Conferenza

"HYBRID CYBER WARFARE AND THE EVOLUTION OF AEROSPACE POWER: risks and opportunities"

Discorso del Gen. D. Francesco Cannillo

Casa dell'Aviatore

Viale dell'Università, 20 – 00185 Roma

9 Novembre 2017

Autorità, gentili ospiti, preliminarmente, mi faccio interprete dei sentimenti di sincera partecipazione e vicinanza del Sig. Capo di Stato Maggiore, Generale Vecciarelli, a questo prestigioso evento al quale, suo malgrado, non ha potuto presenziare per consolidati e concomitanti impegni istituzionali.

Mi unisco al pensiero del Sig. Capo di S.M.A. rilevando l'assoluta attualità del tema oggetto del convegno e l'ampiezza di spettro di trattamento grazie all'approccio interdisciplinare che vede la partecipazione del mondo accademico e del settore industriale che ringrazio per la gentile partecipazione ed il prezioso contributo.

Lo scenario geopolitico internazionale è caratterizzato da un livello crescente di complessità, dinamicità, incertezza ed imprevedibilità, in particolare nelle relazioni tra gli innumerevoli attori in campo, statuali e non (*non State actors*, cellule terroristiche, organizzazioni criminali), in cui anche l'equilibrio tra le parti interessate tende all'instabilità ed alla rapida evoluzione.

Tutto questo è stato vertiginosamente accelerato e potenziato dalla diffusione a livello globale di INTERNET e delle tecnologie ICT che hanno progressivamente connotato un driver fondamentale a quella che oggi può definirsi:

- la globalizzazione dell'incertezza, dal livello fisico al livello cognitivo, propria del cosiddetto "cyberspazio".

In questo senso l'importanza del nuovo dominio cyber nell'ambito militare è stata recentemente sancita nell'ultimo Summit NATO a Varsavia (8-9 luglio 2016) riconoscendo il "cyberspace" quale nuovo dominio delle operazioni militari.

Ciò ha determinato per la NATO, l'UE e per le nazioni alleate la necessità di avviare nei confronti delle hybrid / cyber threats due complessi processi:

- il conseguimento di un robusto livello di resilienza sin dal tempo di pace
- e lo sviluppo di specifiche capabilities per operare negli scenari ibridi e cyber.

Lo scontro militare in campo aperto è pertanto solo un aspetto (il più evidente) di un conflitto più complesso che viene combattuto su più piani (spesso invisibili all'osservatore esterno) ed in un teatro che travalica quello meramente fisico, dove il centro di gravità può essere individuato nell'ambiente dell'informazione in cui viene combattuta una delle battaglie decisive della guerra moderna:

- la battaglia delle narrative e della comunicazione strategica.

Ancorché il tema delle minacce ibride non sia nuovo, solo recentemente sta maturando la consapevolezza dell'importanza della dimensione digitale tanto da diversificare, nel lessico e nella sostanza, l'entità della minaccia.

Non a caso l'analisi della differenza tra Information Warfare e Cyber Warfare – da non confondere con Electronic Warfare – è stato l'oggetto dell'ultima Conferenza Nazionale sulla Cyber Warfare.

Sin qui abbiamo succintamente descritto lo scenario di riferimento, veniamo ora al tema centrale del Convegno: l'evoluzione richiesta al Potere Aerospaziale.

La digitalizzazione di alcuni asset ha portato ad un paradosso secondo cui più si è evoluti tecnologicamente più si è sotto attacco.

Il Potere Aerospaziale (PA), infatti, è sempre più interessato dall'utilizzo malevolo di tecnologie innovative teso a perpetrare atti illeciti ed attacchi terroristici, attraverso una vasta gamma di soluzioni tecnologiche che rappresentano un'area di interesse per la sicurezza e la Difesa di ogni nazione.

Tali nuove minacce ibride (cyber) richiedono quindi la strutturazione di una adeguata resilienza nazionale del potere aerospaziale sin dal tempo di pace in tre specifiche aree:

- la prima afferisce agli attuatori spaziali:
  è evidente come gli abilitanti spaziali permettano oggi un vasto range di servizi e di funzioni (comunicazione satellitare, navigation position/time and remote sensing, ISR e supporto al settore meteorologico) e supportano a tutto campo le moderne operazioni militari.
  Pertanto la totale o parziale degradazione di tali abilitanti derivante da un attacco ibrido e cyber può impattare la capacità di condurre operazioni connesse con l'Air Domain, sin dal tempo di pace.
- la seconda area interessa le infrastrutture critiche:
  un esempio tra tutti è il campo dell'Air Traffic Management. Il Programma SESAR prevede che attraverso il System Wide Information Management

(SWIM) si arrivi ad una condivisione globale dell'informazione ATM su scala europea, sulla base di standard tecnologici comuni e ispirati alla interoperabilità su soluzioni cloud e web based, che rappresentano un aspetto ad alta criticità in relazione alla minaccia cyber.

Ciò potrebbe impattare la sorveglianza dello spazio aereo nazionale e i discendenti processi di identificazione, attestati all'apparato della Difesa Aerea, che sono altamente dipendenti dalla fusione di dati del settore ATM.

- terza area, non certo meno importante, riguarda le Tecnologie commerciali a basso costo.

  un esempio è rappresentato dall'utilizzo di minacce provenienti dall'ambiente aereo attraverso le cosiddette Low, Slow and Small (LSS) aerial threats.

  In questo specifico ambito di minaccia ibrida, il gap tecnologico consiste nello sviluppare un complesso di funzioni che possano contribuire alla difesa da tali piattaforme per le quali la F.A. sta rapidamente attivando Programmi tesi a mitigare tale tipologia di minaccia e definire un nuovo paradigma che evolva la Difesa Aerea Nazionale tradizionale.

Va da se' che le operazioni espressione del Potere Aerospaziale devono necessariamente evolvere in funzione della minaccia cyber per acquisire capacità operative dedicate, acquisire capacità difensive per sincronizzare le proprie azioni offensive con le operazioni cyber.

Il riconoscimento del nuovo dominio delle operazioni cyber impone al potere aerospaziale sia di evolvere per sincronizzarsi con esso, sia di potenziare la sua resilienza e capacità operativa cibernetica.

Negli ambiti summenzionati l'impatto delle hybrid threats (tra cui il cyber) rappresenta un fattore di vulnerabilità di cui deve tener conto il processo evolutivo/di sviluppo del moderno potere aerospaziale (PA) inteso come espressione dello stato dell'arte della tecnologia.

Pertanto, si dovrà necessariamente ricercare adeguati livelli di security by design.

La multidimensionalità (land, maritime, air, space e cyberspace) dell'ambiente operativo, unitamente al carattere ibrido della minaccia, amplifichera' la complessità e la sicurezza dei futuri ambienti operativi, rispetto a quelli del passato.

Sul piano operativo militare, i diversi domini dovranno quindi essere fortemente integrati e interoperabili garantendo rilevanza ai livelli strategico, operativo e tattico.

In particolare per fronteggiare le hybrid threats, dovrà essere perseguita una vera e propria "sinergia tra i domini" attraverso l'impiego complementare / piuttosto che additivo / delle capacità in modo tale da accrescere l'efficacia complessiva dell'intero strumento ed assicurare la massima libertà d'azione per assolvere la missione.

Negli ultimi 30 anni il PA ha avuto un ruolo centrale nelle crisi che si sono succedute dalla fine della Guerra Fredda, adattandosi ad un ambiente in rapida evoluzione determinato dall'emergere di un nuovo tipo di minaccia terroristica.
Il PA, basato sui pilastri del Controllo dell'aria, Ingaggio, Mobilità Aerea ed Intelligence e Situational Awareness,
ha continuato a svilupparsi capitalizzando sulle nuove tecnologie attraverso complessi programmi di acquisizione (JSF, Sistemi APR, C2, Cyber, etc.), permettendone l'impiego a livello strategico, operativo e tattico.

In particolare, la sua intrinseca flessibilità ed agilità consente oggi – e ancor di più nel futuro - di generare anche effetti non-letali, offrendo uno strumento assai efficace e multiruolo per il decisore sia politico che militare.

Tenuto conto del mutamento dell'impiego della forza militare nei conflitti degli ultimi 30 anni, nei quali rapidità di intervento, precisione e minimizzazione dei danni collaterali all'azione cinetica sono diventati complementi irrinunciabili e di sempre maggior rilevanza strategica e capacitiva, il PA continuerà ad evolvere in modo sempre più determinante proprio per le sue caratteristiche e capacità di offrire uno strumento efficace, flessibile e fortemente adattivo anche in termini politico-diplomatici.

In conclusione, per il PA si tratterà di perseguire e mantenere costantemente nel tempo, la capacità di operare in ambienti di tipo "hybrid, complex, competitive and contested".

Tutto ciò presuppone lo sviluppo di capacità, selettive e proporzionali, nei vari settori e in tutte le sue componenti non materiali (organizzative, procedurali ed addestrative) e materiali (sistemi e piattaforme), in grado di adattarsi ai mutevoli scenari ibridi.

Tale orientamento strategico non può comunque prescindere ed essere disgiunto da una politica di investimenti nel settore del cyberspazio con lo spostamento di risorse dalla difesa militare cinetica classica in favore della difesa cyber.

Grazie e buon lavoro