Geopolитика.ru
Carthago delenda est
14.07.2023

LE OPERAZIONI SPECIALI NEL CONTESTO DELLE GUERRE IBRIDE: UNO SGUARDO FRA DOTTRINA E PRASSI DEL PRESENTE

di Lorenzo Maria Pacini

Nel contesto molto ampio delle cosiddette hybrid war, si rende opportuno definire con maggior precisione le coordinate delle Operazioni Speciali, sia per dottrina che per la prassi emersa nel presente a seguito, in particolare, dell'inizio della Operazione Militare Speciale fra Federazione Russa e Ucraina.

Vi è infatti molto spesso una generica approssimazione che tende ad accreditare come guerra ibrida qualsiasi tipologia di conflitto non-simmetrico o con impiego di strategie, strumenti e risorse non convenzionali, e ciò non è errato in sé; tuttavia, all'interno delle guerre ibride si riconoscono e definiscono varie tipologie, presso le quali l'etichetta di Operazione Speciale trova uno spazio singolare.

Un alfabeto per le Operazioni Speciali

Il primo passo è quello di definire, riconoscere e caratterizzare un'Operazione Speciale all'interno dell'ampio vocabolario strategico. In primo luogo, occorre individuare l'obiettivo, ovvero lo scopo che l'Operazione si propone e che è di grandissima importanza. Esso è strategico, in quando il ricorso ad operazioni di questo tipo consente di conseguire obiettivi di natura operativa o tattica in maniera eccezionale, fuori quindi dagli schemi ordinari. Le Operazioni Speciali vengono pertanto svolte solo se gli obiettivi sono di grande importanza e delicatezza e, talvolta, di grande peso e rischio politico. È quest'ultimo punto ad essere, a mio giudizio, fondamentale: nella programmazione strategica, l'elemento politico[1] è importante perché in un mondo globalizzato ogni azione ha una reazione potenzialmente amplissima e, dunque, bisogna sempre tenere presente sulla bilancia il peso degli effetti che genera; ancora, nel caso delle guerre ibride, il trinomio azione-reazione-proazione che si manifesta nella politica è la cartina tornasole per verificare lo status dell'operazione. Ciò viene adottato laddove non vi siano altre scelte "accettabili" per conseguire l'obiettivo, dunque allorché la diplomazia ufficiale e quella parallela hanno fallito e gli strumenti di deterrenza non sono risultati efficaci.

A seguito di ciò derivano alcune conseguenze e considerazioni. L'obiettivo di livello strategico-politico viene assegnato dai massimi vertici dell'organizzazione politico-militare, genericamente senza frapporre degli intermediari proprio a ragione della delicatezza della missione, la cui pianificazione ed esecuzione è di carattere, appunto, speciale, con la nomina di un commander in chief scelto nello Stato Maggiore della Difesa o lo stesso Ministro della Difesa, con l'istituzione di un comando operativo riservato[2] .

Altra caratteristica delle Operazioni Speciali è quella di essere seguite da unità specificatamente designata, selezionate, addestrare ed equipaggiate, con un'organizzazione procedurale e di impiego dedicate[3] . Le forze speciali sono unità che nascono diverse dalle altre proprio per la loro destinazione d'uso, alla quale si giunge dopo un'accurata preparazione itinerante e permanente. Quasi tutto il tempo della loro vita operativa, le forze speciali lo passano ad addestrarsi e ripetere quelle tecniche e procedure sino a quando, solo raramente, vengono chiamate all'impiego operativo[4] .

Un terzo aspetto osservabile è quello della singolarità nella pianificazione, dalla concezione fino al momento dell'hot wash up. Questa unicità richiede inevitabilmente una formazione altrettanto unica, per la quale vengono impiegati esperti nei settori richiesti. Ciò richiama ancora una volta alla necessità di forma di comando struttura in maniera differente rispetto all'ordinaria amministrazione delle Forze Armate, il che ci riporta alla mente la extra-ordinarietà di alcune operazioni che abbiamo visto svolgere in questi anni, passate alle cronache, come non da ultimo nel conflitto russo-ucraino.

Le Operazioni Speciali sono interforce per loro natura, si sviluppano in tutti i domini (terra, acqua, aria, spazio e infosfera) ed impiegano costantemente l'intelligence, in particolare una actionable intelligence per il supporto informatico concreto soprattutto in ambito politico, diplomatico e geoeconomico, con il prezioso contributo della codifica e decodifica dei pattern of life, delle tecnologie e delle strategie e tattiche politiche e commerciali che sono poste in gioco. Conformemente a questa impostazione, le Operazioni Speciali sono genericamente condotte con lo scopo di avvantaggiarsi sull'avversario, stabilendo una superiorità relativa da perfezionare nel corso degli eventi.

Tabella 1: Livelli di azione strategica.
Come evidenziato, l'arrivo all'impiego delle Operazioni Speciali è un tassello al di sotto della guerra convenzionalmente definita, mentre è al di sopra, o in parallelo, alle guerre ibride di recente sviluppo.

Variazioni di stile nella zona grigia

Le Operazioni Speciali si muovono sul filo del rasoio della zona grigia, in quello spazio indefinito e dai contorni sbiaditi che caratterizza il nostro tempo. L'impiego di questo genere di missioni sarà d'ausilio alle altre forme di guerra ibrida, laddove l'impiego di una forza armata sarà più necessario rispetto alla risoluzione "senza armi" precedentemente tentata.
In alcuni casi, ad esempio, le Operazioni Speciali possono essere clandestine o usare tecniche e procedure clandestine, così come anche la NATO usa definire «An operation planned or concluded in such a way to assure secrecy or concealment», ovvero un'operazione pianificata o conclusa in modo da garantire la segretezza o l'occultamento. L'aggettivo della clandestinità sta in questo caso a indicare il non riconoscimento della paternità di un'operazione o comunque di non svelare mai l'identità e la tipologia delle forze impiegate. In lingua inglese guerra si traduce con due termini: war, che indica più generalmente il concetto, lo stato, la condizione; warfare si riferisce invece oltre a ciò anche alla condotta della guerra e alle operazioni militari.

L'evoluzione di questo genere di operazioni è tipicamente grigia, proprio come la zona grigia, a cavallo fra ciò che è concesso dal diritto (nazionale, internazionale, militare) e ciò che non lo è, tra ciò che si può dire e quel che verrà negato costi quel che costi, sempre in virtù dell'obiettivo per il quale viene indetta la missione.

Similmente avviene per le cyberwar, guerre ibride cibernetiche dove la messa a sistema di tecnologie digitali e informatiche valica spesso i confini del tracciato giuridico e morale, essendo l'internet un mondo in cui le regole sono estremamente relative e variabili in poco tempo. Un cyberattacco è l'interruzione o la corruzione deliberata da parte di uno Stato di un sistema di interesse per un altro Stato, ed in cui l'obiettivo, in alcuni contesti, può anche diventare una rappresaglia, una sommossa popolare o una disattivazione delle comunicazioni informatiche online.

Sempre centrale è la percezione della deterrenza, la quale richiede che l'avversario sia in grado di distinguere il rischio dall'assenza di esso, l'essere punito dal non essere punito. Nella fattispecie delle cyberwar, la deterrenza è molto più complessa, perché lo spazio digitale non è come quello fisico e la percezione è distorta al punto che non potrebbe essere comprensibile il rischio di ritorsione, sia essa accidentale o pianificata. Ciò dimostra la forte asimmetria di questa tipologia di guerra ibrida.

Nelle infowar, per fare un altro esempio, l'impiego di forze armate

speciali è pressoché infinitesimale, facendosi bastare gli asset dell'intelligence e gli analisti, poiché lo scopo è quello di immettere un certo tipo di informazioni affinché esse provochino degli effetti su più livello cognitivi sociali e individuali, nonché politici. Information warfare è un termine entrato nel vocabolario del Dipartimento della Difesa americano dalla metà degli anni '90, per includere forme di guerra come l'attacco alla catena di comando e controllo, l'intelligence, la guerra elettronica, le operazioni psicologiche, la guerra informatica, la guerra delle informazioni economiche e appunto la Cyberwarfare o guerra cibernetica. Essa di fatto consiste nello sfruttamento delle informazioni a fini strategici e la guerra cibernetica è diventato in tempi più recenti un sinonimo di information warfare strategica data la pervasività del dominio cibernetico nelle operazioni militari e nell'infrastruttura digitale dell'economia di un Paese.

Il Rapporto Rand del 1996 (e seguenti[5]) individua sette caratteristiche tipiche dello strategic information warfare: base barriere delle tecnologie informatiche, confini tradizionali sempre più sfumati, accrescimento del potere di inganno delle tecnologie informatiche, importanza dell'intelligence strategica, difficoltà di distinguere l'atto criminale dall'attacco informatico, il problema della costruzione delle alleanze e la vulnerabilità nazionale. La Dottrina americana fino a pochi anni fa parlava di Computer Network Operations (CNO) che comprendeva le Computer Network Attack (CNA), le Computer Network Defense (CND) e le Computer Network Exploitation (CNE). Ora si parla di Cyberspace Operations (CO) come di quelle operazioni in cui l'impiego di capacità cyber ha lo scopo primario di raggiungere obiettivi nel cyberspazio o attraverso di esso[6] .
Le CO comprendono le Offensive Cyber Operations (OCO), ovvero quelle operazioni che hanno lo scopo di proiezione di potenza tramite l'applicazione della forza nel cybersdpazio. All'interno esistono anche le Defensive Cyberspace Operations (DCO) che consistono in operazioni passive ed attive condotte allo scopo di preservare la capacità di utilizzare le capacità del cyberspace e di proteggere i dati, le reti, le capacità che poggiano sulle reti e i sistemi di interesse amico. L'ultima categoria è quella delle Defensive Cyberspace Operation Response Action (DCO-RA), ovvero misure o azioni difensive svolte al di fuori dalle reti da difendere allo scopo di proteggere e difendere le capacità cyber del DoD o altri sistemi di interesse[7] .

Nell'impiego di questo tipo di guerre ibride, è difficile spesso attribuire la paternità dell'attacco e ciò rende altrettanto complessa la pianificazione della risposta, andando ad agire sulla soglia militare della liceità di una risposta cinetica ad un attacco cibernetico.

Il fatto che un'operazione cibernetica colpisca obiettivi militari legittimi, ma soprattutto che produca un effettivo "vantaggio militare" può essere un criterio per attribuire carattere militare ad una operazione cibernetica prescindere dal fatto che sia condotta da personale militare. Il concetto di soglia militare è stato risolto attraverso la decisione a discrezione del Consiglio Atlantico di attivare l'art.5 del Trattato di Washington sulla difesa collettiva, senza stabilire preventivamente la causa scatenante. La NATO ha riconosciuto il valore aggiunto di lasciare dei "toni di grigio" nell'area grigia del confine tra guerra cibernetica e crimine informatico, senza dichiarare quale è la soglia oltre la quale la NATO ritiene si debba intervenire, per impedire agli aggressori di spingersi fino alla soglia militare senza superarla e quindi colpire senza avere una risposta militare.
Le nuove tecnologie, in particolare l'Intelligenza Artificiale già in sviluppo ed uso militare da molti anni, permettono ovviamente un approccio molto più preciso e sistemico a questo tipo di guerre. L'impiego di questo strumento[8] si è rivelato centrale nelle infowar, specie per quanto riguardo le cosiddette fake news, sia prodotte che sventate, poiché le reti neurali permettono di generare e riconoscere delle "realtà" virtuali talmente simili alla realtà vera, da non permettere ad un primo approccio il riconoscimento effettivo dell'inganno.

Una conclusione concettuale, non necessariamente dottrinale

Da quanto considerato fin qui, è chiaro che le Operazione Speciali assumano gradualmente nuovi criteri di definibilità. L'attributo "speciale" non può giustamente essere dato come grado di encomio a qualsivoglia tipo di guerra non convenzionale, ma è altrettanto vero che sembra ormai una forzatura mantenerlo solo per operazioni con impiego di forze speciali. Si potrebbe altresì concordare, ed è forse questa la via più corretta epistemologicamente, che le Operazioni Speciali non possono fare a meno delle multiformi e multidominanti guerre ibride, che le precedono nell'ordine d'impiego e le accompagnano in tutte le fasi del loro svolgimento.

Tabella 2: Revisione dei livelli di azione strategica
È chiaro che, in quest'ottica e stanti ai recenti eventi bellici, le Operazioni Speciali vadano legandosi sempre di più con le guerre ibride, non venendone assorbite nella definizione ma nella operatività. Ciò può significare anche la disposizione di forze speciali di carattere ibrido, capaci di mescolare le caratteristiche delle due. Inoltre, ciò si sta rendendo evidente anche dal punto di vista del governo bellico, dove le componenti ordinarie delle gerarchie dello Stato Maggiore vanno sempre più mescolandosi con quelle dei reparti speciali, perlomeno nel caso di

alcuni Stati militarmente impegnati[9].

Volendo tracciare una conclusione concettuale, si ritiene necessario chiarire che le Operazioni Speciali non sono, dottrinalmente parlando, solamente o unicamente delle guerre convenzionali né delle guerre ibride; si tratta invece di operazioni multiformi occasionali caratterizzate da eccezionalità, agibili trasversalmente rispetto ai livelli strategici teorizzati.

Ciò non toglie la possibile evoluzione anche dottrinale, andando a considerare le Operazioni Speciali come una definizione più ampia e comprensiva, ridefinendo di conseguenza e con gradualità le definizioni delle tipologia, delle topografie e delle proiezioni strategiche.

Notas:
[1] Riporta l'Allied Joint Doctrine: «Special operations create strategic or operational level effects or are executed where significant political risk exists» (AJP 3,5), in https://www.gov.uk/government/publications/ajp-01-d-allied-joint-doctrine:
[2] Questa prassi è in un certo senso in contrasto con la presenza, istituita formalmente, dei comandi operativi interforce destinati alle Operazioni Speciali, come il COVI o il COFS in Italia, costituenti una sorta di gradino di mezzo fra i vari vertici di comando. Nel panorama internazionale, i Comandi delle Operazioni Speciali fanno riferimento direttamente al commander in chief pur confrontandosi con operazioni multidominio genericamente gestite dai Comandi di vertice interforce, intrecciando professionalità, qualità, competenza ed efficacia. In alcuni Paesi le Operazioni Speciali sono gestite da un service a parte, una vera e propria forza armata istituita, alle dirette dipendenze del Ministro della Difesa o di chi delegato.
[3] Sempre nel AJP si legge: «Special operations are military activities conducted by specially designated, organized, trained, and equipped forces using distinct techniques and modes of employment» (AJP 3,5).
[4] Capita che nelle Forze Armate i reparti speciali siano visti non di buon occhio, in quanto rappresentano una voce di spesa militare logicamente più alta rispetto agli impiegati convenzionali. Non potrebbe, però, non essere così, perché alle forze speciali è richiesto di fare qualcosa che agli altri non sarebbe possibile fare, con minimi margini di errore e con la responsabilità della riuscita, o del fallimento, di operazioni di alto calibro strategico.
[5] Cfr. M. C. Libicki, Cyberdeterrence and Cyberwarfare, RAND, Santa Monica (CA) 2009
[6] Secondo F. D. Kramer esistono 28 differenti definizioni del termine cyberspace. Cfr. Id., Cyberpower and National Security: Policy Recom-

mendations for a Strategic Framework, in Cyberpower and National Security, ed. by F.D. Kramer, S. Starr, L.K. Wentz, National Defense University Press, Washington (D.C.) 2009.
[7] Cfr. P. Scotto di Castelbianco, La cyber minaccia: attori, mutamenti e sfide al sistema Paese. Il ruolo della cyber intelligence, in Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale, a cura di U. Gori e L. S. Germani, FrancoAngeli editore, Milano, 2012.
[8]Cfr. U. Gori e L.S. Germani, Information Warfare 2010. Le nuove minacce provenienti dal cyberspazio alla sicurezza nazionale italiana, a cura di Id., FrancoAngeli, Milano, 2011
[9]Ad esempio nella Federazione Russa dove troviamo la compartecipazione a tutta la pianificazione sia dell'incaricato per la Operazione Militare Speciale, sia del Capo di Stato Maggiore della Difesa, sia del Ministro della Difesa, sia del Capo dei Servizi Segreti; ma anche nella stessa Ucraina, dall'altro lato della barricata, dove il Presidente ha assunto almeno formalmente la carica di amministratore di tutti i settori strategici, seppur coadiuvato da potenze estere.