La guerra ibrida

Alessandro Pascolini
Università di Padova

Il recente "non paper" del ministro della difesa Guido Crosetto "il contrasto alla guerra ibrida: una strategia attiva" ha attitato l'attenzione dell'opinione pubblica italiana sulle nuove forme di guerra cui l'Italia è esposta, assieme agli altri paesi europei e della NATO. Il documento definisce come minaccia ibrida "azioni coordinate in più domini condotte da attori statuali e non-statuali, al di sotto della soglia del conflitto armato e spesso non attribuibili, mirate a danneggiare, destabilizzare o indebolire".

In particolare, la minaccia ibrida in Italia comprende "vulnerabilità in energia, infrastrutture critiche ed ecosistema politico-sociale", mediante azioni cibernetiche ("minacce quotidiane sotto soglia alla pubblica amministrazione, sanità, energia, manifattura"),"disinformazione e interferenza nei processi elettorali; coercizione geo-economica; *choke points* logistici (Mar Rosso/Suez-Bab el-Mandeb); dimensione militare 'grigia' (sconfinamenti e posture coercitive, mercenari/contractors, esercitazioni provocatorie, disturbi alla navigazione)". Gli attori principali di tali minacce sono individuati in Russia, Cina, Corea del Nord e Iran.

Va notato che non esiste una definizione comune del concetto di guerra ibrida da un punto di vista accademico, storico o giuridico, ma sono state proposte varie interpretazioni da parte di teorici militari, esperti di politica e istituzioni internazionali; ciò riflette la complessità della sua natura ed evoluzione. Sostanzialmente, la guerra ibrida differisce dalla guerra tradizionale perché si estende oltre il campo di battaglia fisico. Le azioni ibride, per raggiungere obettivi politici, impiegano in modo coordinato e sincronizzato sia strumenti militari che cibernetici e mediatici moderni.

L'ambiguità è una caratteristica chiave ed elemento distintivo della guerra ibrida data la natura spesso non attribuibile di attività clandestine. Fornisce la capacità di colpire un avversario con molteplici elementi sincronizzati costringendolo in uno stato di impasse cognitivo riguardo alle intenzioni politiche, strategiche e tattiche dell'attaccante.

Evoluzione del concetto

Il concetto si è sviluppato ed espanso a tre differenti livelli: il primo riguarda operazioni sul campo di battaglia, il secondo aggiunge ai combattimenti attività nell'ambito comunicativo e cibernetico, il terzo comprende una varietà di azioni tutte assolutamente incruente.

La prima comparsa del termine 'guerra ibrida' (hybrid warfare) viene accreditata al 1998; il concetto è ripreso nel 2002, in uno studio della guerra russo-cecena, con riferimento all'impegno simultaneo e coordinato di forze militari convenzionali e irregolari (guerriglieri, ribelli, criminali e terroristi).

Da un punto di vista storico, in questi termini il fenomeno della guerra ibrida non è nuovo; si rintraccia negli scritti di Sun Tzu e di Tucidide (entrambi del V secolo aC). Nella storia più recente, eserciti imponenti come la Grande Armée di Napoleone, la Wehrmacht di Hitler e le forze francesi, prima, e americane, poi, in Viet Nam trovarono gravi difficoltà nell'affrontare eserciti convenzionali supportati da combattenti irregolari.

A livello tattico, in molti di questi conflitti, le varie componenti hanno operato in teatri diversi o in formazioni distintamente separate, con le forze irregolari impiegate per

operazioni secondarie rispetto alle forze convenzionali. Nelle guerre ibride del XXI secolo, i diversi elementi sono fusi in una stessa forza operante sul medesimo campo di battaglia.

Eventi del 2014 in Medio-oriente e in Ucraina hanno ridefinito radicalmente il quadro concettuale della guerra ibrida sia sul piano teorico che su quello pratico, ampliando il quadro delle operazioni ibride dai campi di battalia a un ampio spettro di azioni, in particolare nel dominio informativo. Alle articolate modalità ibride del coinvolgimento dell'Iran nella guerra civile siriana si aggiunse, con la conquista di Mosul, l'emergere dello Stato Islamico dell'Iraq e della Siria (Daesh) con le sue capacità economiche, informatiche, informative e l'efficace propaganda per un significativo proselitismo in vari paesi.

Sempre dal 2014, la Russia ha impiegato l'uso simultaneo di misure politiche, tecnologiche e militari per raggiungere i propri obiettivi in Ucraina, in piena ambiguità. Una serie di proteste e disordini politici nell'Ucraina orientale e in Crimea fu rapidamente e segretamente sfruttata dalla Russia per ottenere consenso alle successive azioni politiche e militari. Forze speciali (*spetznaz)* infiltrate addestrarono milizie locali, al fine di generare una situazione favorevole a un attacco convenzionale. La guerra condotta dai separatisti a Donetsk, nel Donbass e in Crimea è stata portata avanti tramite una combinazione di asset militari regolari e irregolari e il lancio di attacchi informatici a confondere gli osservatori locali e internazionali.

Numerosi accademici e centri di ricerca si sono impegnati ad analizzare e comprendere questo secondo livello di guerra ibrida, con una vasta produzione di documenti e pubblicazioni. La NATO ha preso le minacce ibride più seriamente, e nel 2015 ha dichiarato di voler sviluppare una strategia efficace per contrastare questa forma bellica, che "comporta un'interazione o fusione di mezzi convenzionali e non convenzionali come strumenti di forza e mezzi di sovversione. Le minacce ibride combinano mezzi militari e non militari, nonché mezzi palesi e occulti, tra cui disinformazione, attacchi informatici, pressione economica, dispiegamento di gruppi armati irregolari e uso di forze regolari. I metodi ibridi vengono utilizzati per confondere i confini tra guerra e pace e per tentare di seminare dubbi nelle menti delle popolazioni bersaglio. Mirano a destabilizzare e minare le società".

L'attenzione di ricercatori e analisti nel campo delle minacce ibride si andò spostando in modo crescente dagli aspetti militari alle operazioni di informazione e cognitive. Operazioni strategiche di informazione mirano a plasmare le narrative politiche nei paesi bersaglio, utilizzando programmi radio e televisivi mirati, finanziamento di think tank per promuovere le opinioni degli attaccanti, impiego di troll, bot e fabbriche di notizie false in Internet. L'obiettivo principale è quello di intorbidire le acque, degradare l'informazione e gettare dubbi sulle verità oggettive per accreditare le posizioni e le narrazioni del paese attaccante.

Ancora più preoccupanti risultano vere operazioni cognitive, atte a modellare le visioni del mondo, gli interessi e i sistemi di valori delle persone, trasformando la sfera cognitiva dei gruppi obiettivo. Un attacco cognitivo mira a trasformare la percezione della realtà e il processo decisionale delle singole persone e della coscienza collettiva. Esso sfrutta lo stress emotivo per ridurre la capacità di pensiero razionale delle vittime dell'attacco e guidarle verso le condizioni cognitive desiderate dall'avversario attaccante.

Si parla addirittura di 'colonizzazione digitale' qualora si raggiunga il controllo cognitivo di una porzione significativa della società attaccata dentro e attraverso il cyberspazio mediante l'uso delle moderne tecnologie dell'informazione, dei social media e degli strumenti di intelligenza artificiale. La colonizzazione digitale mira a gestire le visioni del

mondo, gli interessi e i valori delle persone, a differenza della conquista e colonizzazione di un territorio o dell'economia di uno stato.

La crescente attenzione agli aspetti incruenti della guerra ibrida ha portato alla presente fase del concetto, in cui il confronto ibrido non contempla necessariamente scontri armati.

A livello europeo, il Centro europeo di eccellenza per il contrasto alle minacce ibride (Hybrid CoE), creato a Helsinki, propone la definizione: "le minacce o campagne ibride descrivono azioni coordinate e sincronizzate che prendono deliberatamente di mira le vulnerabilità sistemiche delle istituzioni democratiche utilizzando un'ampia gamma di mezzi, mirando a influenzare diversi processi decisionali a livello locale, regionale, statale o istituzionale, per promuovere gli obiettivi strategici dell'agente e danneggiando l'obiettivo".

Anche il 'rapporto Niinistö' sulla "preparazione europea nella risposta civile e militare alle crisi", pubblicato nel novembre 2024, nel capitolo "Superare in astuzia gli attori malevoli per scoraggiare gli attacchi ibridi", affronta "le campagne ibride malevole progettate per destabilizzare, indebolire e dividere l'Unione europea (UE) e i suoi Stati membri, utilizzando – in modo coordinato – una combinazione di attività coercitive e sovversive, con metodi convenzionali e non convenzionali, pur rimanendo al di sotto della soglia di una guerra convenzionale aperta".

Un concetto sdrucciloso

Il rapporto Niinistö ritiene che "l'UE e i suoi Stati membri sono attualmente bersaglio di una campagna ibrida che coinvolge sabotaggio, attacchi informatici, coercizione economica, il disturbo e la falsificazione di segnali satellitari, la strumentalizzazione dei migranti, la manipolazione e l'interferenza straniera delle informazioni, così come l'infiltrazione politica." A fronte dell'esistenza concreta dell'aggressione ibrida, si propone di rafforzare la capacità dell'UE di "deterrenza attraverso la punizione", mediante "contromisure per colpire l'attore della minaccia con crescente precisione. L'UE dovrebbe segnalare chiaramente agli autori di minacce ibride che non potranno più sfuggire alle conseguenze delle loro attività dannose".

Il rapporto Niinistö evita accuratamente il termine 'hybrid war' e nella letteratura in inglese si distingue fra 'hybrid war' – attuale guerra ibrida, come per esempio in Ucraina, e 'hybrid warfare' – modalità ibrida di conduzione di un conflitto, la quale può essere anche solo potenziale, ma in italiano entrambi i termini vengono tradotti come 'guerra ibrida', non avendo gli studiosi e strateghi italiani sentito la necessità di distinguere i due aspetti con termini specifici.

Così il 'non paper' del ministro della difesa italiano conclude con la chiara affermazione: "È in atto una guerra continua che ci minaccia senza sosta, giorno e notte. Gli obiettivi sono le nostre infrastrutture critiche, i centri decisionali, i servizi essenziali, le strutture commerciali, le nostre industrie, le catene di approvvigionamento, il patrimonio cognitivo delle nostre popolazioni, e, in ultima analisi, la tenuta complessiva del Paese. È una guerra combattuta con 'bombe' meno visibili di quelle fisiche, ma che cadono incessantemente, producendo danni che, se guardiamo le tendenze e se non cambiamo l'approccio, potremmo non essere in gradodi contenere."

L'uso del termine 'guerra' senza attributi limitativi vuole chiaramente trasmettere un senso di estrema gravità, generare nelle istituzioni e nella popolazione un clima di tensione e di preparazione a privilegiare la 'difesa' rispetto agli altri obiettivi sociali, accettando un aumento di finanziamenti al settore militare, un aumento delle forze armate ('la leva volontaria'?) e la creazione di nuove unità, "un'Arma Cyber adeguatamente dimensionata e

capace di operare senza soluzione di continuità" e "un Centro per il Contrasto alla Guerra Ibrida dotato di comando e controllo per contrastare le azioni ostili nel campo della guerra cognitiva".

Un aspetto ancora più delicato della denuncia dello stato di 'guerra' è l'estensione dello spettro di opzioni che ci si riserva per reazioni 'punitive' di attacchi ibridi incruenti. Contromisure e punizioni potranno venir interpretate come un escalation del confronto, ad aggravare il livello dello scontro in una dinamica sempre più difficile da mantenere esente dal coinvolgimento militare.

Padova, 8 dicembre 2025