Oltre il dominio terrestre: è il Cyber il nuovo fronte della guerra moderna?

Pubblicato il 15/10/2026

Per secoli, la superiorità militare è stata determinata principalmente dalla capacità di conquistare e mantenere il controllo del territorio. Gli eserciti si affrontavano sul terreno, le offensive puntavano a occupare posizioni strategiche e la distruzione delle forze avversarie rappresentava uno dei principali strumenti per ottenere la vittoria. L'evoluzione dell'aviazione, delle forze navali e, successivamente, delle capacità spaziali ha progressivamente ampliato le dimensioni del conflitto, senza tuttavia eliminare la centralità delle operazioni terrestri.

Oggi questo equilibrio sta cambiando. Non perché carri armati, artiglieria, fanteria e mezzi convenzionali abbiano perso importanza, ma perché la loro efficacia dipende sempre più da infrastrutture tecnologiche che si trovano al di fuori del campo di battaglia tradizionale. Sistemi di comando e controllo, comunicazioni satellitari, reti informatiche, capacità di intelligence e piattaforme digitali costituiscono ormai una componente essenziale dello strumento militare.

Un esercito può disporre di una considerevole superiorità numerica e tecnologica, ma vedere compromessa la propria capacità operativa se un avversario riesce a

interrompere le comunicazioni, alterare il flusso delle informazioni o rendere indisponibili i sistemi dai quali dipende il coordinamento delle forze.

È in questo contesto che il dominio Cyber ha assunto un ruolo strategico. La sua particolarità non consiste soltanto nella possibilità di colpire sistemi informatici a distanza, ma nella capacità di produrre effetti che possono estendersi a tutti gli altri domini operativi. Il cyberspazio non rappresenta semplicemente un ulteriore ambiente nel quale confrontarsi con l'avversario: è diventato una delle infrastrutture sulle quali poggia l'intero funzionamento delle moderne Forze Armate.

Dalla conquista del territorio alla superiorità delle informazioni

Nel luglio 2016, durante il vertice di Varsavia, la NATO riconobbe ufficialmente il cyberspazio come dominio operativo, affiancandolo a quelli terrestre, aereo e marittimo. Nel dicembre 2019 anche lo spazio venne riconosciuto come dominio operativo, completando un quadro che oggi comprende cinque ambienti fondamentali: Land, Air, Maritime, Space e Cyberspace.

La decisione dell'Alleanza Atlantica non fu soltanto un aggiornamento della terminologia militare. Rappresentò il riconoscimento di una trasformazione che già interessava l'organizzazione, la pianificazione e la condotta delle operazioni.

La progressiva digitalizzazione dello strumento militare aveva infatti modificato il rapporto tra le forze impiegate sul terreno e i sistemi necessari per dirigerle. Le comunicazioni digitali, la condivisione delle informazioni e l'integrazione dei sensori consentono oggi di coordinare capacità distribuite su distanze considerevoli, riducendo i tempi necessari per individuare una minaccia, valutarla e decidere un eventuale intervento.

Questa evoluzione ha portato allo sviluppo delle operazioni multidominio, conosciute come *Multi-Domain Operations* (MDO), nelle quali le capacità terrestri, aeree, navali, spaziali e cyber vengono integrate per ottenere effetti coordinati.

Il principio alla base di questo approccio è che la superiorità in un singolo dominio non sia sempre sufficiente per conseguire un risultato operativo. Una forza terrestre può beneficiare del supporto dell'aviazione e dell'intelligence satellitare, mentre la disponibilità e la sicurezza dei collegamenti digitali possono diventare determinanti per il coordinamento dell'intera

operazione.

Da questa prospettiva emerge il ruolo particolare del Cyber. Mentre le forze terrestri operano sul territorio e quelle aeree nello spazio atmosferico, le infrastrutture informatiche attraversano trasversalmente tutti gli ambienti operativi, collegandone funzioni e capacità.

La superiorità informativa diventa quindi una componente fondamentale della superiorità militare. Non significa semplicemente possedere una quantità maggiore di dati, ma essere in grado di raccogliere informazioni attendibili, elaborarle, proteggerle e renderle disponibili ai decisori nel momento in cui sono necessarie.

L'Ucraina e la dimostrazione concreta della guerra nel cyberspazio

La guerra tra Russia e Ucraina ha offerto una delle dimostrazioni più significative dell'integrazione tra operazioni informatiche e attività militari convenzionali.

Il 24 febbraio 2022, circa un'ora prima dell'inizio dell'invasione russa, un attacco informatico colpì la rete di comunicazioni satellitari KA-SAT, gestita da Viasat. L'operazione provocò l'interruzione del servizio per migliaia di utenti in Ucraina e decine di migliaia di collegamenti in altre parti d'Europa.

Il 10 maggio dello stesso anno, l'Unione europea attribuì ufficialmente l'attacco alla Federazione Russa, indicando che l'operazione aveva contribuito a facilitare l'aggressione militare.

L'episodio è particolarmente importante perché dimostra come un'azione condotta nel cyberspazio possa precedere un'offensiva convenzionale e concorrere alla preparazione delle condizioni operative.

L'attacco non aveva distrutto il satellite né compromesso direttamente i suoi sistemi di bordo. Secondo la ricostruzione tecnica pubblicata da Viasat, gli aggressori avevano sfruttato una configurazione vulnerabile di un apparato VPN per accedere alla rete di gestione e impartire comandi che resero inutilizzabili numerosi modem degli utenti.

Si trattò quindi di una compromissione di sistemi terrestri di gestione delle comunicazioni satellitari, con conseguenze che si estesero su un'area geografica molto più vasta rispetto a quella direttamente interessata dalle operazioni militari.

Il caso KA-SAT evidenzia un aspetto centrale della guerra contemporanea: un'operazione informatica può compromettere una capacità strategica senza dover colpire fisicamente l'infrastruttura che la rende disponibile.

Nel corso del conflitto, entrambe le parti hanno dovuto confrontarsi con la necessità di proteggere le proprie comunicazioni, mantenere disponibili le informazioni e operare in un ambiente caratterizzato da attacchi informatici e intensa guerra elettronica.

L'impiego su larga scala di droni, sistemi di ricognizione e piattaforme digitali per il coordinamento delle unità ha ulteriormente accentuato l'importanza delle comunicazioni e della sicurezza dei dati.

Allo stesso tempo, la guerra in Ucraina ha mostrato i limiti delle operazioni cyber. La capacità di ripristinare i sistemi, utilizzare infrastrutture alternative e adattare le procedure operative ha spesso consentito di contenere gli effetti degli attacchi. Il cyberspazio non ha sostituito l'impiego della forza convenzionale, ma ne ha modificato le condizioni di esercizio.

Il comando e controllo come obiettivo strategico

Per comprendere pienamente il peso assunto dal dominio Cyber è necessario considerare il funzionamento dei moderni sistemi di comando e controllo, comunemente identificati con la sigla C2, *Command and Control*.

Ogni operazione militare richiede un flusso continuo di informazioni tra i comandi e le unità dipendenti. I comandanti devono conoscere la posizione delle proprie forze, ricevere dati sull'avversario, valutare l'evoluzione della situazione e trasmettere decisioni e ordini.

La digitalizzazione ha aumentato notevolmente la velocità con la quale queste informazioni possono essere distribuite e utilizzate, consentendo un coordinamento che in passato richiedeva tempi molto più lunghi.

La stessa evoluzione ha però introdotto nuove vulnerabilità.

Quando una funzione essenziale dipende da un'infrastruttura informatica, la compromissione di quest'ultima può tradursi in un problema operativo. Un collegamento interrotto può rallentare la trasmissione degli ordini; un sistema informativo non disponibile può ridurre la conoscenza della situazione; dati alterati possono compromettere l'affidabilità delle valutazioni effettuate dai

comandi.

L'effetto di un'operazione cyber non deve quindi essere necessariamente misurato in termini di distruzione fisica.

In determinate circostanze, interrompere un flusso informativo può risultare sufficiente per ritardare una manovra, ostacolare il coordinamento di più unità o limitare temporaneamente l'impiego di una capacità militare.

Questo non significa che le reti militari siano facilmente penetrabili. I sistemi più sensibili possono essere protetti attraverso segmentazione, ridondanza, cifratura e procedure alternative, comprese soluzioni che non dipendono da connessioni con reti pubbliche.

Tuttavia, la crescente complessità tecnologica rende la protezione delle informazioni una responsabilità che va ben oltre gli specialisti informatici.

La sicurezza del sistema di comando e controllo è oggi parte integrante della capacità di un'unità di svolgere la propria missione.

Una forza armata moderna deve quindi essere in grado non soltanto di utilizzare efficacemente le tecnologie disponibili, ma anche di continuare a operare quando parte di esse viene compromessa, disturbata o resa indisponibile.

Quando il conflitto supera i confini del campo di battaglia

Uno degli elementi che distinguono il cyberspazio dai domini militari tradizionali è il rapporto con le infrastrutture civili.

Le moderne società dipendono da sistemi digitali per la distribuzione dell'energia, le telecomunicazioni, i trasporti, la produzione industriale, l'approvvigionamento alimentare e il funzionamento dei servizi essenziali.

Molte di queste infrastrutture sono inoltre strettamente collegate alle capacità necessarie per sostenere un'operazione militare, direttamente o attraverso servizi forniti da operatori commerciali.

Di conseguenza, la vulnerabilità di una rete civile può assumere un significato strategico anche dal punto di vista della difesa nazionale.

Un esempio recente arriva dalla Francia, dove nell'ottobre 2026 un attacco informatico ha compromesso i sistemi di refrigerazione di numerosi supermercati, provocando la perdita di prodotti alimentari e consistenti danni economici.

Le ricostruzioni pubblicate il 14 e 15 ottobre descrivono la manipolazione di sistemi di controllo collegati a Internet, utilizzati per gestire il funzionamento degli impianti frigoriferi. Reuters ha riferito di circa 350 punti vendita colpiti, mentre altre ricostruzioni hanno indicato un numero più elevato di strutture interessate dalle anomalie.

La responsabilità dell'operazione non è stata ancora accertata pubblicamente e non vi sono elementi sufficienti per qualificarla come un attacco militare o attribuirla a uno Stato.

L'episodio assume tuttavia rilevanza per le conseguenze materiali prodotte attraverso la compromissione di sistemi digitali.

Nessuna infrastruttura è stata bombardata e non è stato necessario impiegare esplosivi per provocare l'interruzione di attività economiche. Gli effetti sono derivati dall'alterazione del funzionamento di apparati industriali controllati informaticamente.

Questo collegamento tra mondo digitale e mondo fisico rappresenta una delle principali questioni di sicurezza delle infrastrutture moderne.

Sistemi analoghi, pur con caratteristiche e livelli di protezione differenti, vengono utilizzati nella gestione dell'energia, dei processi industriali, dei trasporti e di numerose altre attività essenziali.

Una loro compromissione può produrre conseguenze economiche e operative e, nei casi più gravi, anche rischi per la sicurezza delle persone.

Il problema non riguarda esclusivamente il settore civile. Le Forze Armate dipendono, in misura variabile, da infrastrutture nazionali e commerciali per trasporti, approvvigionamenti, comunicazioni e supporto logistico.

La capacità di sostenere un conflitto prolungato è quindi legata anche alla resilienza dell'apparato industriale e dei servizi del Paese.

In questo quadro, la difesa del cyberspazio supera la protezione delle singole reti militari e diventa una componente della sicurezza nazionale.

La NATO e la trasformazione della difesa digitale

La crescente interdipendenza tra capacità militari e infrastrutture digitali ha portato la NATO a rafforzare progressivamente il proprio approccio alla difesa cyber.

Nel 2024 gli Alleati hanno concordato l'istituzione del NATO Integrated Cyber Defence Centre, con l'obiettivo di migliorare la protezione delle reti, la conoscenza delle minacce e l'integrazione della dimensione cyber nella pianificazione e nella condotta delle operazioni.

Il 13 gennaio 2026 l'Alleanza ha inoltre pubblicato la nuova *Alliance Digital Strategy*, un documento che delinea gli indirizzi della trasformazione digitale della NATO con una visione estesa fino al 2035.

La strategia attribuisce particolare importanza alla capacità di mantenere la superiorità informativa e decisionale attraverso infrastrutture digitali sicure, resilienti e interoperabili.

La trasformazione prevista non riguarda esclusivamente il rinnovamento degli apparati tecnologici. Coinvolge l'organizzazione delle informazioni, la gestione dei dati, l'integrazione dell'intelligenza artificiale, l'interoperabilità tra le forze alleate e la capacità di mantenere operative le funzioni essenziali anche in condizioni di comunicazioni degradate.

Il documento richiama inoltre l'adozione dei principi *Zero Trust*, basati sulla verifica continua degli accessi e sulla limitazione dei privilegi, nonché la necessità di predisporre sistemi ridondanti e soluzioni alternative per garantire la continuità delle missioni.

L'obiettivo è assicurare che i comandanti possano continuare a ricevere informazioni, prendere decisioni e dirigere le forze anche quando parte delle infrastrutture digitali risulti compromessa.

Questa impostazione evidenzia una trasformazione importante del concetto stesso di prontezza operativa. Accanto alla disponibilità di uomini, mezzi, munizioni e capacità logistiche, assume crescente rilevanza la capacità di proteggere e mantenere funzionanti i sistemi informativi dai quali dipende l'attività militare.

Il cambiamento interessa anche la formazione del personale. Le competenze informatiche specialistiche rimangono indispensabili, ma la consapevolezza delle vulnerabilità digitali e la capacità di operare in condizioni tecnologicamente degradate devono trovare spazio anche nell'addestramento delle unità convenzionali.

Una competizione che può precedere il conflitto armato

Il cyberspazio introduce inoltre una dimensione temporale differente rispetto alla guerra convenzionale.

La preparazione di un'operazione informatica può svilupparsi molto prima dell'inizio delle ostilità, attraverso attività di ricognizione delle reti, individuazione di vulnerabilità, raccolta di informazioni e tentativi di accesso a infrastrutture considerate strategiche.

Alcune di queste attività possono essere riconducibili allo spionaggio, altre alla criminalità informatica o a campagne di pressione politica. Non ogni intrusione costituisce una preparazione militare e l'attribuzione delle responsabilità richiede verifiche tecniche e di intelligence.

Tuttavia, la possibilità che un attore statale cerchi di acquisire accessi utilizzabili in una successiva situazione di crisi rappresenta una questione rilevante per la sicurezza nazionale.

Il cyberspazio permette infatti di sviluppare attività ostili anche in assenza di uno scontro armato aperto, rendendo meno immediata la distinzione tra competizione strategica, spionaggio e operazioni militari.

Questa caratteristica pone problemi anche sul piano giuridico.

La NATO riconosce che un attacco informatico particolarmente grave potrebbe, in determinate circostanze, portare all'invocazione dell'articolo 5 del Trattato Nord Atlantico, relativo alla difesa collettiva.

Non esiste tuttavia un automatismo che trasformi qualsiasi cyberattacco in un'aggressione armata. La valutazione dipende dalle circostanze, dagli effetti prodotti e dalle decisioni politiche degli Stati alleati.

Rimane il fatto che la capacità di esercitare pressione contro infrastrutture e istituzioni di un altro Paese non richiede necessariamente lo spostamento di forze militari attraverso una frontiera.

È una delle ragioni per cui la sicurezza cyber viene ormai considerata parte integrante della deterrenza e della preparazione alla difesa.

Il futuro dei conflitti e il ruolo del dominio terrestre

La crescente centralità del cyberspazio non deve portare a sottovalutare le lezioni della guerra convenzionale.

Il conflitto in Ucraina continua a dimostrare che il controllo del territorio, la capacità di manovra, la potenza di fuoco, la disponibilità di munizioni e la tenuta logistica rimangono fattori determinanti.

L'impiego di nuove tecnologie non ha eliminato la necessità di conquistare e difendere posizioni, proteggere le linee di rifornimento e sostenere le unità impegnate nelle operazioni.

Ha però modificato profondamente le condizioni nelle quali queste attività vengono condotte.

Un esercito che dispone di mezzi avanzati, ma non è in grado di proteggere le proprie comunicazioni e mantenere affidabili i sistemi di comando, può perdere parte del vantaggio offerto dalla propria superiorità tecnologica.

Allo stesso modo, una forza dotata di sistemi meno sofisticati ma capace di adattarsi rapidamente, distribuire le proprie infrastrutture e mantenere la continuità operativa può dimostrare una resilienza maggiore di quanto suggeriscano le sole caratteristiche dei mezzi disponibili.

La sfida non consiste quindi nel trasferire la guerra dal dominio terrestre a quello cyber, ma nell'integrare quest'ultimo nella preparazione e nella condotta delle operazioni, senza creare dipendenze tecnologiche eccessivamente vulnerabili.

La superiorità militare del futuro dipenderà anche dalla capacità di combinare efficacemente potenza convenzionale, informazioni, sicurezza digitale e resilienza organizzativa.

La guerra non si combatte più soltanto sul terreno

La trasformazione in corso impone di riconsiderare il modo in cui viene valutata la potenza militare di uno Stato.

Il numero di carri armati, aeromobili, unità navali e militari continua a fornire indicazioni importanti sulla consistenza delle Forze Armate, ma non descrive da solo la capacità di impiegare efficacemente queste risorse.

La disponibilità di reti sicure, sistemi di comunicazione resilienti, informazioni attendibili e infrastrutture digitali affidabili è ormai una componente essenziale dell'efficienza operativa.

Un attacco informatico non è necessariamente in grado di ottenere gli stessi risultati di un'offensiva convenzionale, così come la compromissione di una rete non equivale automaticamente alla neutralizzazione di una forza militare.

Ma il cyberspazio ha introdotto nuove possibilità per condizionare le operazioni dell'avversario, interferire con le sue capacità e influire sulla preparazione e sulla prosecuzione di un conflitto.

Il dominio terrestre rimane uno degli ambienti nei quali si determinano gli esiti della guerra. Il dominio Cyber, tuttavia, è diventato una componente dalla quale può dipendere la capacità stessa di combattere efficacemente sulla terra, nel cielo e sul mare.

È questa la trasformazione più significativa: il fronte non coincide più necessariamente con il luogo nel quale sono schierati i soldati.

Può estendersi alle reti di comunicazione, ai sistemi di comando, alle infrastrutture energetiche e ai servizi che sostengono l'apparato militare e industriale di un Paese.

La guerra del XXI secolo continuerà a richiedere soldati, mezzi e capacità convenzionali. Ma una parte sempre più importante delle condizioni che ne determinano l'impiego si definirà anche nel cyberspazio, spesso ben prima che le forze contrapposte entrino in contatto.