberspazio e nello spettro elettromagnetico. Ciò significa che le azioni di disturbo e guerra elettronica avversaria potranno creare interruzioni e vuoti nel flusso di informazioni, ma che il ciclo di comando e controllo non dovrà interrompersi.

Per questi motivi, la priorità per le Forze Armate statunitensi *in primis*, ma sempre più comunemente anche per le altre forze occidentali, è acquisire sistemi di comando capaci di agire come *network* omni-pervasivi e altamente dinamici. Negli Stati Uniti si guarda quindi al Joint All Domain Command and Control. Nel Regno Unito si lavora al cosiddetto “Digital

Backbone”. Diversi nomi per architetture *hardware* e *software* che hanno però la stessa missione: consentire la raccolta di dati da una rete globale di sensori, piattaforme e sistemi d’arma interconnessi, così che le informazioni possano essere rapidamente elaborate in *intelligence* di qualità sufficiente a consentire l’immediata azione e la condivisione, così come l’integrazione di capacità non propriamente militari.

Con le giuste informazioni disponibili nelle giuste tempistiche, i Comandanti possono avere ben chiara la situazione sul campo ed impiegare l’arma o “l’effetto” meglio posizionato, a prescindere dal Dominio di provenienza e di applicazione finale.

Ne consegue il ritorno in auge, in particolare, dell’artiglieria terrestre, in virtù della sua relativa inferiore vulnerabilità agli attacchi missilistici avversari, mentre missili lanciati da terra possono ora servire ad aprire la strada alle forze aeronavali andando ad eliminare batterie SAM e missili anti-nave nemici a lungo raggio. Il fatto che l’artiglieria terrestre debba colpire obiettivi puntiformi e mobili anche a centinaia o addirittura migliaia di chilometri di distanza comporta una “fame” di dati, informazioni, ISR e *targeting* per localizzare, acquisire e “tenere nel mirino” i bersagli, ancor maggiore.

La presenza pervasiva di droni su tutto il campo di battaglia e la sfida del contrasto ai missili in arrivo a velocità ipersonica richiedono a loro volta più sensori, più dati, e una capacità d’ingaggio più rapida e onnipresente.

2.3 C2 e operazioni aeree

Per quanto esistano delle differenze d’approccio e di organizzazione fra nazione e nazione, in generale è inevitabile distinguere fra quello che gli americani identificano come Combatant Command (Command Authority)¹⁷ e OPCON (Operational Control). Nel primo caso si tratta della più ampia autorità possibile sulle forze sotto-ordinate, che include, oltre alla gestione strategica dell’operazione (partendo dalla definizione degli obiettivi e dei cosiddetti “end state”), la responsabilità su altri aspetti quali la logistica, l’addestramento, ecc. Il Comandante a cui viene delegato l’OPCON assume invece la direzione delle unità assegnategli per compiere una specifica missione, senza doversi occupare al contempo di organizzazione, approntamento e così via.

¹⁷ La definizione in inglese, ripresa dalla Joint Publication [JP] 1, Doctrine for the Armed Forces of the United States, rende meglio il concetto. “Combatant command (command authority) is defined as “nontransferable command authority, which cannot be delegated, of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces; assigning tasks; designating objectives; and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command”.

Durante le operazioni, il Comandante a cui vengono assegnate le forze dispiegate in teatro è noto, nella nomenclatura statunitense, come Joint Force Commander (JFC), ove controlla elementi provenienti dalle diverse Armi, o Combined Force Commander (CFC) dove sono presenti anche contingenti alleati. Il J/CFC ha l'autorità per impiegare le forze poste al suo comando e tipicamente si avvarrà di comandi subordinati generati dalle varie Armi, nominando Land, Sea, Air ecc. Component Commanders.

Il ruolo del Joint/Combined Force Air Component Commander (J/CFACC), con tutto il suo *staff*, è esercitare il comando e controllo tattico, prima di tutto pianificando la campagna aerea e compiendo il processo di *targeting* per individuare i bersagli, priorizzarli e definire le capacità tecniche per la loro eliminazione. Questo comporta la compilazione di una strategia di operazioni che è poi costantemente raffinata ed aggiornata tramite il Joint Air Tasking Cycle, che determina le esatte azioni da compiere in relazione alle forze disponibili, delineando quindi il Master Air Operations Plan.

Al cuore di questo processo si trova il Joint/Combined Air Operations Center (J/CAOC), ovvero il nodo C2 di livello Strategico/Operativo, che consente al comando delle Forze Aeree di dirigere e supervisionare le attività dei reparti assegnati e monitorare/gestire le operazioni.

Il CAOC necessita quindi prima di tutto di ottima e sicura connettività con comandi superiori ed inferiori, oltreché con i comandi "lateral", ovvero di altre Armi/Componenti. Deve inoltre disporre del miglior accesso possibile all'*intelligence*, da qualunque fonte essa provenga.

Il CAOC dipende poi dal cosiddetto "Theatre Air Control System" per poter esercitare effettivamente il comando e controllo in teatro. Il TACS si compone per esempio di radar e sistemi C2 mobili dispiegati in teatro, radar e installazioni *in loco* o forniti dagli alleati e sistemi aeroportati come gli AWACS.

Il CAOC assolve le sue funzioni grazie alle proprie Divisioni funzionali: la Divisione Strategy si occupa di definire obiettivi e piani oltre l'orizzonte delle 96 ore; la Divisione Combat Plans si occupa del *near term*, sulle 48 ore, ed è particolarmente importante perché, sulla base del Master Air Operations Plan, formula gli Air Tasking Orders (ATO) che dicono ai piloti come e quando volare, che armi impiegare e come comunicare.

La Divisione Operazioni controlla l'esecuzione degli ATO e la valutazione degli effetti che questi hanno sul nemico. Esistono poi ovviamente Divisioni che si occupano dell'*Intelligence*, dell'aeromobilità, ecc.

Tutto ciò che vola sul campo di battaglia rientra in un ATO poiché è indispensabile coordinare gli assetti in volo così che tutti possano essere riforniti e gli spazi aerei adeguatamente de-conflittualizzati per evitare collisioni ed incidenti, ma il J/CFACC non

ha mai la completa autorità su tutte le forze coinvolte. Uno dei motivi è che, storicamente, le altre Armi preferiscono mantenere il controllo sulle proprie unità aeree; un altro motivo è la sostanziale impossibilità tecnica di controllare in modo centralizzato le moderne forze aeree che operano su velocità e distanze che rendono il compito proibitivo.

Mentre le forze di superficie possono delegare il comando e controllo a comandi di rango inferiore, le forze aeree devono delegare ad elementi del Theatre Air Control System, quindi “pacchetti” di velivoli vengono controllati da radar a terra o in volo (AWACS), oppure dagli Air Support Operations Centers sul campo, e infine dalle Tactical Air Control Parties dispiegate con le forze a terra.

Le forze aeree più di ogni altra Arma sono comunemente legate al concetto di Supporting Force e Supported Force: l'esempio più ovvio è quello delle forze di terra che, in qualità di forze da supportare, si aspettano di ricevere Close Air Support dall'Aeronautica.

Alla Supported Force spetta definire gli obiettivi generali dello sforzo e quantificare il requisito CAS; alla Supporting Force tocca determinare le procedure, le tattiche e le comunicazioni, oltre a quantificare le dimensioni del “pacchetto” aereo necessario a rispondere alla richiesta. Questo è il ruolo dei già citati Air Support Operations Centers.

La tecnologia stessa ha negli anni fatto sbiadire e confondere le linee di demarcazione fra la direzione delle operazioni e la loro esecuzione. I *datalink* tattici, in particolare ovviamente il Link 16, hanno aperto le porte ad un ciclo decisionale dinamico con tempistiche molto più brevi del ciclo vita di un ATO, tutt'oggi indicato in 24 ore.

All'interno di una singola missione della durata di poche ore è possibile, ed invero indispensabile, fare fronte a molteplici cambiamenti della situazione sul campo. Si pensi ad una missione di recupero di un equipaggio abbattuto, per esempio, o al Time Sensitive Targeting di importanti bersagli – a cominciare dai lanciatori del Firing Weapons Complex avversario - che improvvisamente si possono rivelare e che richiedono azione immediata.

Non solo, negli ultimi 20 anni si è dovuto e potuto fare sempre maggiore ricorso al Dynamic Targeting contro bersagli di natura maggiormente tattica, con missioni d'attacco/CAS che prendono forma nel giro di poche decine di minuti.

In teoria, l'applicazione del consueto ciclo *Fix, Find, Track, Target, Engage, Assess* (F2T2EA) che dovrebbe definire le caratteristiche di questi attacchi richiederebbe un ruolo ancora maggiore del comando centralizzato a livello Air Operations Center. Nella pratica, i progressi tecnologici nella connettività e nell'*information management* fanno sì che nodi tattici avanzati, come i velivoli AWACS o ISR, già dispongano della capacità di svolgere un controllo tattico fluido e di fare un completo ciclo di *targeting*, a tutto beneficio della Joint Force.

Per tutti questi motivi, negli Stati Uniti non è nemmeno contemplato un livello di Tactical Command (TACOM), ma si parla soltanto di Tactical Control, che riassume in sé tutte le relative funzioni.

La distinzione fra comando e controllo tattico appare invece nella dottrina francese ed anche in ambito NATO, con il TACOM incaricato di definire e attribuire le diverse operazioni aeree e il TACON responsabile per l'esecuzione delle missioni, gli spostamenti e il ciclo di valutazione post-missione.

A prescindere da questa differenza concettuale, rimane il fatto che la nozione di “comando centralizzato/esecuzione distribuita” è ben radicata nella cultura delle varie Aeronautiche, che lavorano in questo modo da molti decenni. L'USAF ha formalizzato il concetto *Centralized Control/Decentralized Execution (CC/DE)* nella propria dottrina già nel 1975. Di fatto, la decentralizzazione tattica è stata parte integrante della storia dell'aviazione: in passato non esisteva alternativa alla decentralizzazione semplicemente perché mancavano i mezzi tecnici per esercitare il controllo, o anche solo per comunicare efficacemente con i velivoli in volo.

D'altra parte, le forze aeree che hanno fallito nel mantenere un controllo centrale coerente delle proprie operazioni hanno subito sconfitte spettacolari, come esemplificato dall'Aeronautica Francese nel 1940, sottolineando la difficoltà nel trovare il giusto bilanciamento.

Oggi si perseguono modelli di condotta tattica decentralizzati e dispersi con la consapevolezza che esistono i sistemi di comunicazione e targeting per mantenere il controllo e movimentare grandi quantità di informazioni nelle due direzioni. La decentralizzazione è necessaria per ridurre i tempi di reazione, “coprire” campi di battaglia sempre più vasti e attraversati da armi sempre più veloci e letali, e per aumentare la survivability del C2 nei confronti dell'azione avversaria.

CAPITOLO 3

Verso un nuovo C2 distribuito

3.1 Il nuovo scenario strategico: ripensare il C2

Nei nuovi concetti Multi/All-Domain, il fattore cruciale è il tempo. Le tempistiche sono sempre state importanti nell'arte della guerra, ma oggi più che mai comprimere i tempi di reazione e pianificazione è diventato un *must*. Sul nuovo campo di battaglia globale, connesso, congestionato e complesso, vince chi per primo scova e colpisce i gangli cruciali della volontà e possibilità dell'avversario di continuare a combattere.

Con l'A2AD e la disinformazione, gli avversari puntano a rallentare in ogni modo possibile la capacità delle democrazie occidentali di reagire, così da porle di fronte a fatti compiuti. In risposta, a partire dagli USA si sta puntando sul concetto Joint All Domain Operations per accelerare il ritmo di battaglia contemporaneamente a tutti i livelli (politico, economico, militare) e in tutti i domini (aria, terra, mare, spazio, spettro elettromagnetico).

In ambito JADO, l'integrazione fra le varie Armi dovrà raggiungere livelli completamente nuovi, più ambiziosi che mai: le Forze Armate dovranno Scoprire, Pianificare, Decidere ed Agire in concerto, simultaneamente in ogni Dominio, così da garantirsi libertà d'azione vicendevolmente. Banalmente, se in passato il potere aereo doveva, quasi senza eccezione, "aprire la porta" alle forze di terra, con le JADO è perfettamente plausibile che sia l'azione di artiglierie e forze terrestri ad indebolire quelle capacità A2/AD che impediscono all'Aeronautica di colpire in profondità.

Il successo dipenderà dalla capacità di far convergere "effetti" sviluppati su scala globale, e attraverso tutti i Domini, per generare "dilemmi" che soverchino la capacità dell'avversario di reagire tempestivamente, costringendolo ad esporre le sue vulnerabilità. Una volta aperta una "finestra d'opportunità" sarà fondamentale avere la capacità di sfruttarla, agendo con la massima rapidità.

Per questo è necessario mettere a fattor comune ogni informazione, ogni sistema d'arma, ogni capacità strategica. Il Comando missione deve essere centralizzato per quanto concerne gli obiettivi di massima, ma il Controllo deve essere ampiamente distribuito su tutto il campo di battaglia, così che l'Esecuzione della missione sia decentralizzata, agile e dinamica, ovvero adattativa rispetto all'evoluzione dello scenario operativo.

Molti piccoli posti comando ed ampia libertà d'azione ai livelli tattici più bassi sono fondamentali sia per ridurre la vulnerabilità delle funzioni di Comando e Controllo all'azione e alle artiglierie avversarie sia per garantire quella responsività che un singolo grande *staff* non potrebbe mai offrire. La decentralizzazione tattica riduce anche gli effetti nefasti che

l'interruzione delle comunicazioni con comandi di livello più alto potrebbero altrimenti avere sull'op-tempo.

Non sorprende quindi che la priorità numero 1 per il Dipartimento della Difesa americano sia sviluppare ed acquisire un sistema Joint All Domain Command & Control (JADC2) che assicuri la connessione di tutti i sistemi delle varie Armi, superando vecchie logiche *single-service* e limitazioni tecniche¹⁸. Tecnologie 5G e sistemi di trasmissione dati avanzati, con sempre più componenti basate nello Spazio, saranno fondamentali per garantire la distribuzione sicura e simultanea delle informazioni, e la mole di dati richiederà lo sviluppo di moduli di AI che assistano gli Ufficiali nel farvi fronte e ricavarne le informazioni effettivamente necessarie.

Lo Spazio avrà un ruolo sempre più importante, sia per le comunicazioni globali e per garantire la copertura di rete necessaria, sia per la sorveglianza del campo di battaglia e il contrasto alle armi ipersoniche. Si punta quindi a “democratizzare” l'accesso all'*intelligence* satellitare a livelli mai visti prima: con il satellite dimostratore Carbonite, la Royal Air Force vuole rendere possibile la visione dello *streaming* video del satellite direttamente da parte del pilota a bordo di un aereo in volo. Nei nuovi piani del MOD britannico per una costellazione di satelliti ISR multi-sensore si inserisce anche la sotto-costellazione Minerva, che dovrà mettere i vari satelliti in *network* fra loro e consentire l'elaborazione dei dati direttamente nello Spazio, e la disseminazione dell'*intelligence* direttamente agli utilizzatori finali sul campo. A ciò bisogna aggiungere l'interesse per l'uso di *link* ottici laser per trasmettere enormi quantità di dati in modo virtualmente non intercettabile e impossibile da disturbare.

La dispersione sarà fondamentale per sopravvivere all'azione avversaria ma anche per incrementare il numero di “dilemmi” da “presentare” al nemico, e il ciclo di *targeting* dovrà giocoforza avvenire a livelli tattici sempre più bassi.

Nei progetti per caccia di nuova generazione saranno fondamentali i gregari/adjunct, velivoli senza pilota che faranno di ogni velivolo pilotato un “mini-squadrone” con una varietà di capacità operative senza precedenti. Questo aumenterà enormemente le responsabilità del singolo pilota.

Il *trend* si riscontra in tutte le Armi, con la sempre maggiore enfasi posta sulla disponibilità di maggiori capacità ad armi combinate e multi-dominio anche ai livelli più bassi. Basti pensare ai nuovi Littoral Regiments dell'US Marine Corps, con il loro battaglione di difesa

18 Su questa lunghezza d'onda si sta muovendo anche la Difesa secondo la quale le FA di domani dovranno gravitare attorno al concetto di “*Joint by design*”, per il quale ogni attività militare ed ogni piattaforma necessaria ad espletarla dovranno esser concepite secondo logiche di interconnessione fra sistemi (*networking warfare*), di integrazione, digitalizzazione e condivisione delle informazioni (*information superiority* e *information sharing*), di velocizzazione dei processi di comando, controllo e coordinamento delle azioni, in un'ottica multi-dominio (*multi-domain warfare*).

aerea integrato e l'enfasi su armamenti missilistici, anche anti-nave, a lunghissimo raggio, o alla Future Commando Force dei Royal Marines.

3.2 Comando centralizzato, controllo distribuito, esecuzione decentrata

La disponibilità di AI, machine learning, cloud computing e sistemi di comunicazione avanzati permette ai comandi superiori centralizzati di avere una visione del campo di battaglia granulare come non mai. In teoria, sarebbe possibile centralizzare il controllo delle funzioni tattiche anche di livelli di comando molto bassi: abbiamo già visto nell'occasione dell'uccisione di Osama Bin Laden in Pakistan come sia oggi possibile per il Presidente degli Stati Uniti essere in contatto diretto, in tempo reale, con un piccolo team di forze speciali nel pieno di un'azione dall'altra parte del globo. Nel 2020, il First Sea Lord sir Tony Radakin è stato similmente in contatto diretto con le squadre di Royal Marines impegnate a Cipro nella sperimentazione della Future Commando Force, con la possibilità di accedere direttamente da Northwood alle telecamere sugli elmetti e al network sugli smartphone modificati indossati sul petto dai soldati.

Oggi più che mai i comandi superiori possono esercitare il controllo da posti comando che non necessitano più di dispiegarsi in teatro. La 3rd Commando Brigade della Royal Navy, nell'esercitazione Cold Response 2022 in Norvegia, ha sperimentato per la prima volta il suo nuovo modello di operazioni che prevede che il comando brigata rimanga a bordo delle navi anfibe. Il comando brigata sta al contempo "ibridandosi", con la componente terrestre e navale del ruolo comando che si mescolano in un unico staff. Il comando brigata si è trovato ad esercitare il controllo su piccoli team impegnati in raid in profondità a terra, coordinandoli fino al singolo individuo ed assumendo oltretutto un ruolo più ampio anche nella gestione degli aspetti navali della guerra litoranea.

A fronte dell'accorpamento di 2 comandi superiori a 1 stella che erano fino in tempi recenti ben distinti, e a contraltare della sostanziale scomparsa di un comando tattico di brigata sul campo di battaglia, sono state aumentate le capacità di comando, controllo e comunicazioni dei singoli battaglioni Commando, affinché essi possano esercitare il controllo in modo distribuito, godendo al contempo dell'accesso, in remoto, alle risorse disponibili presso livelli di comando superiori dislocati in Paesi amici, sulle navi o direttamente in patria.

Nell'USAF si sta similmente rivalutando il ruolo del CAOC, con il suo enorme numero di personale e i suoi cicli di pianificazione su molte, troppe ore. Ad un recente evento, il Col. Brian Tyler, USAF, responsabile per le operazioni Cyber e non cinetiche presso l'Air Combat

Command, è stato tranciante nell'affermare che l'odierno CAOC non ha assolutamente la capacità di sincronizzare moderne operazioni multi-dominio in un contesto ad alta intensità

A fronte di un comando sempre più centralizzato e centrale nel definire ambito e obiettivi di un'operazione, assume importanza sempre maggiore la distribuzione del controllo.

Il Colonnello Johnathan Hughes, USAF, Chief Command and Control, Intelligence, Surveillance and Reconnaissance Operations Division, Air Combat Command, è convinto che l'unico modo di far fronte ai nuovi requisiti sia disaggregare le funzioni di comando e controllo su una piattaforma comune in Cloud. Il Cloud rimuove il requisito di avere localmente disponibile tutto l'hardware e il software, con ovvi vantaggi per le possibilità di spostamento e sopravvivenza dei vari nodi.

Si parla quindi di aggregare i dati, tutti i dati, da qualunque fonte essi provengano, disaggregando al contempo l'architettura fisica dei grandi e vulnerabili posti comando. Le ambizioni del concetto Multi-Domain potranno essere realizzate soltanto attraverso lo sviluppo di una rete tattica di connessione capace di collegare tra di loro le pedine distribuite e garantire unquadro della situazione condiviso.

Dobbiamo essere tuttavia consapevoli che quella rete tattica apre un nuovo fronte di vulnerabilità: se da una parte riduciamo l'esposizione del personale e dei comandi a minacce cinetiche, la dipendenza da dati e comunicazioni rende più che mai esposti ad attacchi cyber ed elettronici.

La rete tattica dovrà necessariamente avere come doti la robustezza e la capacità di auto-diagnosticare attività malevole avversarie in corso. Dovrà essere ridondante, per continuare a funzionare anche sotto attacco. Dovrà quindi esprimersi attraverso molteplici diversi "ponti"¹⁹ e ripetitori attraverso i vari domini, e utilizzare nuove tecnologie dove possibile. Particolarmente utili risulteranno sistemi di cifratura quantistici e link broadband ottici basati sul laser, che proteggeranno le informazioni e, nel secondo caso, andranno a moltiplicare esponenzialmente la quantità di dati trasmissibili.

La rete dovrà avere una diffusione capillare e dovrà spingersi verticalmente fino al più basso livello tattico possibile, al contempo allargandosi orizzontalmente a collegare fra loro le diverse Armi. Questo sarà fondamentale per consentire il proficuo impiego delle piccole o medio-piccole unità ad armi e domini combinati che saranno centrali nelle future operazioni.

Presso queste nuove pedine di manovra integrate dovranno quindi operare nodi di comando e controllo distribuiti che garantiscano il necessario coordinamento e l'allocazione

19 A cominciare dai droni: in volo, a terra e in mare.

delle risorse – in termini di supporto di fuoco, intelligence, ricognizione, ecc. - che passano attraverso la rete.

Senza questi nodi, la rete rimarrebbe “anarchica” e verrebbe a mancare la necessaria connessione fra gli sforzi delle varie componenti. Occorre, dunque, un livello di comando e controllo spinto fino al più basso livello tattico per coordinare tutti gli “utenti” che popolano la tactical grid e assicurare che le loro azioni si inseriscano sempre in un disegno di missione unitario, così come delineato e sviluppato dal comando centrale.

Volendo sintetizzare possiamo immaginare uno schema come il seguente:

Comando centralizzato. Alto livello: definizione della missione e della forza, e assegnazione degli obiettivi; elaborazione del piano strategico; coordinamento e gestione dei nodi distribuiti intermedi;

Nodi distribuiti. Livello intermedio: pianificazione operativa e tattica; coordinamento e gestione delle pedine tattiche; assegnazione delle risorse;

Pedine. Livello tattico: esecuzione della missione; autonomia operativa e capacità di adattamento/modifica della missione.

3.3 Strutture orizzontali e livelli intermedi

La delega del controllo dovrà avvenire non solo verticalmente, ovvero trasferendo capacità e responsabilità a livelli più bassi della catena di comando, ma anche orizzontalmente, ovvero superando le attuali divisioni fra le varie Armi.

In ambito multi-dominio, in cui ciascuna Forza Armata è sia Supportata che Supportante, il trasferimento di autorità da un’Arma all’altra, a seconda degli obiettivi e della situazione contingente, è praticamente inevitabile. Comandi “ibridi” come il nuovo Littoral Strike Command britannico per la 3rd Commando Brigade e le relative componenti navali rispondono più realisticamente ai requisiti di massima integrazione e flessibilità.

Serviranno competenze trasversali per ottenere il massimo risultato da unità che assumeranno ruoli molto più ampi e complessi: l’adozione di armamenti missilistici con capacità anti-nave a lungo raggio dell’USMC e nell’artiglieria dello US Army rappresenta un altro esempio. Il Precision Strike Missile dell’artiglieria campale avrà un ruolo chiave nella soppressione delle difese aeree nemiche, mentre la manovra d’aeroassalto potrà beneficiare di nuovi e radicalmente più veloci elicotteri a lungo raggio (FVL, Future Vertical Lift)²⁰ capaci di penetrare in profondità nel dispositivo avversario per disarticolarlo.

²⁰ Il programma FVL è un programma dell’US Army che al momento coinvolge anche i Marines ed è suddiviso in due tronconi: FARA (Future Attack Reconnaissance Aircraft), per una macchina monomotore da ricognizione armata con la quale rimpiazzare l’OH-58 Kiowa Warrior, il cui ruolo è attualmente ricoperto “ad interim” dagli elicotteri AH-64E Guardian e dagli UAV RQ-7B Shadow, e FLRAA (Future Long-Range Assault Aircraft), per lo sviluppo di una macchina d’assalto con la quale rimpiazzare il Black Hawk. Per la gara FARA sono in gara l’elicottero compound e

Saranno molte le capacità che richiederanno la messa a fattor comune di sistemi ad oggi tenuti “artificialmente” separati, e quelli che oggi sono per la maggior parte circuiti ad Arma singola dovranno in futuro essere in grado di comandare ed impiegare in modo intercambiabile e simultaneo sistemi d’arma disparati non in base all’Arma di appartenenza, ma al miglior posizionamento sul campo in relazione alla minaccia.

In questo modo sarà possibile per tutti gli utenti – navali, terrestri e aerei - scambiare grandi volumi di informazioni – video, messaggi, dati – in tempo reale, utilizzando ogni canale di comunicazione possibile: militare e commerciale, satellitare, radio ecc. Ciascuna unità, a prescindere dalla sua Arma d’appartenenza e dalla dispersione sul campo di battaglia, dovrà poter inserire informazioni nella bolla informativa, riceverne altre, condividere una singola immagine situazionale e mettere i propri sistemi d’arma a completa disposizione della Joint Force.

In questo contesto si vanno a collocare i BFM (Battle Force Manager) che dovranno avere le seguenti capacità:

- monitorare e comprendere lo stato del network condiviso, intervenendo automaticamente in caso di problemi, per garantire l’auto-ricostituzione della rete e l’aggiramento di ostacoli, quale che sia la loro natura;
- monitorare ed impiegare le capacità delle unità disperse mantenendone le capacità operative e mappando anche i requisiti logistici;
- scovare, sorvegliare, prioritizzare e allocare i bersagli;
- controllare remotamente l’ingaggio, servendosi degli effettori più opportuni e meglio posizionati, a prescindere dall’Arma di appartenenza.

Ecco, dunque, il livello di controllo distribuito intermedio che cercavamo. Anni fa, l’USAF aveva ipotizzato una parziale applicazione di queste idee con quello che avrebbe dovuto diventare l’E-10, ovvero un velivolo multi-ISR che avrebbe accentrato in sé capacità ISR oggi garantite dagli RC-135 Rivet Joint, dagli E-3 AWACS e dai velivoli radar JOINT STARS. Ciascun E-10 sarebbe stato una mini-cella di targeting e battle management capace di gestire la missione di un pacchetto di forze aeree e/o di superficie.

L’E-10 non si è mai realizzato, ma quei “quarterback” distribuiti sono soltanto diventati più numerosi e con migliori doti di sopravvivenza. In particolare è l’F-35 il primo vero esempio di nodo “omni-role” che ha già dimostrato in diversi esperimenti di poter fare da battle manager avanzato, sfruttando la sua relativa impunità e la ricchezza di sensori e

rotore coassiale contro-rotante Raider-X di Lockheed Martin/Sikorsy ed il più convenzionale, ma dotato di generose semiali con funzione portante, 360 INVICTUS di Bell. Per la gara FLRAA, invece, sono in gara l’elicottero compound con rotore coassiale SB-1 Defiant, sviluppato da Lockheed Martin/Sikorsky e Boeing, e il convertiplano V-280 VALOR di Bell.

sistemi di comunicazione per acquisire bersagli a favore di altri sistemi d'arma, come i missili terra-aria antiaerei/antimissile Patriot dell'Esercito o gli Standard della Marina, o i missili stand-off lanciati da velivoli di quarta generazione, o da trasporto, dal di fuori delle "bolle" A2/AD avversarie. Sull'F-35 torneremo più avanti.

La creazione di una rete consente anche ad altri velivoli di diventare nodi di comunicazione, targeting e fusione delle informazioni. Si guarda con interesse alle aerocisterne, da equipaggiare con gateway di rete capaci di mettere a fattor comune vari network e "tradurre" segnali da un datalink ad un altro. Questo accade sia negli USA, con applicazione di Advanced Battle Management System sui KC-46 Pegasus, sia nel Regno Unito dove il progetto Babelfish ha visto un nodo di rete installato su un'aerocisterna Voyager, capace ora di assorbire dati da molteplici datalink, dai satelliti e da altre fonti²¹.

I vari progetti per sistemi di combattimento aereo di sesta generazione (siano essi l'NGAD dell'USAF, il Tempest a guida britannica o il franco-tedesco SCAF) sono tutti incentrati su caccia pilotati che saranno essi stessi nodi di comando, controllo e targeting, circondati da "piccole unità" composte di sciami di droni e gregari senza pilota. Droni e caccia pilotati insieme saranno equipaggiati con sensori e strumenti di bordo tali da poter identificare obiettivi, integrare dati da molteplici sensori per comporre un quadro tattico situazionale in un'ampia zona, guidare effettori di varia provenienza sui bersagli e condividere le proprie armi e informazioni con gli altri nodi.

3.4 L'esperienza americana. Dall'ABMS al programma Skyborg

L'USAF ha un ruolo chiave da giocare nella maturazione del concetto di Joint All Domain Command & Control. Il ruolo delle forze aeree nello *strike* e nella raccolta di informazioni rimane assolutamente centrale, in particolare proprio nelle Forze Armate occidentali, e come abbiamo visto sono proprio le forze aeree che, per vari motivi, sono in qualche modo già avviate su certi concetti da molti anni.

Al cuore degli sforzi dell'USAF c'è l'Advanced Battle Management System (ABMS), che ha cominciato a mostrare le sue potenzialità negli eventi "On Ramp" tenutisi a partire dal dicembre 2019. L'ABMS deve prima di tutto risolvere un problema ben noto nei sistemi d'arma odierni: l'essere concepiti quasi in isolamento. Nonostante tecnologie come i Data Link e il Cooperative Engagement Capability dell'US Navy, sensori e armi odierne non sono in grado di condividere continuamente e senza ostacoli le relative informazioni e capacità. Ci vogliono dei *gateway* dedicati che "traducano" le informazioni di un sistema d'arma a favore di un altro, e molti minuti di traffico dati e radio per ricostruire un'immagine d'insieme.

21 Qualcosa in tal senso si sta provando anche in Italia con il G550 CAEW.

Oggi l'integrazione delle informazioni provenienti dai vari sensori avviene ancora primariamente nella mente degli Ufficiali nei posti comando, che devono mettere insieme quello che sentono dai vari operatori. L'obiettivo è automatizzare e velocizzare questo processo.

Il progetto ABMS è, inevitabilmente, un programma a lungo termine, fatto di molteplici componenti sia *hardware* che *software*. Come tale, può prendere forma soltanto per fasi successive, ma questo lo rende un programma difficile da sorvegliare e da valutare, tanto che il Congresso, insoddisfatto dalle spiegazioni fornite dall'USAF, ha ripetutamente rivisto al ribasso le cifre stanziare, addirittura tagliandole della metà nel Fiscal Year 2021.

Questo nonostante i risultati promettenti dei 4 eventi "On ramp" tenutisi nel dicembre 2019, fra agosto e settembre 2020 e nel febbraio 2021. Nel corso di queste esercitazioni sperimentali, l'ABMS ha dimostrato la condivisione di tracce *radar* fra sensori dell'Esercito, delle navi dell'US Navy e dei caccia F-22 ed F-35. Ha anche generato una Unified Data Library (UDL), un ambiente in *cloud* che semplifica il monitoraggio spaziale mettendo a fattor comune sensori terrestri e basati nello Spazio. L'On Ramp 2 ha dimostrato ulteriore integrazione fra sensori delle varie Armi ed è culminata nell'abbattimento di missili cruise simulati da droni bersaglio con l'uso di missili aria-aria Sidewinder, lanciati da un UAV MQ-9B REAPER, razzi laser-guidati APKWS, lanciati da caccia F-16, e proiettili ipersonici, sparati da cannoni da 155 mm dell'Esercito e da 127 mm della Marina.

L'On Ramp 3 ha dimostrato il potenziale dell'aerocisterna KC-46 Pegasus come posto comando e *gateway* volante per mettere in comunicazione F-22, F-35 e velivoli *legacy* di quarta generazione.

L'esperimento On Ramp 4 si è tenuto in Europa ed è stato incentrato sulla condivisione di informazioni con gli alleati, nello specifico velivoli di Regno Unito, Olanda e Polonia, ma l'evento è stato ridimensionato rispetto alle previsioni originarie a causa dei menzionati tagli al *budget*, che hanno anche cancellato del tutto un quinto evento.

Il primo progetto d'acquisizione avviato in ambito ABMS discende direttamente da quanto dimostrato nell'On Ramp 3: la Capability Release 1 infatti ha visto l'USAF ordinare, nel Fiscal Year 2022, fra 4 e 10 pod-gateway da impiegare sulle aerocisterne KC-46. Sta inoltre prendendo forma il piano per una Capability Release 2, che riguarderà una soluzione *hardware* e *software*, completa di intelligenza artificiale, per accelerare il comando e controllo nelle missioni di difesa dello spazio aereo nazionale. La successiva Capability Release 3 si concentrerà sul *network* e sulla capacità di processare grandi quantitativi di dati.

In generale, ABMS si occupa di 6 macro-ambiti, ciascuno dei quali si sviluppa tramite molteplici ricerche e contratti. Parliamo di integrazione di sensori; trasmissione e distribuzione dati; connettività da macchina a macchina; *cybersecurity* e crittografia; applicazioni *software* ed infine sistemi d'arma.

All'interno di questi ambiti ci sono almeno 28 diversi "prodotti" in vari stadi di sviluppo e valutazione, a partire da sistemi Cloud sicuri: a livello strategico si parla di CloudONE, una sorta di rete internet appositamente sviluppata, a cui si agganciano altri *cloud* e applicazioni che consentono di condividere dati e accedervi in modo sicuro, con limitazioni agli scambi a seconda dei livelli di comando. Per esempio, in ambito tattico viene usato EdgeONE, un *cloud* che consentirà di salvare dati presso l'utente periferico, ovvero, per esempio, il sensore sul campo, per poi trasmetterli automaticamente appena la connessione viene ristabilita. DataONE dovrebbe invece accogliere dati raccolti da tutti i sensori di tutte le Armi, mentre CrossDomainONE è un'applicazione che consente il trasferimento di informazioni in entrambe le direzioni lungo la catena gerarchica, con i necessari gradi intermedi di sicurezza e criptazione. A livello *hardware* c'è un progetto, denominato RadioONE, per una nuova radio interforze e anche un programma ApertureONE per nuove antenne per comunicazioni satellitari.

Si sta pure lavorando a diverse "applicazioni-assistenti", come ad esempio il Project Maven, che tramite l'intelligenza artificiale contribuiscano a scremare i dati grezzi e ad accelerare il processo decisionale. Infine, sotto il nome GatewayONE si cela il sistema di *hardware* e *software* che "traduce" i segnali provenienti da diversi *datalink* sicuri, consentendo il passaggio di dati da e per le piattaforme di quinta generazione.

Visti gli obiettivi, ABMS andrà con il tempo a toccare praticamente ogni ambito e sistema. Si appoggerà per la trasmissione di dati anche a nuove tecnologie e nuove costellazioni di satelliti. A tal proposito vale la pena soffermarsi per un attimo sulla nascente costellazione Transport Layer, una vasta rete di piccoli satelliti, relativamente poco costosi, che formano una rete internet resiliente basata su 6 diverse orbite. Il 28 febbraio scorso, Lockheed Martin, Northrop Grumman e York Space hanno ricevuto ciascuna un contratto per la produzione di 42 satelliti, per un totale di 126, tutti da consegnare entro il 2024. Si tratta della "Tranche 1" di questo progetto, che segue la Tranche 0 che aveva già visto l'acquisizione di 10 satelliti da Lockheed Martin e altrettanti da York Space, per il lancio nel 2021.

La resilienza di questa costellazione deriva in buona misura dall'essere così ampiamente distribuita da rendere sostanzialmente impossibile la sua distruzione fisica. I satelliti comunicheranno fra loro con *link* ottici, in pratica dei laser, e potranno quindi aggirare "buchi" nella costellazione ricreando la rete con percorsi alternativi.

Il grande obiettivo per il futuro è impiegare i laser anche per trasmettere verso la terra e addirittura verso mezzi in movimento. Una connessione ottica di questo tipo può trasmettere dieci volte più dati ed è virtualmente impossibile da intercettare o disturbare poiché qualunque disturbo o intromissione richiede di piazzarsi fisicamente lungo il percorso del laser. Tuttavia, mentre le comunicazioni via laser fra satellite e satellite sono già una realtà piuttosto matura, adottata anche dalla costellazione Starlink di SpaceX, le comunicazioni verso la terra devono ancora superare diverse sfide legate agli effetti atmosferici che disturbano il fascio laser.

Gli sforzi per usare il laser come sistema di comunicazione si sono moltiplicati negli ultimi tempi, ma già negli anni '90 si pensava al laser come possibile soluzione per trasmettere informazioni dai satelliti ai sottomarini, anche in immersione. Nel 2020 General Atomics ha dimostrato che il suo Airborne Laser Communication System (ALCoS) per velivoli senza pilota come l'MQ-9 può tracciare i satelliti e stabilire una connessione. Una volta maturo, il sistema consentirebbe di trasmettere una mole di dati 300 volte più grande di quella possibile con gli attuali *link* satellitari in radiofrequenza, e con la quasi inviolabilità della trasmissione.

L'USAF sta investendo per realizzare in tempi brevi un obiettivo ancor più ambizioso: lo sviluppo di un *pod* che consentirebbe ai velivoli di combattimento in volo di stabilire un *link* laser con i satelliti. Chiaramente ci sono enormi difficoltà da superare nel creare un sistema di comunicazione in *pod* che sia in grado di mantenere un laser puntato su un satellite nello Spazio, mentre il velivolo manovra, vibra, attraversa condizioni atmosferiche cangianti e potenzialmente "mette in ombra" il *pod* durante alcune manovre. Space Micro, una piccola azienda di San Diego controllata da Voyager Space, ha identificato una soluzione nello sviluppo di avanzate lenti deformabili che si adattano per cancellare i disturbi atmosferici e mantenere il laser coerente ed inalterato. Il progetto, battezzato DEFORMO, è condotto in *partnership* con Rhea Space Activity (RSA) e con la Johns Hopkins University di Baltimora. L'US Air Force Laboratory punta a dotare velivoli come l'F-35 di un *pod* capace di trasmettere dati in modo virtualmente inviolabile al ritmo di 10 Gigabit per secondo, consentendo quindi lo scambio di una mole di informazioni esponenzialmente maggiore di quanto possibile oggi, e senza l'emissione di alcun segnale in radiofrequenza che il nemico possa intercettare.

Abbiamo visto in precedenza come i nuovi concetti pongano particolare importanza sull'uso di velivoli senza equipaggio come gregari autonomi per i caccia pilotati, in particolare, ma non solo, per i futuri caccia e bombardieri di nuova generazione. Al livello più "basso" parliamo di piccoli droni sacrificabili, dal costo e dalle capacità contenute, più simili a

munizioni circuitanti o civette autonome che non ad aerei da combattimento. In quest'ambito rientrano i droni aero-lanciati e aero-recuperabili X-61 Gremlin di Dynetics. Questi piccoli velivoli saranno relativamente semplici e pensati per ruoli specifici, e trarranno la loro forza dall'operare in sciami per distrarre o soverchiare le difese aeree avversarie.

Ad un livello superiore si pensa a velivoli di dimensioni comparabili a quelle dei caccia, e quindi con sensori e carichi d'armamento molto più importanti. Gli sforzi dell'USAF per arrivare ad un velivolo senza pilota "spendibile" (Low-Cost Attributable Aircraft Systems, LCAAS) con cui incrementare la sua massa vanno avanti dal 2015 e l'USAF si aspetta di farne un programma d'acquisizione vero e proprio a partire dal Fiscal Year 2023.

La capacità di questi velivoli di mantenere la formazione e manovrare ed operare i propri sensori in autonomia è fondamentale per ridurre il carico di lavoro del pilota da caccia che, da bordo del suo velivolo, dovrà in futuro controllare l'intero gruppo ed autorizzare i droni ad impiegare armamenti. I sistemi a pilotaggio remoto usati fin qui, infatti, non hanno un pilota a bordo ma richiedono una grande quantità di personale a terra per la condotta delle missioni. Questo dispendio di forze deve essere superato perché la visione alla base del concetto LCAAS possa realizzarsi.

Per arrivare a schierare quel tipo di capacità, l'USAF ha dunque investito prima di tutto sullo sviluppo di un "cervello" da poter installare su aerei di caratteristiche e produttori diversi, da scegliere in seguito. Quel sistema operativo ad intelligenza artificiale, capace di ampia autonomia, è noto come Skyborg Autonomy Core System (ACS), un apparato comprensivo sia di *hardware* che di *software*, in corso di sviluppo da parte dell'azienda Leidos.

Nel dicembre 2020, nell'ambito del progetto Skyborg, sono stati assegnati fondi a 3 produttori di droni: 2 di questi hanno già raggiunto lo stadio delle prove in volo dopo aver equipaggiato i propri velivoli con l'ACS. Skyborg ACS è andato in volo per la prima volta su un UTAP-22 Mako prodotto da Kratos²², e poi su un MQ-20 Avenger²³ di General Atomics. A mancare all'appello è ancora il Loyal Wingman di Boeing, basato sull'Airpower Teaming System sviluppato in Australia e recentemente battezzato MQ-28A Ghost Bat.

Avenger e Ghost Bat, velivoli di grandi dimensioni con caratteristiche *stealth*, sono indicativi delle capacità che si vogliono ottenere dai Loyal Wingman, che dovranno essere velivoli "Group 5", ovvero i più grandi e capaci secondo la classificazione statunitense. L'UTAP-22 ha dimensioni più contenute, ma offre "indipendenza dalle piste" poiché è lanciato da catapulte portatili, anche a bordo di navi, ed atterra grazie ad un paracadute, sia su terra ferma sia in acqua.

22 Il Mako è un derivato di un aerobersaglio. In Italia, Leonardo potrebbe far valere tutta la propria esperienza nel campo degli aerobersagli per realizzare soluzioni analoghe al Mako.

23 L'Avenger è una variante a getto, con un profilo stealth maggiormente accentuato, dell'MQ-9B Reaper.

Nel corso dei voli sperimentali con i vari droni è stato dimostrato il decollo sotto controllo di un operatore umano seguito, una volta raggiunta un'altitudine sicura, dalla presa di comando da parte dell'ACS. Skyborg ha dimostrato la conduzione del velivolo tramite l'esecuzione di manovre base, la risposta a nuove indicazioni di navigazione, l'esecuzione di manovre coordinate e il rispetto di profili di volo e "barriere geografiche" da non oltrepassare.

Il 26 ottobre 2021 è stato raggiunto un importante traguardo con la cooperazione in volo di 2 velivoli senza equipaggio MQ-20 Avenger di General Atomics, equipaggiati con lo Skyborg Autonomy Core System. Il volo, parte del Large Force Test Event ORANGE FLAG 21-3 sulla base di Edwards, ha visto i due velivoli volare in formazione, autonomamente, scambiandosi al contempo informazioni. Una singola Ground Control Station ha monitorato il duo di velivoli, equipaggiati con il *pod* dotato di sensore IRST Legion di Lockheed Martin. I prossimi esperimenti vedranno formazioni più ampie di droni e velivoli pilotati, per dimostrare come le missioni possano essere portate a termine con la cooperazione *manned – unmanned*.

Il *pod* Legion include anche un sistema di *datalink pod to pod*, ed è già ampiamente impiegato sugli F-15 dell'USAF. Legion conferisce al Loyal Wingman la capacità di volare in prima linea ed acquisire passivamente bersagli a beneficio di altri velivoli in formazione, senza alcuna trasmissione radar che possa essere individuata dall'avversario. Questo è un primo esempio del tipo di ruoli che i *loyal wingman* ricopriranno.

Nel frattempo l'USAF ha anche assegnato contratti a Kratos e General Atomics per lo sviluppo di nuovi velivoli senza pilota, diversi da quelli già in sperimentazione. Chiamati Off Board Sensing Stations, questi nuovi velivoli sono specificamente pensati per affiancare i caccia pilotati, mettendo a disposizione dei piloti dei sensori volanti da usare per scovare bersagli senza esporsi alla reazione avversaria.

Nonostante l'acronimo ponga l'accento sul ruolo dei sensori, è comunque confermato che l'OBSS avrà "significative" capacità di trasporto armamenti per fungere da estensione dell'arsenale di bordo del velivolo pilotato.

General Atomics per ora non ha fornito dettagli sul velivolo offerto per questo nuovo progetto, ma Kratos ha confermato che svilupperà un velivolo dotato di "ampia" stiva armamenti e con carrello tradizionale. L'uso di un normale carrello suggerisce che si tratterà di un velivolo più grosso e di capacità maggiormente sviluppate, a costo di perdere "l'indipendenza dalla pista" offerta dal Mako o dal più prestante Valkyrie.

Il contratto assegnato a Kratos, annunciato il 25 ottobre 2021, ha un valore di 17,6 milioni di dollari e copre ricerca e sviluppo, con completamento entro il 31 ottobre 2022. Se i risultati

saranno stati soddisfacenti, verrà esercitata l'opzione, del valore di 31,3 milioni, per la produzione di un prototipo da dimostrare in volo, entro il 31 gennaio 2024.

Il contratto assegnato a General Atomics, pubblicato il 26 ottobre 2021, ha un valore complessivo superiore di circa 700.000 dollari rispetto al precedente, pur avendo identiche tempistiche ed obiettivi.

Separatamente dalle attività Skyborg propriamente dette, General Atomics Aeronautical Systems (GA-ASI), ha annunciato di aver completato con successo un'altra importante dimostrazione in cui un pilota, in volo in questo caso su un biturbina Beechcraft King Air usato come surrogato di un caccia, ha comandato un velivolo senza pilota Avenger sfruttando una App installata su un *tablet*. Il test, che ha avuto una durata di circa due ore, risale al 25 agosto 2021 ed ha avuto luogo sopra la California meridionale, con l'Avenger decollato dalla base GA-ASI nel deserto del Mojave e il King Air dall'aeroporto "Montgomery-Gibbs" di San Diego. Il *tablet*, che il pilota può indossare assicurato alla coscia, è una possibile soluzione al problema di come portare i droni "dentro" velivoli che non sono stati pensati come posti comando volanti. Modificare il *cockpit* avrebbe costi e implicazioni proibitive, mentre il *tablet*, equipaggiato con l'applicazione RCU-1000 Advanced Human Machine Interface, messa a punto da Autonodyne, rappresenta una soluzione "plug and play" che consente al pilota umano di mantenere il comando e controllo tattico, impartendo specifiche missioni ai droni, e, nel caso, autorizzando l'uso di armamenti.

L'RCU-1000 offre un'intuitivo interfaccia che mostra al pilota le informazioni provenienti dai droni e consente di impartire loro ordini, sia singolarmente sia a gruppi, sfruttando i *datalink* del caccia.

L'RCU-1000 è un sistema agnostico sviluppato per essere compatibile con diversi droni, ed è già stato testato con "dozzine" di diversi UAV, che vanno dal quadcoptero tascabile Parrot Anafi, selezionato dall'USMC e gradito dalle Forze Armate di svariati Paesi, fino al citato Mako di Kratos.

Il *software* di Autonodyne non è legato ad un *hardware* specifico e può quindi essere caricato in un'ampia varietà di *device*, da telefonini a computer portatili "induriti". Il *tablet* "da coscia" è uno strumento già comune e conosciuto dai piloti, quindi rappresenta una buona base di partenza.

L'esperimento ha sicuramente l'attenzione dell'USAF e probabilmente di tante altre aeronautiche. Nel caso americano, la combinazione di *software* di controllo agnostico e del nucleo comune d'intelligenza artificiale Skyborg potrebbe consentire la rapida conversione di svariati modelli di UAV in gregari/*adjunct*.

CAPITOLO 4

La rilevanza strategica della componente aerospaziale nelle multi-domain operations

4.1 Le operazioni multi-dominio

Il concetto di operazione multi-dominio è nato negli ultimi anni negli Stati Uniti come risposta alla percepita erosione del vantaggio militare americano. Per tutti gli anni dalla caduta del Muro di Berlino e fino, quanto meno, a 4-5 anni fa, la superiorità militare americana ed occidentale non era messa in discussione né era discutibile; anzi, essa costituiva un assunto strategico fondamentale sul quale si fondava in ultima analisi l'egemonia americana e dal quale discendevano poi le dottrine e le condotte operative. Questo assunto valeva soprattutto per la parte aerea dove tutti i conflitti che si sono combattuti in 30 anni – dall'Afghanistan, alla Libia passando per il Kosovo – hanno visto l'incontrastato dominio dell'aria occidentale con operazioni che si sono combattute con la totale assenza di forze aeree e missilistiche ostili che, anche laddove presenti, venivano soppresse in poche ore/giorni. Ciò ha sempre permesso di godere, appunto, di un'assoluta *air-dominance* che ha consentito l'esecuzione di ogni tipo di operazione, in qualsiasi luogo e momento, con scarse o nulle possibilità di abbattimento degli "aerei amici". Una situazione che difficilmente troverebbe riscontro in un conflitto ad alta intensità con avversari di tipo peer/near-peer, dove la presenza di sistemi antiaerei integrati e stratificati e di velivoli, droni e sciame sarebbe verosimilmente certa e di più difficile contrasto. A tal proposito la Guerra in Ucraina ha dimostrato il ruolo fondamentale giocato dalle difese contraeree terra-aria ucraine, soprattutto quelle mobili (assistite in questo caso dal *cueing* NATO ed americano) che hanno imposto un attrito significativo alla VKS (l'Aeronautica Russa) contestandone la superiorità in teatro ed impedendone il conseguimento dell'*air dominance* completa.

Ebbene, sia gli Stati Uniti che i *partner* NATO avevano già mutato la loro percezione al riguardo, riorientando strategie e dottrine, alla luce di quegli scenari esaminati nel Cap.1 e che vedono l'affermarsi di una serie di attori – la Russia, il caso più eclatante, ma a questa bisogna aggiungere anche la Cina ed alcune potenze regionali – che perseguono politiche non solo maggiormente assertive e "dinamiche" ma che sono anche disponibili a mutare l'ordine regionale/internazionale, come, appunto, il caso della Russia con l'Ucraina.

Per il conseguimento dei loro scopi tali attori possono perseguire strategie di conflitto ibrido o di fatto compiuto tese ad "isolare" dagli Stati Uniti una serie di obiettivi periferici e a disarticolare le cinture di contenimento tradizionalmente create dagli stessi Stati Uniti.

Strategie cosiddette “sotto soglia” che, puntando su velocità di pianificazione ed esecuzione, mascheramento, pressione, ecc. mirano a conseguire l’obiettivo prima che la controparte sia in grado di mettere in campo una reazione organica e coerente. Da un punto di vista militare queste strategie sono sorrette dalla creazione di aree di esclusione/interdizione basate sulla stratificazione di sistemi *stand-off* – antiaerei, antinave e balistici/da crociera – e sul loro impiego ai fini della “fratturazione” dell’eventuale risposta/azione della controparte in termini di spazio, tempo e funzione. Tuttavia – ancora una volta, come dimostrato dall’Ucraina – i succitati attori possono anche utilizzare lo strumento della guerra convenzionale su larga scala, non avendo remore anche a subire costi e perdite molto elevate.

Per rispondere in maniera globale a queste strategie, gli Stati Uniti²⁴, ormai qualche anno fa, hanno lanciato il concetto/approccio delle operazioni multi-dominio. Il presupposto del multi-dominio è, come si diceva, la percepita erosione della superiorità convenzionale americana ed occidentale con il venire meno della *dominance*²⁵ data per scontata per tutto il trentennio successivo al Crollo del Muro di Berlino. Bisogna, dunque, ragionare, pensare ed agire in termini diversi, molto più dinamici e flessibili, rispetto a quanto non si faceva già con l’Air Land Battle²⁶ e la Network Centric Warfare. Occorre, dunque, un’integrazione ancor maggiore che consenta la rapida applicazione simultanea di capacità operative appartenenti a domini diversi (con l’inclusione pure di capacità non propriamente militari), ovvero i domini classici – terra, mare e cielo – ai quali si aggiungono quelli spaziale e *cyber* (senza dimenticare che si possono eventualmente considerare a sé stanti anche altri 2 domini: quello elettromagnetico e quello cognitivo). Le operazioni multi-dominio si possono allora definire come l’impiego coordinato e sinergico di piattaforme, sistemi e capacità ai fini del conseguimento di un effetto operativo cumulato (superiore alla sommatoria dei singoli effetti ottenibili con operazioni *single service* ma anche *joint* classiche) a prescindere da dove tali capacità, sistemi, ecc. risiedono o sono generati/concepiti. In altri termini, le operazioni multi-dominio invece di perseguire la vittoria soverchiante sul nemico puntano a sovraccaricare le capacità di reazione attraverso l’utilizzo di un *basket* capacitivo cinetico e non cinetico residente in tutti domini. In pratica, citando il famoso “O-O-D-A Loop” (Observe, Orient, Decide, Act) formulato da John Boyd, l’obiettivo è “fissare” il nemico nella fase O-O, riducendo e/o azzerando la sua capacità di decidere e agire.

24 In particolare l’US Army, da sempre vero motore, con il TRADOC (Training and Doctrine Command), dell’innovazione dottrinale militare americana.

25 Intesa nel caso del presente studio come air dominance.

26 Un esempio pratico della prima si ebbe con la prima Guerra del Golfo (Desert Storm).

Le operazioni multi-dominio si basano su 3 cardini. Il primo è la distribuzione spaziale delle forze, intesa sia come combinazione tra posizione, capacità di manovrare su distanze strategiche e di disaggregarsi/riaggregarsi a seconda delle circostanze, sia come capacità di offrire al nemico una ridotta impronta di *targeting* per complicarne il ciclo.

Da questo punto di vista il Potere Aereo in generale, e la sua evoluzione verso i sistemi di combattimento aereo del futuro (FCAS, Future Combat Air System)²⁷, garantisce più di ogni altro la possibilità di assicurare la distribuzione delle forze: in cielo non ci sono “confini” o ostacoli orografici, e le distanze sono più rapidamente percorribili. Dunque, capacità intrinseca di operare in maniera distribuita, e rapidità intesa sia come rapidità di azione e reazione, e capacità di colmare le distanze e di disaggregarsi/riaggregarsi, sia come capacità di assicurare la convergenza degli effetti. In generale, il Potere Aereo è maggiormente flessibile e versatile rispetto al potere navale e terrestre e più adattabile al concetto di operazione *cross-domain*, essendo meno vincolato alla propria dimensione operativa naturale.

Il secondo cardine è la creazione e l'impiego di formazioni multi-dominio, ovvero di formazioni in grado di operare con una certa autonomia in maniera *cross domain* con la necessaria letalità e resilienza. Stiamo parlando di formazioni sempre più flessibili, con una configurazione variabile e non ortodossa, una dimensione calibrata sulla missione e la capacità di operare in autonomia per adattarsi ad un teatro operativo dinamico ed imprevedibile. In linea di principio, tali formazioni devono poter disporre di un *basket* capacitivo molto ampio: comando e controllo, ISTAR, EW, sistemi autonomi, sistemi per l'ingaggio a lungo raggio e per il fuoco di profondità, sistemi anti-missile/anti-aerei, anti-razzo ed anti-drone, ed, infine, sistemi Cyber. Ciò non significa che ogni formazione debba avere organicamente quanto appena menzionato, ma che sia comunque capace, a prescindere dal suo posizionamento e dal suo livello ordinativo, di potere generare degli effetti potendo coordinare, per esempio, il fuoco di fonti “terze”, o assetti ISR, facendo all'occorrenza pure il *take over* di UAV ad alte prestazioni, senza dover passare da nodi di comando sovraordinati gerarchicamente. In altri termini, se una capacità non è disponibile organicamente, è necessario che nella formazione multi-dominio risieda la possibilità di coordinarla, dirigerla e farla convergere sul punto desiderato interpretando in autonomia una data situazione tattica. Ciò in maniera continua e cumulativa.

27 In questa categoria rientrano tanto sistemi europei quali il Tempest e lo SCAF, quanto sistemi americani come il NGAD (Next Generation Air Dominance).

Giusto per fare alcuni esempi, in campo navale una formazione distribuita basata su una fregata e su alcune unità navali *unmanned*, o a basso livello di pilotaggio, potrebbe rimpiazzare un Surface Action Group su 3 DDG, mentre il classico pacchetto formato da caccia e velivoli di scorta potrebbe essere rimpiazzato da un pacchetto comprendente un caccia che opera come velivolo C2ISR che coordina droni e gregari di diverso tipo per compiti EW, ISR e/o “suicidi”/strike e/o guida sui bersagli missili *stand-off* lanciati da altre piattaforme. In campo terrestre, invece, al posto delle tradizionali grandi formazioni pesanti/meccanizzate, possiamo immaginare complessi minori basati su veicoli ruotati altamente mobili, dispiegabili e proiettabili, dotati di una robusta capacità di C2 “on the move” e di una vetronica superiore, capaci di operare con droni e *loitering munitions*, ed affiancati/integrati con UGV per missioni logistiche e ISR ma anche di supporto di fuoco.

Ancora una volta il potere aereo, con la sua ultima evoluzione nei sistemi di combattimento aereo del futuro, è quello maggiormente in grado di garantire la possibilità di operare con formazioni ampiamente flessibili, e ridondanti, capaci di garantire autonomia, letalità, persistenza e resilienza.

Il terzo cardine è la convergenza, intesa come la rapida e continua integrazione delle capacità in tutti i domini ai fini di ottimizzare gli effetti e mandare in crisi il nemico impedendogli di decidere ed agire in maniera coerente. Da questo punto di vista, l'integrazione dei domini non è semplicemente l'estensione del concetto “jointery” con l'aggiunta delle componenti spazio e *cyber*, bensì il coordinamento/ottimizzazione delle azioni/attività condotte in tutti domini, per sortire l'effetto desiderato, con: 1) precisione e simultaneità; 2) dove richiesto; 3) quando richiesto, affinché l'effetto finale desiderato sia maggiore della semplice somma degli effetti prodotti nei singoli domini. Il valore aggiunto sta quindi nel poter riunire l'intera gamma di capacità letali e non, militari e non, e integrarne l'uso per il massimo vantaggio. Si può dunque affermare che maggiore è il livello di accuratezza e di sincronizzazione di dette azioni nei diversi domini, tanto più è possibile la convergenza degli effetti sul punto, o i punti, desiderato/i. In tal senso il classico approccio lineare e “geometrico” alle operazioni militari, retto da parametri quali distanze, gittate e tempi di percorrenza, deve essere necessariamente rivisto ed esteso, perché più esteso e multidimensionale è il campo di battaglia. Anche in questo caso il Potere Aereo è quello che per natura è più idoneo ad operare in contesti non lineari ed estremamente dinamici, dove il tempo diventa un fattore ancor più importante, dove le distanze tendono a ridursi e dove è necessario essere rapidi, presenti, persistenti e adattivi.

4.2 L'F-35 come *battle manager* e nodo multi-dominio

Prima di esaminare nei paragrafi successivi l'organizzazione ed il funzionamento di un modello di sistema di combattimento aereo del futuro, o di sesta generazione che dir si voglia, occorre fare un passo intermedio e soffermarci sull'F-35 e su quanto questa macchina sia rivoluzionaria rispetto alla generazione precedente e quanto questa abbia anticipato alcune delle caratteristiche che vedremo meglio espresse nel FCAS.

Innanzitutto, possiamo dire che l'F-35 è un velivolo che per sua natura si presta in maniera ottimale ad operare in un contesto multi-dominio. Nella stessa macchina, difatti, coesistono capacità diverse che si completano e che consentono all'F-35 di caratterizzarsi come un nodo complesso capace di svolgere:

- attività di raccolta e aspirazione dati. In tal senso l'F-35 rappresenta una vero e proprio aspirapolvere capace di raccogliere dati di diverso tipo, sia in campo elettromagnetico che in campo infrarosso;
- attività di elaborazione, processamento e prioritizzazione dati, e creazione di un quadro tattico organico e coerente;
- attività di distribuzione dati. Più in dettaglio la condivisione con altri F-35 avviene tramite il *datalink* dedicato a bassa rilevabilità MADL, mentre con le altre piattaforme attraverso il Link 16;
- attività di comando, controllo e gestione operativa, intesa come capacità di coordinare/guidare le altre piattaforme sulla base dell'evoluzione della situazione tattica;
- attività di *strike* di precisione, intesa come capacità di scoprire bersagli mobili o fissi e neutralizzarli con un alto grado di confidenza, riducendo e contenendo i tempi di tutto il ciclo localizzazione-attacco, grazie a sensoristica e bassa rilevabilità;
- attività di interdizione aria-aria, intesa come capacità di svolgere il combattimento aereo con grande efficacia (nonostante una formula aerodinamica non propriamente da caccia); ancora grazie a sensoristica e bassa rilevabilità, e ad un *software* di controllo del volo all'avanguardia.

Se immaginiamo uno scenario multi-dominio, abbiamo i nodi superiori di comando e controllo, posti generalmente a migliaia di chilometri dal teatro di battaglia e dall'area di minaccia, le piattaforme di supporto strategiche (*tanker*, AWACS, velivoli SIGINT, ecc.), che operano a distanza di sicurezza dall'area di minaccia, i nodi complessi, appunto i velivoli di quinta generazione come l'F-35, e i nodi elementari, caccia *legacy*, UAV, ecc. L'F-35 rappresenta dunque una sorta di elemento mediano che garantisce la continuità dell'azione operativa ed il coordinamento tra il livello strategico e quello tattico, grazie anche alle

caratteristiche di bassa rilevabilità e grande autonomia che gli permettono di penetrare buona parte delle difese avversarie, entrandovi e uscendovi all'occorrenza, e di essere persistente²⁸.

Da questo punto di vista, l'F-35 è una macchina che può trasmettere e ricevere informazioni in tempo reale dialogando con diverse piattaforme e coordinandone l'azione. Non solo, i dati ricevuti possono ulteriormente essere raffinati grazie all'elaborazione ed alla fusione di bordo e trasformati in un'informazione di alta qualità che la macchina può distribuire all'utilizzatore più opportuno nel momento più appropriato all'azione che è necessario fare sulla base della pianificazione prevista o dell'opportunità che si viene a creare su un campo di battaglia dinamico. Insomma, *intelligence* azionabile a tutti gli effetti, *intelligence* cioè produttiva di un'azione operativa, rilasciata da un "mediatore" di informazioni multi-dominio e da un connettore del campo di battaglia. L'F-35 può, infatti, ricevere e fornire dati via link 16, o attraverso altri *data link* tattici, da e a droni, FAC, navi, centri di comando superiori e così via, comportandosi, anche grazie alla presenza del pilota a bordo, come un centro avanzato per la gestione tattico-operativa. La presenza del pilota a bordo è fondamentale perché è il pilota che in determinate circostanze può garantire quella verticalità e quella contestualizzazione che anche la macchina più sofisticata non potrà mai offrire. A tali caratteristiche bisogna aggiungere la possibilità, in corso di implementazione con la *release* di *software* Block 4 (di cui parleremo nel paragrafo conclusivo di questo capitolo), di controllare direttamente i droni utilizzandoli per massimizzare l'effetto ottenibile sul campo di battaglia attraverso la moltiplicazione del carico di missione e la moltiplicazione delle varie funzioni operative.

Tutto questo è reso possibile dall'Integrated Common Processor (ICP), ovvero da un processore di nuova generazione dotato di una potenza di calcolo enorme e connesso a tutti i sistemi di bordo. L'ICP, è una macchina con una capacità superiore di un ordine di magnitudo alla capacità del processore installato a bordo dell'F-22 ed è in grado di processare tutti i dati provenienti dai diversi sensori di bordo, ma anche da sensori esterni, e di analizzarli e presentarli in maniera semplice ed immediata al pilota. Dall'ICP dipende, pertanto, la *sensor fusion* dell'F-35 e, cioè, la capacità di raccogliere, analizzare e processare le informazioni presentando alla fine al pilota un dato univoco, contraddistinto da un unico simbolo, e sgravandolo così dalla necessità di dover lui stesso analizzare e valutare la mole dei dati grezzi. Allo stesso tempo l'ICP può "aiutare" il pilota, qualora questo

28 L'F-35, nella sua versione CTOL, è un caccia nell'ordine delle 30 t di peso massimo al decollo, con un'importante dotazione di carburante interno. Nel complesso la variante CTOL del velivolo può immagazzinare ben 18.250 libbre di carburante, contro, per esempio, le poco più di 7.000 dell'F-16 (o le 11.000 dell'Eurofighter Typhoon o, ancora, le 13.500 libbre di un F-15E senza i CFT).

lo richieda, a “verticalizzare” l’informazione su una certa minaccia. Per analizzare, prioritizzare e fondere tutti i dati ricevuti, l’ICP usa algoritmi dedicati, distinti per ciascuna funzione.

In definitiva l’F-35 è una macchina realmente “omni-ruolo”, che ha anticipato molte di quelle caratteristiche che vedremo espresse ancora meglio e su larga scala nei sistemi di combattimento aereo del futuro, al cui centro opererà il caccia di sesta generazione. Prima però di affrontare più nel dettaglio l’argomento FCAS (Future Combat Air System) ci sembrava doveroso soffermarci per un attimo anche sul programma NATO per il rimpiazzo della flotta di velivoli AWACS.

4.3 AFSC: il *key enabler* NATO per la sostituzione degli AWACS

Uno dei programmi più interessanti, insieme a TEMPEST e SCAF²⁹, nel contesto di un nuovo concetto per un C2 aereo di nuova generazione è sicuramente quello riguardante il futuro sostituito della flotta di AWACS della NATO. Come noto, infatti, entro il 2035 è previsto il ritiro dei velivoli NATO E-3A AWACS (*Airborne Warning & Control System*) e l’ingresso in servizio di un sostituto. Al fine di determinare come l’Alleanza sostituirà tale fondamentale asset strategico, per mantenere le sue prerogative in termini di *situational awareness* e C2 aeroportato, durante il vertice NATO del 2016 a Varsavia è stata lanciata ufficialmente l’iniziativa *Alliance Future Surveillance and Control* (AFSC). Il progetto AFSC è valutare la possibilità di svolgere le missioni attualmente ricoperte dagli AWACS, secondo una logica di sistema dei sistemi mediante l’integrazione con sistemi già esistenti - garantendo l’interoperabilità – ma pure con quelli che verranno introdotti per affrontare i nuovi scenari. Come effetto operativo, l’AFSC cambierà sostanzialmente rispetto agli AWACS che andrà a sostituire. Intanto, si tratterà, come si accennava poco fa, di un sistema distribuito che, quindi, difficilmente rappresenterà una mera sostituzione integrale degli attuali velivoli E-3A SENTRY. Per quanto la NATO non abbia ancora espresso requisiti consolidati, è verosimile ritenere che, anche in questo caso, come nel sistema di combattimento aereo di sesta generazione, vi possa essere un “velivolo madre” capace di coordinare piattaforme e dispositivi diversi (aerei, terrestri, ecc.) dedicati alla scoperta/raccolta di informazioni e a garantire ridondanza al sistema dei sistemi di combattimento vero e proprio.

L’AFSC dovrà fornire capacità di sorveglianza e controllo multi-dominio all’interno dell’intero spettro di possibili scenari operativi (permissivi, contestati, negati, ibridi, ecc.). Dovrà, inoltre, disporre di sistemi di stoccaggio e trasmissione/distribuzione dati (ad ampia larghezza di

29 I due programmi per i sistemi di combattimento di sesta generazione sono, rispettivamente, anglo-italiano-svedese, e franco-tedesco, per ora.

banda e che sfruttino *datalink* tattici e reti commerciali) allo stato dell'arte, al fine di garantire un adeguato supporto ai centri di comando e controllo dell'Alleanza Atlantica, affinché le forze siano poi in grado di operare nel miglior modo possibile in ognuno dei 5 domini (aereo, cibernetico, navale, spaziale e terrestre). Inoltre, il velivolo madre dovrà possedere elevate capacità di sopravvivenza e di autoprotezione, considerando una minaccia sempre più sofisticata e a lungo raggio, nonché una spiccata modularità, scalabilità e "aggiornabilità". Le capacità principali dell'AFSC saranno, grosso modo, le seguenti:

- scoperta e tracciamento di bersagli aerei, ma anche terrestri e navali, grazie all'adozione di antenne AESA sempre più potenti e basate su componentistica GaN (nitruro di gallio);
- creazione di una battlespace situational awareness e di una picture operativa comune, accurata, integrata e costantemente aggiornata in tempo reale, e relativa distribuzione a tutti i nodi ed a tutte le pedine operative mediante potenti *datalink* di nuova generazione;
- controllo, coordinamento e direzione delle pedine operative per il contrasto delle minacce;
- eventuali compiti accessori (nella logica del supporto del sistema di combattimento aereo del futuro): relay di comunicazione, stoccaggio dati.

Per quanto concerne le tempistiche, a partire da febbraio 2017 il *North Atlantic Council* (NAC) ha designato la NSPA (*NATO Support and Procurement Agency* con sede in Lussemburgo) come ente responsabile degli studi dedicati alla nuova piattaforma e dello sviluppo dei concetti operativi e tecnologici. Attraverso tali attività, la NSPA sta valutando nuove tecnologie (riguardanti architetture di sistemi, sensoristica, automazione/intelligenza artificiale, processamento dati, scambio/condivisione informazioni, difesa cibernetica) ed esplorando un tipo di approccio basato, ancora una volta, sul concetto di "sistema dei sistemi" comprendente potenziali combinazioni di sistemi aerei, terrestri, marittimi, cibernetici e spaziali, capaci di lavorare insieme per raccogliere e condividere informazioni. A tale scopo, la NSPA ha costituito un ufficio preposto, l'*AFSC Project Office* (che dispone di un *budget* di 118,2 milioni di euro), che ha il compito di gestire le attività inerenti la fase di sviluppo del progetto AFSC in collaborazione con altri enti NATO, governi e annesse industrie. A dicembre 2018 si è conclusa la prima fase del programma, con la definizione dell'architettura base e dei requisiti e con lo sviluppo di 4 "*Small Case Studies (SCS)*". Si è poi proseguito con la Fase 2, definita "*Concept Stage*", il cui scopo era sviluppare e analizzare la fattibilità dei potenziali concetti (*High Level Technical Concepts, HLTC*), mentre ad aprile 2022 la NSPA ha assegnato 3 contratti per l'avvio di uno studio di Risk

Reduction & Feasibility (RRF). I 3 contratti sono stati assegnati rispettivamente a General Atomics, al consorzio ABILITI (composto da Boeing, Indra, Leonardo, Inmarsat, Thales, ESG, Lufthansa Technik, e Mott MacDonald), e al consorzio ASPAARO (formato da Airbus, Northrop Grumman, BAE Systems, MDA Systems, Lockheed Martin, Kongsberg Defence and Aerospace, GMV Aerospace, Exence S.A., e IBM).

4.4 Il sistema di combattimento aereo del futuro

I sistemi di combattimento aereo del futuro – dal TEMPEST, allo SCAF passando per il Next Generation Air Dominance americano – possono essere considerati senza dubbio il cardine ed il cuore delle operazioni multi-dominio.

Ma cosa si intende con precisione per Future Combat Air System? Si intende un sistema dei sistemi aereo che in tutte le sue componenti combinate è chiamato ad effettuare la missione in maniera coordinata e sinergica utilizzando un’infrastruttura basata su comando, controllo e comunicazione di nuova generazione di tipo distribuito implementabile grazie a 3 nuove tecnologie *disruptive* - intelligenza artificiale, super calcolo e *combat cloud* – e a *datalink* di nuova generazione contraddistinti da altissima velocità e capacità di trasferimento di enormi volumi di traffico, e da resilienza *cyber* e auto-adattabilità.

Senza questa infrastruttura il FCAS non potrebbe esistere ed operare come tale. Ad onor del vero il sistema dovrebbe poter operare anche in assenza del *cloud*, e delle comunicazioni, continuando ad assicurare l’efficacia della missione. Per questo, come discutevamo già nel precedente capitolo, si parla già di bolle e *network* di opportunità, basati su UAV operanti come *data relay* e micro-satelliti in orbita bassa, e su un *cloud* ed un *computing* ad alte prestazioni di tipo flessibile e modulare, capace cioè di assicurare le funzionalità richieste e non pregiudicare l’efficacia della missione a causa di un singolo “point of failure” (il concetto di resilienza calibrata nel tempo e nello spazio in base alla tipologia ed all’ampiezza della missione).

Da un punto di vista “organizzativo” l’Air Combat System è composto dai seguenti elementi:

1. il caccia madre di sesta generazione, denominato anche “core platform”;
2. gli *adjunct*, ovvero i droni/UAV gregari che lo dovranno coadiuvare ed accompagnare nella missione;
3. gli *effector*, ovvero quel complesso di sistemi, sensori o più semplicemente capacità in grado di produrre un effetto sul campo di battaglia, tale da poter essere messo a sistema con gli altri effetti per creare un cumulo.

Partiamo con il caccia di sesta generazione. In via generale, diciamo subito che con la *core*

platform si amplia notevolmente il tradizionale ruolo del caccia³⁰. Innanzitutto, la *core platform* dovrà essere capace di difendersi e attaccare in egual misura, dato uno scenario altamente contestato, con densità di minaccia e persistenza delle difese antiaeree avversarie, inquinamento elettromagnetico, alta dinamicità dei *target* e così via. In scenari come questi nessuno dei due aspetti potrà essere trascurato, per cui si dovrà pensare ad una macchina capace di condurre con efficacia missioni di *defensive counter air* ed offensive counter air, ma anche di ingaggiare bersagli a terra come siti e batterie della difesa aerea, centri di comando e controllo, lanciatori per missili balistici e/o antinave, ecc. È per questa ragione che il caccia di Sesta Generazione dovrà mantenere le caratteristiche tattiche tipiche di un caccia e per questa stessa ragione il ruolo di “madre” non potrebbe essere svolto da un aereo da trasporto, o da un altro tipo di velivolo “commerciale” – come emerso anche di recente in certi studi e valutazioni – ai quali, ovviamente, per natura e struttura mancano certi attributi: velocità, maneggevolezza, bassa osservabilità e così via.

Secondo, il caccia madre dovrà operare come nodo C2 avanzato al quale spetterà il compito di gestire tatticamente la missione coordinando simultaneamente gli *adjunct/gregari*, guidando missili ed armi di vario tipo e raccogliendo, analizzando e distribuendo informazioni. Insomma, la *core platform* dovrà gestire quel *network* distribuito necessario per complicare il ciclo di pianificazione e il *targeting* dell'avversario. Dunque, la *core platform* dovrà avere anche delle caratteristiche tipiche degli AWACS, operando come un *battle manager* o, se si preferisce, come un vero e proprio *quarterback* dell'aria incaricato di dirigere e coordinare l'azione tattica nel suo complesso. Da qui, appunto, il coordinamento degli *adjunct* che ne dovranno costituire elemento di moltiplicazione operativa in uno spettro molto ampio di ruoli - comunicazioni, *strike*, ISR, ecc. - pur non dovendo dipendere da essi per le proprie prestazioni funzionali. Questo è un aspetto cruciale per capire cosa potrà essere veramente la *core platform*, ovvero un assetto in grado di svolgere comunque una serie di missioni autonomamente, a prescindere dai gregari. Prendiamo, per esempio, uno *scramble*, ovvero una missione per la quale sono richieste prestazioni di spunto e velocità impossibili per un *adjunct*, a meno di non alterarne la natura ed il rapporto di costo-efficacia. Insomma, come dice il nome, gli *adjunct* dovranno “semplicemente” aggiungere qualcosa alla *core platform*: ridondanza, persistenza, copertura e così via. L'*adjunct* è pertanto un “enhancer” ed un moltiplicatore, non un qualcosa che sostituisce funzionalità base del caccia madre.

30 Che può svolgere essenzialmente 2 ruoli primari: la difesa aerea e l'intercettazione di aerei avversari, e l'attacco contro bersagli al suolo. In alcuni casi, esistono velivoli con una predominanza nell'uno o nell'altro ruolo (caccia da superiorità aerea o velivolo per l'attacco al suolo/bombardiere), in altri velivoli tali capacità sono disponibili più o meno in egual misura sulla stessa macchina (caccia multiruolo).

Come terzo elemento, infine, aggiungiamo le capacità ISR. Anche questo è un altro aspetto da mettere bene a fuoco perché qui non si tratta, come nel caso dei caccia di quinta generazione, solo di capacità NTISR (Non Traditional ISR), ovvero di capacità ISR disponibili su piattaforme non dedicate, ma di vere e proprie capacità di *intelligence*. Cosa significa questo? Significa che il caccia madre dovrà raccogliere un'enorme mole di informazioni e, grazie all'AI, elaborarla, analizzarla e categorizzarla non solo per presentare al pilota un dato organizzato e coerente affinché egli abbia di fronte un quadro tattico snello ed esaustivo, ma anche per trasformarla in *intelligence* di qualità. *Intelligence*, cioè, di tipo strategico, da capitalizzare nelle situazioni di competizione e crisi, e di tipo azionabile da capitalizzare nelle situazioni di crisi e scontro aperto. Resta solo da capire, e questo è oggetto delle attività di ricerca e sviluppo oggi in corso sui sistemi di combattimento aereo di sesta generazione, quanto di questa attività d'*intelligence*, intesa come analisi, potrà essere svolta a bordo della *core platform*, e quanto, invece, nel *cloud* o nelle stazioni a terra. Tuttavia, è chiaro che pure sul caccia madre dovrà risiedere un certo livello di analisi, altrimenti si rischia che il velivolo non sia in grado di gestire le evoluzioni tattiche più complesse.

Per quanto riguarda le caratteristiche tecniche del caccia madre, tra queste vi sarà senza dubbio la grande autonomia. I *mockup* del TEMPEST e dello SCAF presentati finora lo mostrano al di là di ogni dubbio, e del resto nei contestati scenari futuri le missioni saranno lunghe e complesse, e si dovrà dunque essere persistenti operativamente, anche perché l'ISR sarà una componente fondamentale, soprattutto durante le fasi di competizione e nelle aree più grigie delle crisi. Questo significa che l'attività di ISR non dovrà essere svolta in via esclusiva solo con gli assetti dedicati, ma con tutto ciò che è possibile e disponibile in quel momento; dunque, e ovviamente, anche con la *core platform*.

Un'altra caratteristica rilevante sarà la bassa rilevabilità, intesa in questo caso come *mix* tra bassa riflettività radar – possibilmente *all aspect*³¹ – bassa segnatura termica – intesa come superiore capacità di gestione della traccia IR della macchina – e bassa impronta elettronica. Su quest'ultimo aspetto conviene soffermarsi ancora un attimo. Prima di tutto, con bassa impronta elettronica si intende la capacità di ridurre la probabilità di intercettazione delle proprie emissioni elettromagnetiche, ovvero di rendere estremamente complicato per l'avversario rilevare la posizione di una *core platform* a causa delle sue emissioni nello spettro elettromagnetico. In secondo luogo, si intende la capacità di

31 Ad oggi il solo F-22 e il bombardiere B-2 SPIRIT - nel campo dei velivoli con pilota a bordo - possono esprimere tale bassa rilevabilità "all aspect", laddove nell'F-35 si è preferito invece limitare la stealthness soprattutto alla sezione frontale e, soprattutto, contro la minaccia rappresentata dai radar operanti nelle bande "strette", ovvero la X e la Ku.

minimizzare la rilevazione avversaria “seducendola”, “deviandola” o semplicemente “cancellandola”, impiegando la suite EW integrata di bordo.

Tuttavia, vale la pena osservare che nel caccia madre di sesta generazione la bassa rilevabilità, in particolare la bassa riflettività radar, dovrà essere correttamente combinata ed armonizzata con il requisito della velocità. Il contenimento della riflettività è difatti legato non solo e non tanto all’adozione di RAM (Radar Absorbing Materials), ma anche, se non soprattutto, all’adozione di superfici e geometrie ispirate al criterio *stealth*, ovvero alla necessità di restituire l’onda in direzioni diverse da quella di provenienza e/o con un segnale molto attenuato. Tale qualità – che richiede il rigoroso rispetto di certi criteri quali allineamento in pianta delle superfici, tolleranze sostanzialmente pari a zero in termini di discontinuità e gap strutturali, ecc. - va però armonizzata con la necessità per una *core platform* di sesta generazione di operare per lunghi periodi in super-crociera, in modo tale da ridurre al minimo i tempi di intervento e di transito in teatri altamente dinamici e cangianti. Da qui, appunto, il bisogno di un corretto compromesso tra bassa osservabilità e velocità. Infine, un cenno anche alle dimensioni ed all’avionica. Per quanto riguarda il primo aspetto, il caccia di “sesta” non potrà essere piccolo: si parla già oggi di un peso massimo al decollo attorno alle 35 t, ed i *mockup* di FCAS e TEMPEST ancora una volta lo dimostrano chiaramente. Saranno, infatti, necessari ampi spazi a bordo per ospitare dispositivi di generazione elettrica e di raffreddamento con i quali alimentare armi di nuova generazione, a cominciare da armi ad energia diretta, ed un propulsore in grado di garantire un alto rapporto spinta/peso e capace di ottimizzare il ciclo di funzionamento in base ai profili di missione ed ai consumi. A ciò bisogna poi aggiungere la necessità di trasportare internamente un quantitativo di armamento presumibilmente superiore a quello oggi disponibile nei vani bombe dell’F-22 piuttosto che dell’F-35.

Per quanto riguarda l’avionica, con la sesta generazione le caratteristiche di integrazione, elaborazione/analisi e *sensor fusion* verranno spinte ad un livello ancora superiore (rispetto alla quinta generazione) ed ulteriormente potenziate grazie all’estensivo uso dell’AI, mentre l’uso della realtà aumentata migliorerà sensibilmente l’interfaccia uomo macchina. Proprio in termini di interfaccia uomo-macchina, già oggi le industrie stanno lavorando su dimostratori e prototipi di *cockpit* in cui l’elemento centrale diventa il casco indossato dal pilota su cui immersivamente viene proiettata tutta la strumentazione, i pannelli e i *display*, mentre fisicamente nel *cockpit* restano solo la *cloche* e la manetta di pilotaggio. In pratica il pilota interagisce con una realtà completamente sintetica, mentre, grazie a sofisticati algoritmi di tracciamento oculare, i comandi possono essere impartiti solo con il movimento della testa e degli occhi. Questi concetti sono in corso di sperimentazione anche presso

l'avanzato Battle Lab ospitato nello stabilimento di Torino della Divisione Velivoli di Leonardo. Qui sono presenti anche un generatore di scenario – in pratica un grande schermo a parete su cui vengono riprodotti complessi scenari multi-dominio – ed una *prototyping pilot station* di sesta generazione, in cui è possibile vedere proiettati su uno schermo, per esempio, i video ripresi da droni gregari.

Il secondo elemento costitutivo del sistema di combattimento aereo del futuro è come si diceva rappresentato dai gregari/adjunct. Si tratta di droni dotati di autonomia, capaci di agire su comandi di alto livello e con un certo livello di coordinamento. Il concetto in questo caso è evidentemente diverso da quello del drone classico pilotato da remoto, e rimanda piuttosto a quello di droni che operano autonomamente su una pianificazione ed una direzione fornita dallo stesso caccia madre o da un qualunque altro nodo di comando. A ciò bisogna aggiungere che si tratta di macchine pensate sin dall'inizio per operare in maniera strettamente coordinata con i velivoli pilotati secondo il concetto MUM-T (Manned Unmanned Teaming).

Al momento sono state identificate tre diverse categorie di *adjunct*: “survivable”, “attritable” ed “expendable”. La prima categoria comprende droni prestanti, sofisticati e recuperabili, capaci di svolgere più missioni. In pratica, stiamo parlando di veri e propri UCAV, con delle dimensioni comprese in un *range* tra le 4-5 t e le 12-15 t, e prestazioni in tutti i settori significativi. Gli *attritable*, rispetto ai *survivable*, sono droni meno sofisticati, capaci di svolgere comunque più missioni, che possono essere recuperati ma pure persi in virtù di un costo più contenuto rispetto a quello dei *survivable*. Il Boeing ATX Ghost Bat ne costituisce un esempio, così come l'XQ-58 Valkyrie della Kratos, con la differenza che il primo è dotato di carrello mentre il secondo è “runway agnostic” in quanto lanciabile da un sistema pneumatico e recuperabile tramite paracadute. Infine, l'*expendable* è il drone che svolge una sola missione e che “muore” con essa. In pratica, qualcosa di assimilabile ad una “loitering munition”, che a seconda della missione può portare o un carico bellico o un sensore o, ancora, che può operare semplicemente come esca/stimolatore.

La terza componente del FCAS è costituita dagli *effector*, ovvero da “elementi” capaci di produrre un effetto, sia esso cinetico che non cinetico: per cui l'*effector* può essere un'arma, un missile, un sensore e così via. Insomma, un qualcosa che abbia la capacità di produrre un effetto: distruzione fisica, ma anche un effetto d'*intelligence*, trasportando uno o più sensori e *datalink* per la ritrasmissione delle informazioni ai nodi, o un'azione di disturbo (inganno, attività *cyber* offensive, ecc). Più in dettaglio, si tratta di un complesso che va dai missili a lungo raggio super e ipersonici, a sistemi di guerra elettronica ed a capacità ISTAR sempre più spinte, passando per capacità di attacco *cyber*, di rilevazione nel campo radar

e IR, e così via. Capacità che, come abbiamo visto, devono essere distribuite ed “abbassate” fino ai livelli tattici più elementari nella consapevolezza che più si è piccoli meno si è rilevabili, ma che per essere piccoli bisogna essere anche letali o quanto meno esprimere un certo tipo di capacità sia direttamente che indirettamente.

In un contesto multi-dominio, molto complesso e dinamico, il FCAS sarà uno degli elementi abilitanti del *combat power* di Forze Armate di Paesi avanzati e sofisticati. Dovrà, dunque, essere uno strumento straordinariamente flessibile – molto più flessibile rispetto agli “analoghi” sistemi dei sistemi terrestri o navali – utilizzabile in vari modi durante tutte le fasi del *continuum* conflittuale competizione-zona grigia/crisi-guerra, grazie ad uno spettro di capacità particolarmente ampio, per non dire completo. Per cui nella fase di competizione il FCAS sarà chiamato a garantire la necessaria deterrenza dell’eventuale azione ostile, assicurando nel contempo capacità di sorveglianza e monitoraggio dei *target* e delle vulnerabilità dell’avversario, ricerca dei *point of failure*, e capacità *counter-recon*. In questa fase l’obiettivo principale è acquisire *intelligence* strategica, da utilizzare per il mantenimento del posizionamento competitivo del Paese di cui quel FCAS è espressione³² o azionabile nel caso dalla competizione si passi a quelle di crisi e conflitto.

Nella fase di transizione alla crisi e di crisi, il FCAS potrà essere impiegato come strumento di contrasto alle strategie ibride e di fatto compiuto. In che modo? Innanzitutto, mediante l’impiego di capacità ISR e SIGINT, e sfruttando la superiorità nel settore delle informazioni, smascherando le condotte ibride e gli attori “maligni” che si celano dietro ad esse. In secondo luogo, segnalando l’indisponibilità ad accettare la condotta ibrida mediante *strike* limitati. Nel caso di iniziative di *fait accompli*, il FCAS può garantire una capacità di risposta immediata imponendo, mediante *strike* ad alta precisione e letalità, da subito un costo molto alto a chi intraprenda tale iniziativa. In entrambi i casi, l’obiettivo è porre l’avversario di fronte alla scelta se tornare alla normalità dello *status quo* e della competizione o, se, invece, scalare verso una guerra su larga scala.

Infine, qualora appunto la situazione scali ulteriormente, il FCAS assicurerà la necessaria capacità di *warfighting* e *combat*, la creazione e l’approfondimento dei gap nel dispositivo avversario e la completa libertà di manovra per le forze *joint*.

Più in generale, il FCAS garantisce il controllo di tutto lo spettro del *continuum* e del processo di scala. E questo perché, come già accennato, il sistema di combattimento aereo del futuro può vantare un’intrinseca flessibilità e versatilità data dall’ampia riconfigurabilità, ovvero dalla possibilità di variare il numero delle piattaforme e la tipologia degli effettori e di operare

32 Intelligence strategica sulle vulnerabilità di avversari e amici, da far valere poi sui tavoli e nei grandi congressi internazionali, dove si negoziano “quote di benessere”, e nelle trattative bi o multi-laterali affinché si possa trattare sempre da posizioni di vantaggio.

in maniera distribuita e ridondante. A questa caratteristica bisogna aggiungere la persistenza, ovvero la capacità del Future Combat Air System di “gravare” sull’avversario acquistando e mantenendo la superiorità informativa in un ciclo dinamico ed ininterrotto. Il FCAS, in virtù della sua architettura distribuita su più elementi, già di per sé offre notevoli caratteristiche in tal senso, ma un’ulteriore spinta può (deve) venire pure dall’integrazione con le piattaforme specialistiche *legacy*, a cominciare dai *tanker* e dagli aerei da trasporto, che possono essere riconfigurati installandovi capacità organiche di raccolta informazioni (ELINT, ISR) per renderle “macchine di opportunità” funzionali all’approccio multi-dominio capitalizzando al massimo le loro naturali caratteristiche di autonomia e persistenza operativa³³. Tali velivoli continuerebbero perciò a svolgere la loro missione *core* ma contemporaneamente potrebbero “aspirare” i dati con *pod* dedicati ri/inviandoli automaticamente al *cloud* per il processamento e l’analisi³⁴ o analizzandoli grazie a moduli “leggeri” di AI e super calcolo presenti a bordo. Insomma, una vera e propria rivoluzione multi-dominio.

33 Naturalmente oltre alla connessione con le piattaforme specialistiche *legacy*, sarà necessaria anche l’integrazione con i cosiddetti caccia *legacy*, che dovranno pertanto essere ammodernati con una serie di nuove tecnologie affinché possano operare al meglio ed in piena sinergia con il sistema di combattimento di sesta.

34 La mole di dati che viene solitamente registrata è enorme e richiede un processamento che convenzionalmente è molto dispendioso di risorse. La parte più critica è proprio la capacità di processing di tali big data in tempi minimi, facendo ricorso a AI/machine learning.

CAPITOLO 5

Nuove tecnologie e sensori di 5^a Generazione nel C2 distribuito

5.1 Verticalità vs orizzontalità: il ruolo dell'intelligenza artificiale e del super-calcolo

Nei capitoli precedenti abbiamo delineato un sistema di comando e controllo molto diverso dal tradizionale modello gerarchico, verticistico e centralizzato, e più simile, invece, ad un modello di tipo orizzontale in cui l'autonomia e la capacità decisionale è diffusa fino ai livelli tattici più bassi, ed in cui è necessario adattarsi dinamicamente ad uno scenario operativo molto complesso e rapidamente cangiante. In tale contesto, il comando e controllo deve assumere le vesti di una catena di nodi capace di rispondere ad esigenze di tipo diverse relative a *intelligence*, fuoco, logistica, ecc., ed allocare di conseguenza le risorse più opportune, secondo il principio del controllo distribuito e dell'esecuzione decentrata. Ma per far questo occorre un *mix* adeguato tra capacità umane e intelligenza artificiale/macchine *learning* grazie al quale raccogliere e processare grandi quantitativi di dati, prioritizzare e indirizzare le info, evitare il sovraccarico e la trappola del micro-management, e gestire con rapidità tutto il processo. Nel complesso, un sistema di comando e controllo così rivoluzionato ha tre obiettivi di fondo: comprendere più rapidamente e dinamicamente lo spazio di battaglia; gestire ed impiegare le forze più rapidamente dell'avversario ed ottenere effetti cumulati e sincronizzati sul campo di battaglia attraverso tutti i domini. In pratica, stiamo parlando di comprimere in maniera significativa i tempi del ciclo OODA (Observe Orient, Decide, Act) per restare sempre un passo avanti rispetto all'avversario.

Se prendiamo, per esempio, l'esigenza del fuoco, tale catena nodale deve essere in grado di gestire una rete d'ingaggio a partire da risorse e opzioni disperse/distribuite, sulla base di esigenze e richieste continuamente mutanti allocando ciò che è più idoneo in quella determinata finestra di opportunità ai fini del conseguimento di un effetto cumulato sulle vulnerabilità critiche del dispositivo nemico. La neutralizzazione e/o l'inabilitazione di tali elementi di vulnerabilità crea un effetto a cascata che potrebbe in ultima analisi portare al collasso ed alla disarticolazione del dispositivo avversario.

Per fare questo i nodi della catena devono avere la capacità di elaborare, analizzare e filtrare/priorizzare enormi quantitativi di informazioni messi a disposizione da una sensoristica sempre più pervasiva e ridondante, e da sempre più sofisticati strumenti di raccolta. Si tratta di una capacità che va oltre quella della mente umana e che necessita dell'ausilio di un "cervellone" rappresentato dall'intelligenza artificiale. In tal senso, l'AI è quello strumento con il quale gestire e dare ordine alla massa disorganizzata e orizzontale

dei dati sfruttando la possibilità di leggere/adattarsi rapidamente alla situazione apprendendo continuamente mediante il *machine learning*.

In questi casi si parla anche di architetture complesse definibili dall'acronimo C5ISTRE&N (Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, Targeting, Reconnaissance, Engagement & Neutralize), di cui fanno parte anche mezzi *unmanned*, anch'essi gestibili tramite AI. Gli sviluppi tecnologici in materia di AI appaiono legati a caratteristiche quali l'affidabilità, la robustezza, l'autoapprendimento costante e continuo, l'adattabilità e l'impiego di processori neuromorfici³⁵, tali da potenziare un aspetto chiave qual è la fusione di una grande quantità di informazioni, al fine di predire in tempo reale scenari tattici e strategici, valutare rapidamente le minacce e individuare le contromisure più idonee e dunque supportare le decisioni della catena di comando.

Tornando all'esempio della catena di gestione del fuoco, l'AI sarà quello strumento che consentirà di allocare in maniera simultanea e sincronizzata il fuoco a partire da risorse distribuite e disperse su tutto lo spazio della battaglia ed articolate *firing points* multipli. Schematizzando: raccogliere, analizzare, filtrare/priorizzare, assegnare/indirizzare, convergere. Sono questi i passaggi attraverso i quali la catena di ingaggio opera nell'ambito di un modello operativo che potremmo definire a mosaico, laddove le mattonelle di un mosaico rappresentano pedine disaggregate che possono essere riaggregate a seconda delle circostanze e delle esigenze, secondo configurazioni operative variabili per garantire la massima "survivability" possibile, e che possono essere utilizzate per ottenere la massima convergenza possibile degli effetti sul punto desiderato.

Lo stesso discorso vale per la logistica e l'*intelligence* con l'AI che potrebbe suggerire alla componente umana le mosse da intraprendere sgravandole dalle necessità di analizzare l'intero quadro informativo per ricavarne una serie di opzioni sostenibili. Pensiamo all'immagine di un grande scatolone, dove entra un enorme flusso di dati e informazioni, ed escono poche opzioni e/o scelte a disposizione degli operatori e degli utenti; nel nostro caso del nodo di comando e controllo o di un semplice soldato sul terreno e così via.

Per quanto appena descritto, intelligenza artificiale e la *big data analysis* diventano fondamentali, ovvero la *conditio sine qua non* un tale modello³⁶ non potrebbe essere implementato garantendo anche ai nodi di comando di più basso livello tattico la possibilità

35 Un processore neuromorfico è formato da neuroni artificiali (cioè unità di elaborazione con una memoria propria, frutto della nanotecnologia), correlati fra loro e stimolati attraverso informazioni in entrata. Esse vengono elaborate da ciascun neurone artificiale, che rilascia dunque informazioni ad altri neuroni dello stesso tipo, innescando un'elaborazione continua simile a quella del cervello umano, ma più rapida.

36 Peraltro, questo modello che potrebbe sembrare simile a quello precedente relativo alla Network Centric Warfare, è in realtà molto diverso perché se il primo presupponeva il controllo centralizzato da parte dei comandanti di teatro su tutte le forze sotto-ordinate, il secondo presuppone un controllo di opportunità da parte dei nodi tattici su quanto è spazialmente disponibile in un dato momento.

di avere le risorse decisionali e di supporto con le quali rendere possibile il controllo e la gestione di forze distribuite, l'adattamento all'ambiente e lo sfruttamento di quanto esso può offrire. Il tutto ai fini dell'imposizione di un ritmo operativo insostenibile per il "decision making" avversario.

Un tale sistema deve dunque essere in grado di combinare i vantaggi delle due intelligenze, ovvero flessibilità, creatività e improvvisazione per ciò che concerne l'intelligenza umana, e velocità e scala per l'intelligenza artificiale. Verticalità per l'intelligenza umana, ovvero possibilità di approfondire ulteriormente il dato e renderlo azionabile fino ai più bassi livelli tattici, e orizzontalità per l'intelligenza artificiale, ovvero possibilità di gestire la scala e la massa con una velocità ed un'immediatezza impossibili per la mente umana.

Soffermiamoci, però, più nel dettaglio sull'AI approfondendone il concetto e le possibilità. Innanzitutto, possiamo definire l'AI come quell'insieme di tecnologie che consentono alle macchine di auto-apprendere sulla base dell'esperienza e dei dati, di interagire con l'ambiente e di potenziare l'autonomia dei sistemi, e che costituiscono un elemento fondamentale per supportare l'uomo nella vita di tutti i giorni; nel "nostro" caso il militare in ogni condizione operativa. Non si tratta, come molti temono, di rimpiazzare il cervello umano con una macchina, ma di permettere ad una macchina di eseguire alcuni compiti tradizionalmente appannaggio dell'uomo ma alla velocità di un computer. In particolare quei compiti - ripetitivi, ridondanti e molti dispendiosi da un punto di vista dell'attenzione - che potremmo anche "definire", come abbiamo già fatto, orizzontali, in antitesi alla "verticalità" ed alla profondità tipiche della creatività umana. Inoltre la macchina, essendo capace di "apprendere" (*machine learning*), dovrebbe eseguire il compito assegnato sempre meglio ogni volta che lo ripete. L'AI ha un campo di applicazione molto vasto che spazia dall'osservazione della Terra – con la possibilità di elaborare un'immensa quantità di immagini satellitari, sia ottiche che radar, estraendone informazioni preziose sulla salute del pianeta, sulla sicurezza, sulla gestione delle emergenze, sull'analisi dei fenomeni atmosferici e così via – alla sicurezza fisica – si pensi al riconoscimento facciale – passando per la robotica e i cosiddetti AIS (Autonomous Intelligent System), senza dimenticare il settore cibernetico. In quest'ultimo caso, si stanno sperimentando ed implementando metodologie avanzate e innovative basate sull'analisi delle immagini al fine di classificare i *malware* all'interno dei *file*. Un segmento in cui l'AI assume un ruolo determinante nella gestione di grandi mole di dati, nella classificazione istantanea delle minacce e nella capacità di correlare le informazioni al fine di rilevare intrusioni.

L'AI, dunque, è fondamentale per elaborare e analizzare l'enorme mole di dati oggi a disposizione, ordinarla e priorizzarla affinché l'utente si trovi di fronte ad un quadro entro il quale può

prendere una decisione “informata”, idonea a produrre un risultato che va a cumularsi con altri in ciclo continuo e dinamico. In tal senso, moduli di AI saranno sempre più inseriti nei sistemi di comando e controllo di livello strategico, operativo e tattico, ma anche nei CMS navali, così come su quelle piattaforme aeree di nuova generazione che costituiranno il cuore dei sistemi di combattimento aereo del futuro di sesta generazione, ma anche sugli *adjunct* o gregari che le accompagneranno in operazione.

L’AI è legata tuttavia anche ad altre innovazioni tecnologiche *disruptive*, a cominciare dal cosiddetto “cloud computing”, declinato in ambito militare come “combat cloud”, inteso come grande magazzino remoto di stoccaggio dati di tipo “intelligente”.

“Cloud computing” e AI sono difatti correlati non solo dal punto di vista funzionale, ma anche dal punto di vista del loro sviluppo. Immaginiamo, per esempio, un programma per il riconoscimento facciale. La capacità di stoccare moltissimi dati permette al *software* di “imparare” (*machine learning*) a trovare le informazioni necessarie a identificare un volto. Una volta appreso, il programma è in grado di eseguire il compito in tempi rapidissimi e di continuare al contempo ad apprendere dai nuovi dati per diventare sempre più affidabile e capace. Gli algoritmi di questo genere richiedono una grandissima potenza di calcolo, tale da rendere sempre più urgente la necessità di disporre di supercalcolatori in grado di sostenere la potenza di calcolo dei nuovi algoritmi. Ed ecco quindi che qui si innesta il terzo grande filone del ciclo di innovazione attuale, ovvero quello del super calcolo. Un supercalcolatore è un complesso di *hardware* e *software* studiato per rimuovere, quanto più possibile, i limiti fisici che impediscono alle applicazioni di eseguire un insieme di compiti all’istante piuttosto che impiegare un tempo indefinito. I limiti sono, appunto, la potenza di calcolo (numero di operazioni per secondo), la quantità di memoria (numero di *byte* nella memoria centrale e su disco), e la banda di I/O (velocità di trasmissione dati sulla rete e sugli altri dispositivi). È chiaro che nessun “supercomputer” oggi esistente riesce a superare in modo definitivo tutti questi limiti, quindi nessuna applicazione può fornire i risultati richiesti all’istante, ma ci si aspetta che il tempo di soluzione si riduca al crescere della potenza del supercalcolatore. Per fare ciò non basta l’*hardware* ma occorre che il *software* sia scritto in modo opportuno per sfruttare l’architettura *hardware*: ad esempio, su tutti i supercalcolatori oggi esistenti il *software* deve consentire di eseguire le istruzioni in modo parallelo, in una gerarchia multi livello. Deve essere parallelo all’interno del singolo dispositivo (GPU e CPU), all’interno del nodo (per sfruttare la molteplicità dei *core*) e sulla rete (per sfruttare la presenza di centinaia di nodi computazionali). Questo è reso possibile da compilatori e librerie che supportano opportuni paradigmi di programmazione, studiati per facilitare la programmazione parallela.

Tutto il complesso *hardware* e *software* sopra descritto deve essere progettato e implementato per ottenere un supercalcolatore bilanciato nelle sue caratteristiche di potenza, memoria e banda di comunicazione in funzione degli obiettivi di riduzione dei tempi di calcolo, che possono essere diversi per i diversi *workload*. Per fare alcuni esempi di impiego classico, i supercomputer vengono usati per previsioni meteorologiche, studi sul clima (per esempio i programmi finanziati dal G8-HORCs), per creare modelli chimici complessi (calcolo di strutture e proprietà, modelli molecolari, ecc.), e simulazioni fisiche (simulazioni aerodinamiche, calcolo della resistenza dei materiali, simulazione di esplosioni di armi nucleari, studio della fusione nucleare, ecc.).

In tale ambito, per esempio, si colloca il supercomputer di Leonardo DaVinci-1 di Genova³⁷, di cui è partner l'azienda Atos. Si tratta di un supercomputer tra i primi in Europa, e il primo in Italia, ad essere dotato degli acceleratori di ultima generazione NVidia A100. Il DaVinci-1 conta su una batteria di oltre 100 unità di supercalcolo, per una potenza di calcolo complessiva superiore a 5PFlops (5 milioni di miliardi di operazioni in virgola mobile al secondo). Le unità sono collegate da una rete ad alte prestazioni e a un sistema di archiviazione dotato delle più recenti tecnologie *hardware* e *software*, per una capacità di memorizzazione dell'ordine dei 20Pbyte (20 milioni di Gigabyte). In generale questo modello di supercomputer coniuga la grande potenza di calcolo con la massima flessibilità consentendo l'impiego di algoritmi estremamente complessi (dal *deep learning* all'Intelligenza Artificiale), la personalizzazione per piattaforma tecnologica e il calcolo delle innumerevoli interazioni tra i dati generati (*data analysis* e *big data*).

Ma per cosa è utilizzato oggi DaVinci-1? Prima di andare nel dettaglio di alcuni esempi significativi, è bene ricordare che DaVinci-1 è stato installato alla fine del 2020 ed è entrato "in produzione", dopo una doverosa fase di test, collaudo e *tuning* solo a marzo 2021, dunque siamo solo agli inizi della sua carriera. Nonostante ciò, è già stato possibile sfruttarlo per importanti progetti di ricerca ed innovazione e, a partire dalla fine del 2021, ha iniziato a "servire" anche le ingegnerie delle Divisioni del Gruppo Leonardo. Tornando a quello che è possibile fare con DaVinci-1, essenzialmente il sistema è stato disegnato e concepito per dare il massimo delle prestazioni per sviluppare Digital Twin e sistemi di processamento per i *big data*, e per sviluppare e "addestrare" gli algoritmi di Intelligenza Artificiale. Rispetto a questo sono già stati potenziati diversi codici di Leonardo usati per la progettazione degli elicotteri, dei velivoli e dei radar per sfruttare il calcolo parallelo e le GPU, con l'obiettivo di abbattere i tempi di simulazione di un fattore 10 (da giorni a ore) ed aumentare l'accuratezza

37 Questo progetto contribuirà in maniera significativa al posizionamento dell'Italia fra le prime cinque nazioni al mondo per capacità di calcolo nei settori della ricerca pubblica e industriale.

stessa delle simulazioni. Infatti grazie all'enorme memoria presente nei nodi di calcolo è possibile scomporre il modello digitale di un elicottero o di un aereo in un numero maggiore di elementi con dimensioni molto più piccole, in modo da poter ottenere un risultato numerico con un dettaglio molto maggiore di quanto era possibile fare in precedenza. Inoltre, rispetto al mondo dei *big data*, in questo momento DaVinci-1 sta supportando lo sviluppo di soluzioni Leonardo per la costituzione di cosiddetti "data lake" dove aggregare i dati aziendali e dei prodotti, provenienti da più sorgenti. I *data lake* sono poi funzionali a supportare tre tipologie di servizi di elaborazione: *data analytics* per l'analisi dei dati, *digital twin* nella componente *data driven*, e sviluppo di modelli di intelligenza artificiale. Ad oggi è già stata completata la prima fase di sviluppo del *datalake* per la divisione elicotteri, ed è in fase di implementazione un *datalake* per la divisione velivoli. Per quanto riguarda lo sviluppo dell'AI, DaVinci-1 sta supportando l'addestramento di reti per la "predictive maintenance", per il riconoscimento delle immagini sia video che satellitari, il riconoscimento del linguaggio naturale e per le previsioni meteo a breve termine a partire dai dati radar meteo.

5.2 Le architetture "combat cloud"

Il "cloud computing" è un'architettura informatica che permette di addensare e processare tutti i dati raccolti da fonti multiple su un unico supporto per poi ridistribuirli secondo necessità attraverso una serie di servizi, il tutto grazie ad una connessione che collega infrastrutture, piattaforme informatiche e *software*. I servizi (informatici) stessi possono essere utilizzati e distribuiti tramite una piattaforma legata all'utente finale con una connessione Internet. Per fare un esempio civile noto a tutti, i servizi video *on demand* (YouTube, Netflix, ecc.) sono largamente basati sul *cloud*. Solitamente l'utente non possiede il *file* video e nemmeno l'applicazione che permette di leggerlo, ma accede direttamente al servizio e al contenuto tramite apposita autorizzazione³⁸. Il *cloud* permette quindi di esternalizzare le funzioni di stoccaggio e processamento ma anche, *mutatis mutandis*, di attingere a dati e servizi ben oltre le capacità interne di un terminale. I servizi di stoccaggio dati come One Drive o Google Drive possono essere a tal proposito considerati dei rudimentali esempi di *cloud computing*.

38 Se pensiamo ad una campagna aerea, questo è evidente già da ora. I dati da processare riguardano tracce radar, immagini provenienti da sensori EO, immagini satellitari e molto altro. Tutti dati molto pesanti rispetto alla normale attività internet di un utente privato. Inoltre, per motivi di resilienza, sarà necessario avere della ridondanza ed evitare di concentrare tutto su un'unica infrastruttura. Allora, se è vero che i Paesi più avanzati pensano oggi in termini di "combat cloud" a livello interforze nazionale, l'architettura di questi cloud sarà molto più articolata e complessa di un grande data-center e sarà basata sia sulla ridondanza sia su cerchi di autorizzazione all'accesso diversificati per utente e temi. Per esempio, ciascuna Forza Armata avrà il proprio sistema che sarà interconnesso con gli altri e da cui tutti potranno attingere una parte delle informazioni reputata di comune utilità.

Si tratta dunque di una capacità di archiviazione decentrata e delocalizzata rispetto al punto di raccolta. Per quanto riguarda le implicazioni militari del *cloud*, la possibilità di non avere una struttura di archiviazione a bordo (o comunque di ridurne l'importanza) e stoccare i dati provenienti da sensori multipli senza doverli scaricare dal singolo velivolo ne rappresenta il principale vantaggio³⁹. Naturalmente, occorre poi che questi dati vengano processati, catalogati ed eventualmente analizzati senza essere travolti dalla massa informe di informazioni che si viene a creare⁴⁰. Ecco perché *cloud* e AI sono intrinsecamente collegati. L'estrazione del valore contenuto in grandi moli di dati è come abbiamo visto il primo compito assegnato alle applicazioni di intelligenza artificiale.

In linea di principio, è chiaro che sarebbe possibile accentrare completamente le capacità in un'unica infrastruttura di aggregazione, alla quale tutti gli oggetti in volo potrebbero attingere, anche alimentandola allo stesso tempo, ma non è così semplice, sia perché si tratta di capacità che poi vanno difese, sia perché dati e capacità tendono a crescere di diversi ordini di grandezza nel tempo. Il *cloud*, dunque, seguirà con molta probabilità un'evoluzione naturale verso un'architettura su più livelli. Immaginiamo, per esempio, un'architettura su due livelli: un livello di prossimità in cui i dati crudi vengono raccolti e preselezionati (livello "edge") in modo da non congestionare le infrastrutture di aggregazione (livello di "consolidamento centrale"), dove risiedono le maggiori capacità di stoccaggio ed analisi dei dati. Il primo livello è costituito da sensori, effettori e piattaforme: qui avviene soprattutto la raccolta, ma anche un certo livello di analisi; quanto meno quello necessario per lo svolgimento di una missione tattica. Questo livello è come accennato "popolato" da sensori – radar, guerra elettronica, infrarosso e così via – sistemi d'arma – un missile piuttosto che un cannone da 127 mm navale, ecc. - ma anche da piattaforme: un MBT, un caccia tattico, per finire giù fino al singolo soldato o al distaccamento delle forze speciali. Il livello centrale è invece quello che custodisce i grandi *data center*, la cui ubicazione è irrilevante ai fini delle operazioni, con le più robuste capacità di stoccaggio e analisi e di fornitura dell'intera panoplia di servizi legata al *cloud*. In questo caso possiamo immaginare (pochi) grandi *server* e super-PC concentrati in strutture remote altamente protette, sicure e resilienti (in senso fisico, cibernetico ed elettromagnetico) dove affluiscono le informazioni gradualmente acquisite e continuamente acquisibili nel tempo, a cui accedere mediante collegamento *datalink* tradi-

39 Oggi il modello prevalente è quello di mega-datacenter. Le reti di Microsoft, Google o Amazon in Europa sostengono i dati e le interazioni di tutti grazie a pochi giganteschi datacenter con capacità continentale. Questo modello in futuro potrebbe essere tuttavia messo in crisi dal fatto che i dati saranno troppi per essere portati integralmente al centro prima di essere processati. Serviranno quindi uno o più livelli intermedi di lavoro per smaltire la massa di dati.

40 Altro problema fondamentale è la natura stessa dei dati, ovvero la necessità di sfruttare rilevazioni di tipo diverso e tradurle in informazione utile.

zionale o satellitare e un'opportuna serie di credenziali gerarchicamente organizzate. Il compito principale di questo *layer* centrale è alimentare il sistema di combattimento nel suo insieme, evitando però di ingolfarlo con informazioni inutili, o poco utili, o di “fuorviarlo” distribuendo info all'utente sbagliato o all'utente che in quel momento non necessita di quel tipo di informazione o, ancora, distribuendo info all'utente giusto ma nel tempo sbagliato. Da qui, appunto, il binomio inestricabile tra *cloud*, super calcolo e intelligenza artificiale.

Detto questo, a nostro avviso la *performance* di tutto il “sistema cloud” sarebbe enormemente migliorata con l'aggiunta di un *layer* intermedio caratterizzato da una robusta capacità di analisi ed elaborazione, ma da una capacità di stoccaggio minore rispetto a quella del *layer* centrale. Questo livello dovrebbe essere “popolato” da nodi mobili quali, per esempio, una portaerei o una grande nave anfibia o, ancora, un mercantile “convertito” – se ragioniamo in termini marittimi – oppure da un caccia di sesta generazione o da un *tanker* – se ragioniamo in termini aerei. Prendiamo per esempio, un *tanker* o un grande velivolo da trasporto: stiamo parlando di piattaforme molto grandi che potrebbero ospitare a bordo “armadi” per l'elaborazione e l'analisi dei dati, con le quali andare a “de-moltiplicare” il livello centrale e rendere tutto il sistema più flessibile e adattivo. Non si tratta, giusto per precisazione, di riconvertire questi velivoli ma solo di installarvi capacità organiche di analisi/elaborazione automatiche sfruttandone gli spazi. Il *focus* in questo caso, infatti, non è sull'immagazzinamento ma sull'elaborazione e l'analisi; ed in questo un aiuto enorme potrà venire dalla capacità dei futuri supercalcolatori di essere sempre più potenti, e sempre più compatti e piccoli. Per cui ciò che oggi può essere ospitato in edifici a terra, tra 10 anni sarà ospitabile – magari, appunto, solo per ciò che concerne capacità di elaborazione e analisi – su caccia tattici o sui grandi *enabler* come un *tanker* piuttosto che un velivolo per l'*early warning*. Un caccia tattico, per esempio, potrà svolgere contemporaneamente il ruolo di “terminale” e, dunque, di *effector*, ma anche il ruolo “intermedio” di nodo intelligente capace di analizzare grandi quantitativi di dati, processarli e produrre di conseguenza un'informazione azionabile per l'utente giusto al momento giusto⁴¹. Lo stesso discorso vale anche per i grandi ricognitori strategici non pilotati come i Global Hawk. Questi velivoli sono dedicati alla ricognizione ad alta quota e lungo raggio sfruttando la loro eccellente sensoristica e la loro grande autono-

41 Quando parliamo di sistemi di combattimento aereo del futuro, parliamo di grandi programmi multinazionali, che prevedono tra le altre cose anche dei database comuni con possibilità di accesso da parte di tutti i Paesi partner. Si dovrà però trovare un buon compromesso tra accessibilità delle informazioni a tutti i partner e sicurezza nazionale delle informazioni di esclusivo interesse di un Paese ma non degli altri. Insomma, ancora una volta, i grandi cloud non saranno dei giganteschi hard disk lineari, ma piuttosto un insieme di insiemi, sottoinsiemi e intersezioni con livelli di condivisione e sicurezza stratificati secondo utente, impiego e scala di utilizzazione (Forza Armata, nazionale, internazionale). I sistemi di alleanze come la NATO potrebbero rappresentare un ulteriore insieme cui ciascun cloud nazionale apporta il suo contributo per avere un nocciolo duro di informazioni condivise in funzione delle campagne militari da affrontare insieme.

mia/persistenza, ma già oggi nell'ambito della prevista modernizzazione verranno equipaggiati con moduli di AI capaci di svolgere già *on board* un grande lavoro di scrematura ed analisi, e successiva distribuzione via *datalink* agli utenti più opportuni. Una rivoluzione vera e propria, potenzialmente in grado di velocizzare enormemente il ciclo OODA.

In ogni caso, l'architettura "combat cloud" nel suo insieme dovrà assicurare un altissimo livello di automazione nell'analisi/elaborazione e nello scambio dei dati, una capacità di analisi predittiva e di calcolo scenaristico, una capacità di gestione della connettività ad ampio spettro, un ciclo di pianificazione sempre più veloce ed una maggiore consapevolezza post-missione⁴².

5.3 Sensoristica di nuova generazione

Finora abbiamo parlato dei dati e del loro processamento. Vediamo, invece, come quanto detto si applica ai sensori, che hanno il compito di condurre tutte le rilevazioni sul campo di battaglia per dar vita ai flussi di informazioni di cui sopra, ed agli apparati che saranno a bordo dei nuovi sistemi aerei da combattimento.

A seconda dei casi, un sensore potrà operare in modo "stupido" come *slave* di un velivolo (pilotato o autonomo) e convogliare a questo i dati, oppure potrà operare in maniera "smart" bypassando il livello velivolo per inviare i dati direttamente al *relay* di processamento in volo. In tal senso, sensori di nuova generazione potranno essere dotati di un applicativo AI che li renderanno sempre più intelligenti e autonomi, e in grado di scremare da soli l'informazione da inviare. Si crea, ancora una volta, un livello di autonomia diversa secondo generazione, ruolo e spendibilità, ma si dovrà tener presente anche la larghezza di banda necessaria allo scambio di informazioni su larga scala, mentre la scelta di processare le rilevazioni a livello locale o centrale dipenderà anche da considerazioni di interoperabilità e bande disponibili.

42 Strettamente legato a supercalcolo, AI e cloud c'è anche il concetto di digital twin, modello digitale. Il termine Digital twin sta ad indicare un programma al computer, alimentato con dati raccolti da un sistema reale, ed in grado di rappresentare in modo sintetico ma fedele (spesso attraverso visualizzazioni con modelli 3D, grafici, curve e cruscotti) lo stato complessivo del gemello reale. Semplificando potremmo dire che il gemello digitale è l'equivalente di una centrale di controllo del gemello reale, implementata all'interno di un software e che può funzionare anche senza il sistema controllato. Di recente il concetto di Digital Twin, invece, sta assumendo nuovi significati in senso di modello digitale olistico di un sistema reale, ovvero di una sua rappresentazione virtuale (sempre all'interno di un programma per calcolatore) che ne replica lo stato ed i cambiamenti di stato, grazie all'utilizzo combinato di dati, simulazioni ed intelligenza artificiale. Tutto questo grazie alla potenza di calcolo e di analisi dati oggi disponibile, nei supercalcolatori o in cloud. La potenza è tale da poter calcolare modelli numerici molto complessi ma accurati, in grado di rispondere sempre meglio alla necessità di prevedere il comportamento di un sistema sotto diverse condizioni di funzionamento, sia esso un'auto, un aereo, una nave, un impianto industriale fino ad arrivare al corpo umano ed alla terra intera (in questi due ultimi casi stiamo parlando ancora di progetti di ricerca). La necessità dell'impiego del gemello virtuale è ulteriormente amplificata in ambito industriale dal progressivo aumento dell'automatizzazione dei processi, dove tutto è gestito da sistemi di telerilevamento, e le azioni operative, di cambiamento della configurazione, di manutenzione devono avvenire senza l'intervento umano. La disponibilità di un gemello virtuale accurato e predittivo è fondamentale anche per prevedere l'effetto di un cambiamento di stato, voluto o non voluto (ad esempio a causa di condizioni ambientali alterate), evitare malfunzionamenti, ridurre i costi di produzione e operatività, in virtù di azioni preventive, fare valutazioni what if, addestrare gli operatori, ecc.

Dal punto di vista fisico, i sensori seguono i *trend* evolutivi delle altre tecnologie: riduzione dei pesi, minor consumo di energia e aumento della prestazione (in termini di sensibilità, guadagno, risoluzione, ecc.). A queste tendenze consolidate si aggiungono i requisiti di bassa osservabilità che rivoluzionano il modo di concepire un sensore. Per esempio, oggi aerei come il Typhoon, il Rafale o il Gripen portano delle “palle”IRST sul muso, mentre per la futura generazione si avranno sensori conformi multifunzione che aderiranno alla sagoma del velivolo. Probabilmente si tratterà di agglomerati di sensori più piccoli che agiranno in modo cooperativo e federativo. Analoga tendenza si registra nel settore dei radar. Per esempio, la DGA francese alimenta da anni uno studio specifico sui radar “conformal” che dovrebbe sfociare in una versione “aumentata” dell’attuale radar di tiro RBE2 del Rafale cui si aggiungerebbero almeno due antenne ulteriori laterali lungo la fusoliera del velivolo. Un esempio ancora più concreto è la proposta di Icarus Aerospace di montare il radar Leonardo Osprey-30/50 a bordo del caccia tattico TAV. Per esempio, 3 o 4 antenne di piccola dimensione opportunamente collocate consentirebbero all’aereo di avere una visuale radar su 360°. Discorso analogo potrebbe essere fatto per i sensori da guerra elettronica. Le ultime versioni dei Dassault Falcon MRA (Maritime Reconnaissance Aircraft) e dei Gulfstream G-550 “speciali” proposte dall’Israeliana IAI dispongono di sensori ELINT conformali al posto delle antenne “a spuntoni” che sporgono dalla fusoliera. Probabilmente, una miniaturizzazione ulteriore di queste tecnologie ne permetterà l’installazione a bordo dei caccia di prossima generazione. Inoltre, non si esclude che ai miglioramenti lineari dei sensori oggi esistenti si aggiungano nuovi sensori in grado di valutare parametri diversi da quelli classici: ottico, infrarosso, radar e radio. Ma al di là della prestazione cruda, il grado di autonomia di ciascun sensore e la presenza o meno di un applicativo AI interno al sensore stesso è un argomento oggi dirimente. Ancora una volta, ad un sensore più autonomo corrisponde anche la capacità di comunicare e condividere la propria informazione con l’intero *network*, possibilmente con sistemi di comunicazione ridondanti comprendenti, ad esempio, *datalink* satellitare, connessione 5G o altro metodo di nuova concezione. Si ritorna quindi alla stretta dipendenza tra capacità di ridurre il consumo energetico e possibilità di montare un sensore a bordo di una piattaforma come un velivolo autonomo, la cui potenza a bordo è giocoforza limitata. Maggiore è il consumo del sensore, minore è la possibilità di rendere questo sensore “intelligente” perché ciò avverrebbe a discapito della potenza disponibile. In altre parole, un sensore dotato di capacità di scremare autonomamente l’informazione utile da quella superflua agevolerebbe il lavoro di calcolo fatto a livello centrale – per esempio dal calcolatore del caccia o dal nodo di calcolo volante a bordo di un *tanker* adattato. Ma questa capacità costringe a compromessi a bordo del vettore che porta il sensore sul campo di

battaglia. Per esempio, se si tratta di un caccia, questo potrebbe dover scegliere quali sensori utilizzare senza poterne attivare troppi, mentre se si parlasse di un adjunct/gregario o di altro UAV si potrebbe dover operare la scelta draconiana di montare un solo sensore o di operarne uno per volta (senza dimenticare poi il problema della compatibilità elettromagnetica tra sensori multipli da installare su superfici limitate). Al contrario, mantenere limitata l'intelligenza del sensore porta poi ad una massa di dati di cui il nodo di calcolo "intermedio" deve farsi carico. Per non parlare del fatto che i dati raccolti da ogni sensore dovranno essere disponibili per numerosi utilizzatori. In linea di massima, quindi, possiamo dire che le capacità espresse dai sensori che andranno a bordo dei sistemi aerei da combattimento del futuro saranno funzione delle tre tecnologie abilitanti di cui abbiamo parlato nei paragrafi precedenti e di quanto queste saranno in grado di rispettare la *roadmap* tecnologica prevista con orizzonte 2035-2040.

Ciò detto, il *trend* che si sta intravedendo con più chiarezza nel campo delle sensoristica di nuova generazione è quello dei sistemi multifunzionali per i caccia di sesta generazione. Con la generazione precedente di caccia, infatti, siamo abituati a pensare a sensori separati – radar, guerra elettronica, elettro-ottico – ciascuno impiegante la propria antenna ed il proprio processamento e, in ultima analisi, in grado di fornire al pilota dati diversi o, meglio, separati. Con la quinta generazione, in particolare con l'F-35, si è passati al concetto di integrazione e fusione con sensori che lavorano all'unisono mediante il *cueing* e con un motore di fusione che attraverso capacità di calcolo e correlazione estremamente sviluppate offre al pilota un dato univoco e coerente. Insomma, se con la generazione cosiddetta "legacy", il pilota oltre che sulla missione doveva concentrarsi anche sull'analisi di dati diversi "grezzi", con la quinta generazione il pilota ha di fronte un dato univoco a tutto vantaggio dell'alleggerimento del *workload* e del *focus* sulla gestione tattica della missione. Con la generazione successiva, ovvero la sesta, questo concetto viene esploso ed enfatizzato ulteriormente, partendo proprio dai sensori. Si parla infatti di sistemi multifunzione, ovvero di sistemi che sfruttando le medesime antenne e/o aperture possono svolgere più funzioni – radar, EW e comms⁴³. Prendiamo, per esempio, il Multi Function Radio Frequency System che Leonardo sta sviluppando per il caccia di sesta generazione del sistema Tempest. Basandoci sui pochi dati divulgati sin qui dall'azienda, si tratta di un sistema capace di svolgere funzioni radar a lungo raggio, di Guerra Elettronica, in particolare attacco elettronico, e comms è caratterizzato da antenne conformali basate su materiali ancora più performanti

43 Con le giuste forme d'onda, la stessa antenna può essere impiegata come radar, come sistema di comunicazione, come ricevitore di segnali diversi e come trasmettitore per jamming e guerra elettronica.

del GaN (nitruro di gallio). L'MFRFS sarà a sua volta parte di un più ampio sistema, denominato ISANKE (Integrated Sensing And Non-Kinetic Effect), che garantirà integrazione, gestione, fusione ed elaborazione dei dati provenienti da tutti i sensori a bordo dell'aereo, sia quelli a base RF sia quelli elettro-ottici. ISANKE sarà presumibilmente dotato di un potente modulo di AI e super calcolo per garantire lo svolgimento delle succitate attività in maniera estremamente rapida e su grande scala. Al momento, tutta questa attività è soggetta ad un alto grado di classifica.

In tale ottica, Leonardo ha assegnato alla società britannica di servizi per l'aviazione 2Excel un contratto per l'approntamento di un banco-prova volante per lo sviluppo delle nuove tecnologie destinate al sistema di combattimento aereo del futuro TEMPEST. Il contratto prevede il ricondizionamento e la trasformazione di un Boeing 757 in un vero e proprio laboratorio volante per sperimentare e testare i complessi sensori integrati, le componenti elettroniche e radar, e le comunicazioni che Leonardo sta sviluppando per il TEMPEST. Tra questi, anche il citato Multifunction Radio Frequency System (MRFS).

Più in dettaglio il contratto segue uno studio, lanciato nel 2019, ma annunciato dal solo MoD britannico, per valutare la fattibilità di trasformare un aereo di linea commerciale in testbed e effettuare la modellazione digitale di alcune delle modifiche proposte, comprese quelle più significative alla parte anteriore, sulla base delle dimensioni, del peso e dei requisiti di potenza delle tecnologie da testare e sviluppare e della necessità di consolidare i requisiti in termini di alimentazione, raffreddamento, *racking* e di collocazione delle stazioni di osservazione, elaborazione e registrazione dati. Le possibili modifiche esterne che verranno apportate, inclusa quella citata riguardante la parte anteriore del velivolo, sono state delineate durante questa prima fase per consentire l'analisi di impatto aerodinamico e strutturale sull'aeromobile, rispettando i requisiti posti da Leonardo per l'installazione degli equipaggiamenti. A giudicare dalle immagini ufficiali rilasciate sotto forma di disegno da Leonardo, il velivolo presenta un muso completamente modificato con un'estremità a pungiglione e delle carenature laterali sulla sezione anteriore della fusoliera in corrispondenza della linea dei finestrini. Il primo volo di qualifica di Excalibur è atteso nel 2023.

Insomma, sui sistemi di combattimento aereo del futuro avremo dei sensori qualificati dalle seguenti caratteristiche: 1) multifunzionalità 2) antenne conformali 3) intelligenza, intesa come capacità di svolgere un primo livello di analisi ed elaborazione del dato.

Sempre in ambito sensoristica di nuova generazione un'altra delle tecnologie più promettenti sembrerebbe quella legata al *quantum computing* ed alle sue applicazioni, per esempio, nel campo della radaristica. Facciamo una premessa. Generalmente ad un sensore si

richiedono due cose. La prima è che risponda in maniera proporzionale all'intensità di ciò che si vuole sentire, ovvero al segnale che voglio misurare. La seconda è che il sensore deve essere estremamente sensibile, ossia capace allo stesso tempo di captare tanto uno stimolo piccolissimo, quanto uno molto più grande. Banalmente, se pensiamo ad una bilancia, questa dovrebbe essere in grado di misurare la frazione di grammo, ma pure i pesi superiori ai 100 kg. Con i sensori convenzionali è difficile ottenere questo risultato, ma con la tecnologia quantistica ciò è possibile. Detto diversamente: la tecnologia quantistica è potenzialmente in grado di garantire una sensibilità semplicemente inarrivabile con le tecnologie attuali e con conseguenze enormi nel campo della radaristica: dalla possibilità di scoprire oggetti piccolissimi a grandissime distanze, alla possibilità di "vedere dietro l'angolo" e così via⁴⁴.

Se la materia dovesse svilupparsi come numerosi centri di ricerca sperano, molte tecnologie oggi ritenute d'avanguardia potrebbero conoscere una prematura obsolescenza. Si tratta di tempi di gestazione lunghi, ma le prospettive di lungo periodo sono avvincenti. Il programma Quantaquest, finanziato dall'UE con 1,4 milioni di euro nell'ambito della finestra sulla ricerca (PADR, Preparatory Action Defense Research) dell'EDF (European Defence Fund), scommette sulla promessa che i radar quantistici renderanno obsoleti i velivoli *stealth*, che superconduttori e magnetometri quantistici rileveranno i sottomarini e che la crittoanalisi computerizzata quantistica romperà i codici creati in modo convenzionale. In aggiunta, Quantaquest si propone di sviluppare il rilevamento quantistico per la navigazione e il cronometraggio in modo che i vettori possano rendersi indipendenti dai sistemi globali di navigazione satellitare e dai sistemi di comunicazione. Tutto questo in vista di una possibile integrazione dei primi elementi tecnologici di questo genere nei programmi futuri delle Forze Armate europee. L'azienda capocommessa del programma è la francese Thales, seguita dalla connazionale Thales Alenia Space France. Per l'Italia, l'azienda più in vista è Leonardo, e la controllata Telespazio. Visto l'argomento, sono stati coinvolti diversi centri di ricerca tra cui il Centre National de la Recherche Scientifique (CNRS) francese, il Laboratorio Europeo di Spettroscopie non Lineari (italiano) e l'Università degli Studi di Padova. Un altro settore potenzialmente interessato dal *quantum computing* potrebbe essere il cyber. Pensiamo, infatti, alla possibilità di criptare su basi quantistiche, anziché sulle convenzionali basi numeriche, e rendere così praticamente impossibile decrittare.

44 La quantistica si basa sullo sfruttamento del fenomeno di "entanglement" (intreccio) dei fotoni. In teoria, la strettissima correlazione fra il rumore di 2 impulsi può essere sfruttata per ottenere vantaggi nell'individuazione di un bersaglio. Un impulso viene trasmesso verso il bersaglio, uno viene trattenuto così da misurare la correlazione al momento del ritorno del segnale trasmesso. Il regime quantistico protegge inoltre dalle interferenze. Tuttavia, le difficoltà da superare sono enormi: il primo dimostratore costruito ha una portata di mezzo metro e non è in grado di misurare distanza, velocità e posizione angolare precisa. Inoltre, perché il sistema funzioni, la generazione degli impulsi correlati deve avvenire a temperature prossime allo zero assoluto.

CONCLUSIONI

Gli scenari militari che ci attendono nei prossimi anni si annunciano sempre più complessi e sofisticati. Gli ultimi conflitti – dal Nagorno Karabah, all’Ucraina – lo hanno dimostrato chiaramente. Prendiamo l’Ucraina. Si tratta di una guerra certamente molto tradizionale, ma molto complessa allo stesso tempo. Innanzitutto, in essa si intersecano più dimensioni: da quella informativa/comunicativa – la guerra delle immagini condotta, dalla parte ucraina, direttamente dal Presidente Zelensky – a quella elettromagnetica e cyber, passando per quella cinetica. In campo elettromagnetico, giusto per fare un esempio, l’apporto NATO è stato fondamentale soprattutto nei primi due mesi, quelli per intenderci combattuti principalmente nel nord e nel nordovest dell’Ucraina. In questa fase i Russi hanno avuto difficoltà evidenti a far valere la loro EW. Prendiamo pure il massiccio impiego da ambo le parti di artiglieria a lungo raggio di precisione – *artillery sniping* – combinata con l’uso dei droni per compiti di osservazione, BDA (Bomb Damage Assessment) e correzione del tiro. In questo modo, Ucraini e Russi colpiscono depositi, posti di comando, ma pure pontoni per l’attraversamento di fiumi e pure colonne meccanizzate. Da questo punto di vista l’artiglieria è un po’ la vera regina della Guerra in Ucraina.

Si è accennato poi ai droni; questi ultimi sono ormai un *must* per una varietà di missioni e compiti - dall’ISR, all’ISR armata, passando per i compiti di *relay* aeroportato e così via – e costituiscono un vero e proprio moltiplicatore. In futuro il loro apporto sui campi di battaglia è destinato a crescere ancora perché l’esigenza di presentare all’avversario sempre nuovi dilemmi in un ciclo continuo e ininterrotto aumenterà a sua volta e sarà sempre più pressante.

Ecco perché, come abbiamo cercato di analizzare in questo lavoro, a fronte di una maggiore complessità e sofisticazione degli scenari è necessario ripensare al comando e controllo ed alle operazioni aeree secondo una nuova logica, più dinamica, e correlata alla necessità di far convergere “effetti” sviluppati attraverso tutti i Domini, per generare “dilemmi” che soverchino la capacità dell’avversario di reagire in maniera coordinata ed organica. Una volta aperta una “finestra d’opportunità” sarà fondamentale avere la capacità di sfruttarla, agendo con la massima rapidità.

Per questo è necessario mettere a fattor comune ogni informazione, ogni sistema ed ogni capacità secondo la logica JADO, che ha come cardine un C2 di nuovo tipo, basato su un’architettura più flessibile e su una distribuzione dell’iniziativa e della decisione verso il basso. In questo contesto come abbiamo visto possiamo pensare ad un comando e controllo delle operazioni aeree diffuso, basato sul principio dell’autonomia dei terminali

periferici e tenuto assieme da nodi intermedi capaci di svolgere un controllo tattico fluido, a tutto beneficio della Joint Force. È il nodo intermedio che dovrà assicurare la rapidità e la sincronizzazione di tutto il ciclo esecuzione-produzione dell'effetto, operando come connettore informativo, mediatore e re/distributore di *intelligence* finita e di qualità per l'utente più opportuno nel momento più opportuno. Un vera e propria rivoluzione, dottrinale, ma anche tecnologica poiché sarà solo grazie alla tecnologia - intelligenza artificiale, super calcolo e così via – che tale rivoluzione potrà attuarsi a beneficio e a garanzia del mantenimento della superiorità militare occidentale sul resto del mondo.

BIBLIOGRAFIA

Libri, Monografie e documentazione

- A New Battle Command Architecture For Multi-Domain Operations, MITRE, 2019.
- Audizione del Ministro della Difesa sulle linee programmatiche del suo Dicastero presso le Commissioni Difesa congiunte della Camera dei Deputati e del Senato della Repubblica, marzo 2021.
- China Naval Modernization: Implications for U.S. Navy Capabilities, Congressional Research Service, agosto 2019.
- China's A2AD and Its Geographic Perspective, Institute of National Defense and Strategy Studies, dicembre 2014.
- Commandant's Planning Guidance, USMC, 2019.
- Concetto SCENARI FUTURI: tendenze ed implicazioni per la Sicurezza e la Difesa, Stato Maggiore della Difesa, 2021.
- Countering Anti-Access/Area Denial Challenges. Strategies and Capabilities, Nanyang Technological University, dicembre 2017.
- Defense Capabilities: Joint All Domain Command and Control, Congressional Research Service, 2020.
- F-35 Joint Strike Fighter (JSF) Program, Congressional Research Service, marzo 2020.
- F-35 Joint Strike Fighter, GAO (General Accountability Office), marzo 2021.
- F-35, la rivoluzione nei cieli, Pietro Batacchi, Speciale allegato a Rivista Italiana Difesa, 2015.
- Future Aircraft Carrier Options, Bradley Martin, Michael McMahon, RAND Corporation, 2017.
- Future of the Aircraft Carrier, Department of Defense, ottobre 2002.
- Future Warfare Anthology, Robert Scales Jr., Strategic Studies Institute, 1996.
- I sistemi di combattimento aereo del futuro. Speciale allegato a Rivista Italiana Difesa, 2021.
- Il concetto strategico del Capo di Stato Maggiore della Difesa, Stato Maggiore della Difesa, gennaio 2020.
- Il Documento Programmatico Pluriennale 2021-2023, Ministero della Difesa, agosto 2021.
- Il programma Joint Strike Fighter – F35, Servizio Studi della Camera dei Deputati, marzo 2021.

- Il programma F-35 Joint Strike Fighter e l'Europa, IAI (Istituto Affari Internazionali), ottobre 2008.
- In Athena's Camp: Preparing for Conflict in the Information Age, John Arquilla e David Ronfeldt, RAND, 1997.
- Joint All-Domain Command and Control (JADC2), Congressional Research Service, gennaio 2022.
- La sicurezza nel Mediterraneo e l'Italia, Michele Nones e Alessandro Marrone (a cura di), Istituto Affari Internazionali, 2015.
- Multi-Domain Operations. Approccio concettuale. Stato Maggiore dell'Esercito. 2020.
- Multiple Dilemmas. Challenges and Options for All-Domain Command and Control, Rand Corporation, 2020.
- Past Revolutions, Future Transformations, Richard Hundley, Rand, 1999.
- Technology and War: from 2000 B.C. to the Present, Martin Van Creveld, The Free Press, 1991.
- The Future of Distributed Operations in the Marine Corps
- and its Vital Role in Forcible Entry from the Sea, Erik Clark, Master of Military Studies Research Paper, 2011.
- The Origins and Development of A Cooperative Strategy for 21st Century Seapower (2015), Peter Swartz, William Rosenau e Hannah Kates, Center for Naval Analysis, settembre 2017.
- USAF role in Joint All Domain Operations, Air Force Doctrine Note-20, 2020.
- What Role Can Land-Based, Multi-Domain Anti-Access/Area Denial Forces Play in Deterring or Defeating Aggression?, Vari Autori, RAND Corporation, 2017.

Articoli di giornale e riviste

- Access denial: il nuovo incubo americano, Luca Pozzi, "Panorama Difesa", agosto-settembre 2005.
- Anti-Access/Area Denial: The Evolution of Modern Warfare, Christopher McCarthy, "Naval War College Student Journal", autunno 2010.
- Future Fighter Force, John Tirpak, "Air Force Magazine", luglio 2021.
- Goldfein's Multi-Domain Vision, Amy Hudson, "Air Force Magazine", agosto 2019.
- Guerra in Ucraina: strategia, coercizione e intelligence, Pietro Batacchi e Tommaso Massa, "Rivista Italiana Difesa", giugno 2022.

- Guerra in Ucraina, lezioni per il futuro, Pietro Batacchi, “Rivista Italiana Difesa”, agosto 2022.
- Il programma FVL, Pietro Batacchi, “Rivista Italiana Difesa”, agosto 2022.
- Information Warfare and Joint All Domain Operations, Bradley Pirolo, “Air & Space Power Journal”, inverno 2020.
- Le bolle Anti Access/Area Denial russe, Andrea Mottola, “Rivista Italiana Difesa”, luglio 2017.
- Le operazioni aeronavali russe nel Mediterraneo e in Siria, Pietro Batacchi, “Rivista Italiana Difesa”, gennaio 2017.
- Loitering munitions, droni e nuovi concetti per la guerra del futuro, Pietro Batacchi, “Rivista Italiana Difesa”, luglio 2021.
- Moving From Situational Awareness to C2: The Second ABMS On-Ramp Experiment Offers a Peek into the Future of JADC2, Brian W. Everstine, "Air Force Magazine", ottobre 2020.
- Optimizing Joint All-Domain C2 in the Indo-Pacific, Stefan Morrell, “Air & Space Power Journal”, estate 2021.
- Sviluppi russi ed occidentali nel settore dei missili antinave, Vladimir Shcherbakov, “Rivista Italiana Difesa”, aprile 2010.
- Table Stakes of the Advanced Battle Management System, Rudy Novak, “Air & Space Power Journal”, autunno 2020.
- Turning the ABMS Strategy into a Reality, Elaine Bitonti, “Air Force Magazine”, febbraio 2022.
- Verso un Potere Aereo 4.0, Pasquale Preziosa, “Rivista Italiana Difesa”, marzo 2018.

Siti Internet

- www.camera.it
- www.defense-aerospace.com
- www.fincantieri.it
- www.aeronautica.difesa.it
- www.mod.uk
- www.bmvg.de
- www.isn.ethz.ch
- www.globalsecurity.org

- www.thedrive.com/the-war-zone
- www.airforce-technology.com
- www.defencetalk.com
- www.defenseindustrydaily.com
- www.defense-update.com
- www.defense.gov
- www.nato.int
- www.defensenews.com
- www.navalnews.com
- www.armscontrolwonk.com

Colloqui e interviste dell'Autore

- Colloquio con Andrea Nativi, Vice President Strategy and Market Analysis Leonardo
- Colloquio con Federico Montrucchio, SVP Engineering - Head of Design Organization Leonardo Divisione Velivoli
- Colloquio con Laurent Sissman, Unmanned System Manager Leonardo
- Colloquio con Lorenzo Mariani, Amministratore Delegato MBDA Italia
- Colloquio con Eugenio Po, Capo Servizio RID, Rivista Italiana Difesa
- Colloquio con Doug Wilhelm, Deputy Vice President e General Manager Lockheed Martin per il programma F-35
- Colloquio con Jon M. Davis, ex Deputy Commandant for Aviation dell'USMC
- Colloquio con Luigi Piantadosi, Director FVL International

Nota sull'IRAD e Nota sull'Autore

IRAD⁴⁵

L'Istituto di Ricerca e Analisi della Difesa (IRAD) è l'Organismo che gestisce, nell'ambito e per conto del Ministero della Difesa, la ricerca su temi di carattere strategico.

Costituito come Centro Militare di Studi Strategici (Ce.Mi.S.S.) nel 1987 e riconfigurato come IRAD nel 2021 a seguito dell'entrata in vigore della Legge 77/2020 - art. 238 bis, l'IRAD svolge la propria opera avvalendosi di esperti civili e militari, italiani ed esteri, in piena libertà di espressione di pensiero.

Quanto contenuto negli studi pubblicati riflette quindi esclusivamente l'opinione del Ricercatore e non quella del Ministero della Difesa.

Pietro Batacchi



Pietro Batacchi è attualmente Direttore di RID – Rivista Italiana Difesa – la principale rivista del settore Difesa in Italia, e una delle principali in Europa, di RID Analytics, Dipartimento di RID specializzato in studi e analisi, e di www.rid.it. Da anni collaboratore dell'IRAD (Istituto di Ricerche e Analisi della Difesa) e di numerose riviste specializzate e non italiane ed estere, commentatore di radio e TV nazionali e internazionali, consulente su questioni di politica di difesa e sicurezza, e docente presso istituzioni accademiche e militari, Pietro Batacchi in precedenza è stato Direttore del Ce.S.I. – Centro Studi Internazionali – e Caporedattore di Panorama Difesa.

ISBN 979-12-5515-038-1



9 791255 150381