

COGNITIVE WARFARE, MA È VERA GUERRA? LA COSTRUZIONE DELLA RESILIENZA PER I MILITARI

Capo Gruppo di Lavoro

Dott.ssa Alessia Chiriatti

Autori

Gen. C.A. Antonio Venci

Dott.ssa Alessia Chiriatti

Dott.ssa Alessia Dorigoni

Dott. Pino Finocchiaro

Dott. Giulio Chiarantoni

**Studio commissionato da S.M.E.
2026**

Email

info@centrostudiesercito.it

Indirizzo

Viale Bruno Buozzi 47,
Roma, 00197

Sito web

www.centrostudiesercito.it

PREFAZIONE DEL PRESIDENTE DEL CENTRO STUDI ESERCITO

Gli Autori chiariscono il concetto emergente di "*cognitive warfare*" e spiegano come questo tipo di conflitto possa operare, gettando così luce su di una categoria polemologica divenuta attuale con il diffondersi dell'uso dei nuovi media. E' un fatto evidente che "la potenza militare operi oggi dentro un ambiente cognitivo accelerato. Ogni operazione cinetica produce effetti informativi; ogni successo tattico viene immediatamente tradotto in narrazione strategica; ogni vulnerabilità sul campo può essere amplificata in forma simbolica; ogni decisione politica viene esposta a pressioni comunicative interne ed esterne". Non che le campagne di disinformazione non fossero attuate anche in passato, oggi però esse risultano pervasive e immediate proprio per effetto della rete e delle piattaforme *social*. Una struttura questa che ora ci ingloba e che esprime sue proprie capacità manipolative, come gli algoritmi che selezionano le informazioni in base agli interessi dei singoli utenti. L'uomo abita la tecnica e da essa è dominato mentre si smarrisce la percezione dell'Essere e la verità diventa post-verità. Partendo da questi fatti, descritti con attenzione agli aspetti tecnologici, le analisi di alcuni pensatori del nostro tempo sono qui proposte per portare all'attenzione del lettore le vulnerabilità delle società occidentali, ora suddivise in infosfere, dove la comunicazione circola e si diffonde con tale rapidità da ridurre i tempi naturali della riflessione critica. Tra gli argomenti trova spazio anche la psicologia del profondo perché ormai è noto come una comunicazione mirata ad attivare gli archetipi dell'inconscio collettivo riesca a polarizzare l'opinione pubblica, rendendo certe idee strumenti di mobilitazione per le masse. Quindi, le neuroscienze vengono chiamate in causa per mostrare come oggi la conoscenza del sistema nervoso consenta di trasformare le strategie della guerra cognitiva in azioni capaci di generare effetti materiali sulle coscienze, ovviamente

all'insaputa del singolo soggetto e di intere collettività quando diventano bersaglio di campagne malevoli. In tale prospettiva il presente lavoro tratta anche delle neurotecnologie applicate, un campo di ricerca avveniristico, ma con notevoli implicazioni etiche. Perché la guerra cognitiva si inserisce nel quadro dei conflitti che travagliano la nostra epoca. In tale quadro i militari sono anch'essi strumenti, bersaglio e soggetti attivi. Ritroviamo così descritti concetti come "caporale strategico", "operazioni basate sugli effetti" e guerra ibrida, ambiti in cui la guerra cognitiva si dispiega. Per difendere le nostre società da questo pervasivo strumento di offesa, capace di delegittimare l'azione dei governi, plasmare secondo un diverso interesse le competizioni elettorali nei paesi democratici, polarizzare le opinioni pubbliche sino a creare torbidi occorre formazione culturale, addestramento all'uso dei social e strutture ad hoc a livello governativo per individuare e neutralizzare le minacce, ma senza compromettere la democraticità dei processi che caratterizzano l'Occidente liberale e democratico. In tale quadro, la resilienza dei militari è un aspetto rilevante, pertinente alla cultura organizzativa militare. Quindi il presente lavoro mostra come soldati motivati dai valori fondanti di questa cultura e ben addestrati a svolgere i propri compiti istituzionali siano già resilienti alle campagne della guerra cognitiva e capaci di non diventare inconsapevoli agenti al servizio delle entità malevoli che operano nella comunicazione.

Gen. C.A. (ris.) Salvatore Farina

Presidente del Centro Studi Esercito



Abstract

Il presente studio analizza l'emergere del *Cognitive Warfare* (guerra cognitiva) come strumento pervasivo di competizione geopolitica e minaccia ibrida. In un contesto fortemente digitalizzato, l'ambiente informativo viene sfruttato da attori ostili non solo per diffondere propaganda, ma per degradare sistematicamente i processi decisionali, la capacità di giudizio critico e l'identità sia delle società civili sia degli apparati di difesa. Attraverso un approccio multidisciplinare, l'opera esamina inizialmente la centralità del dominio cognitivo nelle transizioni di potenza globali e la necessità di una cultura militare solida, basata su addestramento ed etica, come primo bastione di resilienza. Successivamente, lo studio approfondisce le basi neurobiologiche della vulnerabilità digitale, analizzando come le architetture algoritmiche alterino i meccanismi di ricompensa dopaminergica e creino false memorie, per poi spingersi fino alle frontiere etiche e operative delle neurotecnologie e delle interfacce cervello-computer. La ricerca conclude che il contrasto alla guerra cognitiva richiede il passaggio a una sicurezza cognitiva di tipo *whole-of-society*, in cui la cooperazione tra istituzioni, università e industria promuova il pensiero critico e tuteli i valori democratici di libertà e pluralismo.

Premessa

A cura di Pino Finocchiaro

La superiorità cognitiva

La guerra cognitiva si vince con cognizione di causa. Obiettivo della Cogware è la supremazia cognitiva. Il dominio cognitivo può essere compreso, vissuto e affrontato solo in un'ottica multidominio. La guerra cognitiva cerca di sfruttare i vari aspetti del dominio cognitivo per distruggere, minare, influenzare o modificare i processi decisionali modificando il comportamento umano e i processi cognitivi attraverso ogni mezzo e risorsa tecnologica usando qualsiasi tattica militare o non militare, traguardando qualunque operatore militare o la population civile si trovi coinvolto nello spettro della crisi.

Agire nel multidominio implica l'adozione di tattiche ibride. In un quadro strategico che deve tener conto dell'ambiente complesso in cui si opera e delle sue imprevedibili opzioni. Il comitato scientifico della Nato, STO, ha individuato alcune macro priorità:

1. **Competizione nelle aree di evoluzione scientifica, tecnica e tecnologica.**

L'obiettivo è proteggere i propri processi decisionali e al contempo compromettere, confondere e condizionare quelli avversari. Le società vulnerabili si mostrano incapaci a reagire efficacemente.

Questo nuovo campo di battaglia multidominio ci ricorda che il dominio cognitivo col suo mix di dati negati, azioni di influenza camuffate, informazioni occultate e lunghe marce sui sentieri della comprensione e del comportamento procura fatica non solo mentale ma anche fisica nei nostri combattenti digitali e non solo digitali. Seguire il filo di un pensiero che è al tempo stesso minaccia, concreta.

«Le fatiche, gli sforzi, le privazioni costituiscono in guerra un elemento distruttore – leggiamo nel Vom Kriege di Clausewitz – che non appartiene precisamente alla lotta, ma che, più o meno, ne è inseparabile. I suoi effetti si manifestano soprattutto nel campo strategico (...) in cui i tempi e gli spazi sono maggiori, l'effetto non solo è sempre sensibile, talvolta è decisivo».

2. La gara globale per garantirsi la superiorità nell'ambito dell'intelligenza artificiale e delle applicazioni della fisica quantistica.

L'intelligenza artificiale (AI) è necessaria come moltiplicatore di influenza. I sistemi di AI generativi e gli agenti autonomi riducono drasticamente i tempi decisionali sul campo di battaglia.

La sovranità algoritmica, correlata nell'approccio multidominio, mira a sviluppare tecnologie proprietarie per evitare la dipendenza da algoritmi e dati controllati da attori ostili.

3. La rivoluzione nel campo delle bio tecnologie.

Qui l'impegno maggiore consiste nell'occultare agli avversari i progressi ottenuti in un campo da tutelare con rapidità e riservatezza. A che punto siano giunti i nostri scienziati nel campo delle reti neurali è un segreto assoluto, paragonabile soltanto ai successi dei nostri esperti nel campo della guerra meteorologica.

4. Il divario nell'accesso alle risorse.

I conflitti nel mondo nascono per il dominio delle risorse, non solo energetiche. Manca l'acqua. L'acqua da bere e bagnare i terreni e per impastare il pane e per coltivare il riso. La scelta delle priorità è un atto strategico.

5. La frammentazione della coscienza collettiva con conseguente indebolimento dell'opinione pubblica.

La disintegrazione della coscienza collettiva è uno dei principali obiettivi della guerra cognitiva. È praticabile solo teorizzando la sua esistenza come fece il filosofo positivista Auguste Comte e come razionalizzò il suo discepolo Emile Durkheim, considerato il padre della moderna sociologia.

Secondo il filosofo e sociologo francese la coscienza collettiva si concretizza *«nell' insieme delle credenze e dei sentimenti comuni alla media dei membri di una stessa società»*.

Il frammentarsi dei valori condivisi da un gruppo sociale o meglio ancora da una comunità porta all'anomia, ovvero all'assenza di norme. Nella realtà l'anomia non si riferisce all'assenza di regole ma al distacco profondo tra la legge morale dell'individuo o di intere frazioni del corpo sociale rispetto alla legge pubblica. L'anomia porta così al distacco dal sentimento comune, all'emergere di conflittualità, alla mancata adesione ai modi e alle mete sociali. All'estraneamento individuale e alla ribellione di sottogruppi sociali. C'è chi continua a vivere nel gruppo sentendosi non rappresentato, offeso e/o danneggiato dalle scelte dei vertici sino ad assumere atteggiamenti di cruccio e risentimento palesi. Altri si distaccano per ribellione nella speranza che le loro idee prevalgano coltivando un pensiero riformista o intellettualmente rivoluzionario. Altri ancora scadono in comportamenti devianti.

Secondo Robert K. Merton: *«Per struttura sociale, si intende quel complesso organizzato di rapporti sociali i cui i membri della società o del gruppo sono variamente implicati»*.

«L'anomia, quindi, viene concepita come una frattura nella struttura culturale che ha luogo particolarmente quando si stabilisce un conflitto fra le norme culturali e le mete che queste norme impongono e le capacità socialmente strutturate dei membri del gruppo di agire in conformità».

6. La dipendenza tecnologica e le difficoltà di integrazione.

La guerra globale per le terre critiche conferma sempre di più l'impossibilità di accrescere il nostro arsenale cyber-cognitivo sino a quando non potremo aver accesso ai giacimenti di terre rare.

Il campo di battaglia cognitivo. La guerra cognitiva si applica su ogni campo di conoscenza della comunità, società, nazione presi di mira. Ed è il mantenimento dei livelli di conoscenza – cognizione di causa – il miglior modo per difendersi dagli attacchi con azioni di influenza intense al punto da scardinare i punti di riferimento culturali della comunità sotto attacco.

Partiamo da quel che spiega Sun Tzu nell'arte della guerra a proposito di conoscenza: *«Se conosci il nemico e conosci te stesso, nemmeno in cento battaglie ti troverai in pericolo. Se non conosci il nemico ma conosci te stesso, le tue possibilità di vittoria sono pari a quelle di sconfitta. Se non conosci né il nemico né te stesso, ogni battaglia significherà per te sconfitta certa».*

L'obiettivo primario del nemico è disconnettere le nostre connessioni tecnologiche in modo da far passare la sua narrazione. In buona sostanza, l'avversario punta a influenzare i nostri processi cognitivi e i nostri comportamenti per trarne multipli vantaggi. Crea un campo di battaglia cognitivo per interferire e manipolare l'avversario.

A livello sociale mette in discussione la democrazia e il ruolo delle leggi e norme condivise, con l'idea di scardinare il contratto sociale. A livello di gruppi e comunità destabilizzando gli accordi e creando nuove polarizzazioni. Il dubbio, la confusione creati con il disfacimento delle intese collettive colpisce a livello individuale attitudini, capacità di prendere decisioni nell'interesse collettivo e nei comportamenti.

La nostra risposta ha per obiettivo il degrado delle capacità dell'avversario; implementare la nostra resistenza, costruire e propagare fattori di resilienza; migliorare la conoscenza umana e tecnologica. In questa dinamica l'avversario ricorre ai vecchi arnesi dello spionaggio con tattiche militari che si rifanno alle *PsyOps* (operazioni psicologiche) o *InfoOps* (operazioni informative) come parte di comunicazioni strategiche (Stratcom).

Superiorità cognitiva. Dal 2021 gli studi della Nato si sono concentrati sul concetto di superiorità cognitiva. Intanto si ottiene grazie a una diuturna vigilanza perché non è un conflitto dichiarato, però armato con armi non convenzionali ma non per questo meno efficaci.

Afferma Emile Durkheim che i periodi di disintegrazione sociale sono caratterizzati dal dilagare dell'anomia. Le campagne di influenza vanno subito contrasta-

te perché usano strumenti raffinati spesso non percepiti dal pubblico, talvolta neppure dagli esperti militari e della comunicazione.

I cavalli di battaglia del KGB erano la *disinformatia* e la *misinformatia*. Pericolosi soprattutto quando si combinano in una sorta di effetto ciclone, un turbine talmente intenso da nascondere il cumulo di falsità dal quale ha preso energia.

- La *disinformatia* è pura menzogna in modo da apparire autentica. Non è difficile da svelare.
- La *misinformatia* consiste nella propagazione della falsa notizia con argomenti che la fanno apparire vera.

Ci sono libri e film anti-sistema realizzati in occidente che hanno goduto di buon pubblico. Eppure erano stati scritti da agenti del KGB che poi hanno messo il soggetto o il manoscritto in mano a scrittori occidentali che li hanno firmati e proposti, consapevolmente, a produttori e editori. Talvolta con successo. In altri casi sono stati passati sotto banco a scrittori, *influencer* e persino scienziati che li hanno propagati per alimentar il più becero complottismo. Lo hanno fatto inconsapevolmente. Per questo meritano appieno l'appellativo coniato per loro nel mondo delle spie: *utili idioti*.

Mitigare e rispondere all'attacco cognitivo. Tempo, spazio, modi e mete sono essenziali nel multidominio per raggiungere la superiorità cognitiva. La guerra cognitiva si combatte sempre. H24 e 7 giorni su 7. Si combatte in tempo di pace, di crisi e di guerra.

A giugno 2026 il *Nato Defense College* ha riunito i responsabili militari dei paesi alleati per fare il punto sulla supremazia cognitiva dell'Alleanza Atlantica ed ha ribadito che la resilienza è un fatto sociale e va affrontato con l'intesa di industria, università e governo. Il modello di difesa Finlandese, ad esempio, punta su un approccio sociale generalizzato con ricadute significative sulla resilienza nazionale.

La salute mentale è fondamentale per la resilienza cognitiva. Una società in grado di navigare nell'incertezza, adattarsi e resistere alle manipolazioni deve poggiare su solide basi di benessere diffuso tra la popolazione.

Sun Tzu: «*Il fine del dare forma alle operazioni militari è diventare senza forma. Quando si è senza forma, nemmeno le spie più abili riescono a scoprire nulla e il nemico saggio non avrà elementi per poter preparare i suoi piani*».

Difendere la propria competenza in un clima economico conflittuale è diventato una priorità. La modernità liquida di cui parla il sociologo polacco Zygmunt Bauman ha reso fluido persino il diritto a un lavoro stabile giacché i conflitti economici diventano la prosecuzione della guerra con altri mezzi. Non basta sapere di più degli altri. Bisogna conoscere cosa sanno gli altri della nostra competenza. Bisogna saperlo prima.

«La partita del dominio nell'era della modernità liquida – spiega Bauman – non viene giocata tra il più grande e più piccolo, ma tra il più veloce e il più lento. Chi è capace di accelerare in modo da risultare imprevedibile, domina».

Clausewitz è categorico: *«Sapere è qualcosa di diverso dal potere – giacché – la guerra non appartiene né al dominio dell'arte né a quello della scienza, ma al dominio sociale»*. Ancora: *«La guerra è un conflitto di grandi interessi»*; pertanto la conoscenza dell'avversario e di se stessi, ovvero la conoscenza del nostro sistema sociale e della capacità di tollerare l'impegno bellico da parte di ogni singola comunità che compone il concetto di Nazione, Patria, Popolo, resta alla base dell'esercizio di superiorità nel multidominio. Poiché, dice Clausewitz, *«Non si fa la guerra a un avversario astratto, ma ad un nemico reale che non si deve mai perdere di vista»*.

Autorità e potere. Secondo Tocqueville, *«la libertà è immunità dal potere»*. Il pensatore francese, studiando la società americana e gli sviluppi della sua democrazia, affronta al pari di Comte e Durkheim l'antica dicotomia tra autorità e potere.

Lo stato centralizzato retto da un sistema politico democratico che si basa su una costituzione e un sistema elettorale aperto rappresenta l'autorità e salvaguarda gli ultimi, i poveri dalle angherie del potere feudale, territoriale, economico.

La superiorità cognitiva non difende solo i centri di potere e i centri decisionali. Protegge gli esseri umani. La libertà di pensare con un cervello né contaminato né bombardato dai dubbi irrorati nei canali social alla stregua di un veleno nell'acquedotto.

Dobbiamo costruirci roccaforti della conoscenza. Bastioni immateriali del sapere che poggino sulla competenza, non sui titoli. Qui si parla di valore reale delle

competenze forgiate nell'esperienza, non sulle chiacchiere. Dobbiamo armare un popolo al piacere e al dovere della cultura.

Dove troveremo tante armi? Dove impareremo a usarle? Come allargheremo a tutti, senza distinzioni di censo, di razza, di sesso l'accesso ai granai del sapere? Alexis de Tocqueville non ha dubbi, ricorda quel che accadde dopo la rivoluzione francese: *«La letteratura divenne un arsenale aperto a tutti, in cui i deboli e i poveri si recarono ogni giorno a cercare delle armi»*.

Indice

Abstract	
Premessa	
A cura di Pino Finocchiaro	
Indice	
1 <i>Power in transitions</i> e centralità del dominio cognitivo. Trasformazioni della potenza nella competizione strategica contemporanea	1
2 La guerra cognitiva e la costruzione della resilienza dei militari	11
2.1 Abstract	12
3 La guerra cognitiva nell'era digitale, Basi neurobiologiche della vulnerabilità cognitiva e Implicazioni per la sicurezza	14
3.1 Abstract	14
3.2 Introduzione	15
3.3 La guerra cognitiva: definizione, perimetro e specificità	16
3.4 Tassonomia dell'informazione falsa e diffusione nei media sociali	17
3.5 Il cervello di fronte alla disinformazione: circuiti della ricompensa ed effetto di verità illusoria	18
3.6 Le basi neurali dell'influenza persistente: CIEM e memoria falsa	19

3.7	Meccanismi cognitivi della vulnerabilità: <i>bias</i> , cecità attenzionale e cognizione motivata	21
3.8	Amplificazione algoritmica e guerra cognitiva digitale	22
3.9	Il formato come dimensione strategica: non solo cosa, ma come	23
3.10	Strategie di contrasto: <i>debunking</i> , <i>prebunking</i> e resilienza cognitiva	25
3.11	Conclusioni	27
4	Neurotecnologie applicate	29
4.1	Nuove, vecchie tecnologie	29
4.2	Funzionamento della tCS	30
4.3	Applicazioni militari della tCS	32
4.4	Funzionamento della TMS	33
4.5	Applicazioni militari della TMS	34
4.6	Funzionamento delle BCI	35
4.7	Applicazioni militari delle BCI	35
4.8	Direzioni future	36
	Glossario degli Acronimi	42

1

Power in transitions
e centralità del dominio
cognitivo.

Trasformazioni della potenza
nella competizione
strategica contemporanea

A cura di Alessia Chiriatti

La competizione strategica contemporanea impone di ripensare il concetto stesso di potenza. Le categorie tradizionali della politica internazionale, costruite attorno alla disponibilità di risorse materiali, alla capacità militare, al controllo territoriale e alla superiorità economica, restano essenziali, ma non sono più sufficienti a spiegare come gli attori statali e non statali producano influenza, coercizione e vantaggio competitivo. La potenza non scompare nella transizione; cambia forma, cambia ritmo e cambia spazio di esercizio. In questa trasforma-

zione, il dominio cognitivo assume una centralità crescente perché rappresenta l'ambiente nel quale percezioni, decisioni, aspettative, fiducia istituzionale e orientamenti collettivi vengono costruiti, contestati e manipolati.

L'espressione "*power in transitions*" può essere intesa in due sensi complementari. Il primo riguarda la potenza nelle transizioni sistemiche: la competizione tra grandi potenze, la crisi dell'ordine liberale, la frammentazione della globalizzazione, la militarizzazione dell'interdipendenza e la riemersione della guerra convenzionale in Europa. Il secondo riguarda la transizione della potenza: il modo in cui la capacità di influenzare il comportamento altrui si sposta progressivamente da una logica prevalentemente materiale a una logica integrata, nella quale strumenti militari, tecnologici, economici, informativi e cognitivi operano in modo sinergico. In questo quadro, la potenza non coincide più soltanto con ciò che un attore possiede, ma con la sua capacità di orientare l'ambiente decisionale entro cui altri attori definiscono interessi, minacce e opzioni disponibili.

Il punto di partenza resta classico: la potenza è relazione. Essa non esiste in astratto, ma si manifesta nella capacità di produrre effetti sul comportamento di altri soggetti. Tuttavia, la natura di questa relazione è mutata. Nella tradizione realista, la potenza veniva letta soprattutto come disponibilità di risorse tangibili: popolazione, territorio, forza militare, capacità industriale, risorse energetiche, posizione geografica. Con l'evoluzione degli studi sulle relazioni internazionali, il concetto si è ampliato fino a includere forme indirette e immateriali di influenza: legittimità, attrazione, reputazione, capacità normativa, controllo delle reti, produzione di conoscenza. La competizione contemporanea porta questa evoluzione a un livello ulteriore: il potere consiste sempre più nella capacità di strutturare i processi cognitivi attraverso i quali individui, élite e società interpretano la realtà.

Questa trasformazione non implica il superamento dell'*hard power*. Al contrario, la guerra in Ucraina ha mostrato la persistente centralità della forza militare, della logistica, della profondità industriale, della difesa aerea, dell'artiglieria, dell'intelligence e della capacità di sostenere nel tempo uno sforzo bellico ad alta intensità. La NATO, nel Concetto Strategico del 2022, ha definito la Federazione Russa come la minaccia più significativa e diretta alla sicurezza degli Alleati e ha richiamato l'uso integrato di strumenti convenzionali, cyber e ibridi da parte di Mosca. Lo stesso documento collega deterrenza, resilienza e contrasto alle interferenze ostili, segnalando che la difesa dello spazio euro-atlantico non può

essere ridotta alla sola dimensione militare convenzionale.

La novità sta nel fatto che la potenza militare opera oggi dentro un ambiente cognitivo accelerato. Ogni operazione cinetica produce effetti informativi; ogni successo tattico viene immediatamente tradotto in narrazione strategica; ogni vulnerabilità sul campo può essere amplificata in forma simbolica; ogni decisione politica viene esposta a pressioni comunicative interne ed esterne. La dimensione fisica della guerra resta decisiva, ma il suo significato politico viene costruito attraverso processi di percezione. Ciò vale per il morale delle popolazioni, per la coesione delle alleanze, per la credibilità della deterrenza, per la disponibilità dei cittadini ad accettare costi economici e per la capacità dei governi di sostenere strategie di lungo periodo.

La competizione strategica contemporanea si colloca quindi in uno spazio intermedio tra guerra e pace. Le minacce ibride sono precisamente il prodotto di questa zona grigia. Il Consiglio dell'Unione europea definisce le minacce ibride come attività coordinate e malevole che mirano a indebolire Stati o istituzioni attraverso una combinazione di strumenti, tra cui manipolazione dell'informazione, cyberattacchi, influenza economica, coercizione diplomatica e minacce militari. Tali campagne sono progettate per restare sotto la soglia della guerra aperta, rendendo più difficile l'attribuzione, la risposta e la mobilitazione politica. In tale contesto, il potere non si esercita soltanto attraverso la distruzione o la coercizione diretta, ma attraverso la produzione di ambiguità. L'obiettivo non è necessariamente convincere un avversario della verità di una determinata narrazione. Spesso è sufficiente creare dubbio, paralizzare la decisione, alimentare sfiducia, rendere più costoso il consenso interno, frammentare la percezione pubblica della minaccia. Questa è una delle trasformazioni più rilevanti del potere: la sua efficacia non dipende sempre dall'imposizione di una visione alternativa coerente, ma dalla capacità di degradare la capacità cognitiva dell'avversario, cioè la sua possibilità di distinguere, gerarchizzare e decidere.

Il dominio cognitivo diventa dunque il punto di connessione tra sicurezza, politica e società. Esso riguarda il modo in cui gli attori percepiscono il contesto, attribuiscono intenzioni, valutano rischi, interpretano segnali e costruiscono aspettative. In termini strategici, la cognizione è il presupposto della decisione. Se un attore riesce a interferire con il ciclo decisionale dell'avversario, può ottenere vantaggi anche senza prevalere sul piano materiale. Può rallentare una risposta, produrre divisioni tra alleati, indebolire la fiducia nelle istituzioni, orientare

un dibattito pubblico, condizionare l'agenda politica. In questo senso, la competizione cognitiva non è un'aggiunta alla competizione strategica: ne è una componente strutturale.

Il concetto di *cognitive warfare* nasce proprio da questa consapevolezza, anche se resta oggetto di dibattito. La letteratura recente lo descrive come un campo ancora in via di definizione, collocato all'intersezione tra guerra ibrida, *information warfare*, *cyber operations*, psicologia, neuroscienze, scienze comportamentali e tecnologie emergenti. Uno studio pubblicato su *Frontiers in Big Data* osserva che la *cognitive warfare* mira allo sfruttamento della cognizione umana e della tecnologia per disturbare, influenzare o modificare i processi decisionali; segnala inoltre che non esiste ancora una definizione pienamente condivisa e che il concetto tende a sovrapporsi a categorie come FIMI, *hybrid threats* e *information warfare*.

Questa incertezza concettuale non riduce la rilevanza del fenomeno. Anzi, ne rivela la natura transitoria. La *cognitive warfare* è ancora difficile da misurare empiricamente perché molte sue pratiche restano coperte, distribuite, indirette e spesso attribuibili solo in termini probabilistici. Tuttavia, la sua utilità analitica consiste nel mettere a fuoco un passaggio essenziale: il *target* della competizione non è soltanto l'informazione, ma il modo in cui l'informazione viene ricevuta, interpretata e trasformata in comportamento politico. La differenza è sostanziale. L'*information warfare* opera sul flusso, sulla disponibilità e sulla manipolazione dei contenuti. La *cognitive warfare* opera sul rapporto tra contenuti, emozioni, bias, identità, appartenenze e decisioni.

La NATO ha progressivamente attribuito rilievo a questa dimensione. La *NATO Science and Technology Organization* descrive la *cognitive warfare* come la lotta per la superiorità cognitiva e la considera una sfida strategica di ricerca; il tema è entrato nel dibattito dell'Alleanza come parte della riflessione sulle tecnologie emergenti, sulla resilienza e sulla preparazione operativa. Anche la pagina NATO sulle minacce ibride sottolinea che tali minacce combinano mezzi militari e non militari, coperti e scoperti, incluse disinformazione, cyberattacchi, pressione economica, gruppi irregolari e forze regolari, con l'obiettivo di sfumare il confine tra guerra e pace e seminare dubbio nelle popolazioni bersaglio.

La centralità del dominio cognitivo va letta anche alla luce dell'accelerazione tecnologica. Intelligenza artificiale generativa, *microtargeting*, *data analytics*, piattaforme *social*, *deepfake*, sistemi di raccomandazione algoritmica e auto-

mazione comunicativa modificano le condizioni della persuasione politica. La propaganda non è nuova; nuova è la scala, la velocità e la granularità con cui può essere prodotta e distribuita. In passato, influenzare una società richiedeva apparati mediatici relativamente visibili, canali istituzionali, reti di partito, organizzazioni ideologiche o strumenti di *broadcasting*. Oggi la manipolazione può avvenire in ambienti digitali frammentati, attraverso contenuti personalizzati, reti opache, account automatizzati e campagne che sfruttano vulnerabilità emotive preesistenti.

Questa evoluzione produce un effetto strategico preciso: riduce il costo dell'interferenza e aumenta il costo della difesa. Un attore ostile può produrre migliaia di contenuti falsi o distorsivi a costi relativamente bassi; il difensore democratico deve invece verificare, attribuire, comunicare, correggere e preservare al tempo stesso libertà di espressione, pluralismo e legittimità istituzionale. Il vantaggio dell'attaccante deriva dalla possibilità di agire in modo asimmetrico, rapido e plausibilmente negabile. Il difensore è vincolato da norme, procedure, *accountability* pubblica e necessità di non trasformare la risposta alla disinformazione in controllo politico dell'informazione.

La questione è particolarmente rilevante per le democrazie liberali. Nei regimi aperti, lo spazio cognitivo è pluralistico, contestato e istituzionalmente non centralizzato. Questo rappresenta una forza, perché consente adattamento, innovazione, critica pubblica e correzione degli errori. Allo stesso tempo, crea vulnerabilità, perché l'apertura del dibattito pubblico può essere sfruttata da attori esterni per amplificare fratture sociali, polarizzazione, sfiducia verso le élite, delegittimazione dei media e sospetto verso la competenza scientifica. La resilienza democratica non può quindi essere confusa con la chiusura dello spazio informativo. Essa dipende piuttosto dalla qualità delle istituzioni, dall'alfabetizzazione mediatica, dalla trasparenza delle piattaforme, dalla credibilità della comunicazione pubblica e dalla capacità dello Stato di riconoscere tempestivamente campagne ostili senza securitizzare ogni forma di dissenso.

L'Unione europea ha collocato questa sfida dentro una più ampia agenda di sicurezza e resilienza. La *Strategic Compass*, approvata nel 2022, definisce un piano d'azione per rafforzare la politica di sicurezza e difesa dell'UE entro il 2030 e organizza l'azione europea attorno ai pilastri *act, invest, partner* e *secure*. Nel quadro delle minacce ibride, l'UE include manipolazione dell'informazione, cyberattacchi, *lawfare*, coercizione economica e strumentalizzazione

dei migranti. Questa impostazione segnala che la sicurezza europea non riguarda più soltanto la gestione delle crisi esterne, ma la protezione della capacità interna di decidere, reagire e mantenere coesione politica.

Il passaggio dalla potenza come possesso alla potenza come orchestrazione è decisivo. La competizione contemporanea premia gli attori capaci di integrare strumenti diversi dentro campagne prolungate. La forza militare deve essere coordinata con la diplomazia, l'intelligence con la comunicazione strategica, la politica industriale con la sicurezza tecnologica, la protezione delle infrastrutture critiche con la resilienza sociale. Gli Stati Uniti, nella propria *Strategy for Operations in the Information Environment* del 2023, collegano le operazioni nell'ambiente informativo a deterrenza integrata, *campaigning* e costruzione di vantaggi duraturi; il documento sottolinea che l'uso dell'informazione, inclusa la segnalazione strategica, è rilevante per dissuadere i competitori dal valutare l'aggressione come più vantaggiosa della moderazione.

Questa logica è profondamente coerente con il concetto di *integrated deterrence*. La deterrenza non si basa più soltanto sulla minaccia di ritorsione militare, ma sulla capacità di rendere prevedibilmente costosi una pluralità di comportamenti ostili. Essa richiede credibilità, coordinamento inter-agenzia, interoperabilità con gli alleati, rapidità di attribuzione e comunicazione pubblica efficace. Nel dominio cognitivo, deterrere significa anche impedire all'avversario di ottenere vantaggi dalla confusione. Significa mostrare che le società democratiche non sono facilmente paralizzabili da campagne di influenza, che le alleanze non si frantumano sotto pressione narrativa, che la fiducia istituzionale può reggere alla manipolazione.

La potenza cognitiva non coincide però con la propaganda difensiva. Questo è un punto politicamente delicato. Se le democrazie rispondessero alla manipolazione esterna adottando strumenti opachi di manipolazione interna, perderebbero una parte della propria legittimità. La superiorità cognitiva in un contesto democratico non può essere intesa come controllo delle menti o uniformità del discorso pubblico. Deve essere intesa come capacità collettiva di mantenere orientamento, giudizio critico e decisione razionale in condizioni di pressione informativa. Per un regime democratico, il vantaggio cognitivo non nasce dall'eliminazione del conflitto interpretativo, ma dalla possibilità di gestirlo senza trasformarlo in disgregazione istituzionale.

Questo implica una distinzione importante tra influenza, persuasione e manipo-

lazione. Ogni ordine politico produce narrazioni, simboli e interpretazioni della realtà. Ogni politica estera richiede comunicazione strategica. Ogni alleanza deve spiegare ai propri cittadini perché determinate scelte sono necessarie. La manipolazione cognitiva, tuttavia, interviene quando l'obiettivo non è argomentare ma degradare la capacità autonoma di giudizio; quando l'informazione viene distorta intenzionalmente per produrre reazioni emotive, sfiducia sistemica o comportamenti funzionali agli interessi di un attore ostile. La linea non è sempre semplice da tracciare, ma è essenziale per preservare la distinzione tra competizione politica legittima e interferenza malevola.

La dimensione cognitiva ridefinisce anche il concetto di vulnerabilità. Nella sicurezza tradizionale, una vulnerabilità è spesso associata a un asset fisico: una base, una rete elettrica, una rotta marittima, un'infrastruttura digitale, un sistema d'arma. Nel quadro cognitivo, una vulnerabilità può essere una frattura sociale irrisolta, una minoranza percepita come esclusa, una sfiducia storica verso lo Stato, una memoria traumatica, una dipendenza informativa da piattaforme esterne, una bassa alfabetizzazione digitale, una polarizzazione identitaria. L'avversario non crea necessariamente queste vulnerabilità; spesso le individua, le amplifica e le connette a obiettivi strategici.

Per questa ragione, la resilienza cognitiva è inseparabile dalla qualità della democrazia. Una società con istituzioni credibili, media pluralisti ma responsabili, scuola capace di formare competenze critiche, amministrazioni trasparenti e leadership politiche affidabili è meno permeabile alla manipolazione ostile. Al contrario, una società già attraversata da sfiducia, precarietà, disuguaglianza e disorientamento informativo offre un terreno più favorevole alle campagne di influenza. La sicurezza cognitiva non può essere prodotta soltanto dai ministeri della Difesa o dagli apparati di intelligence. Richiede politiche educative, sociali, tecnologiche e regolatorie. Richiede una postura *whole-of-society*, nella quale sicurezza nazionale e coesione democratica siano pensate insieme.

La competizione cognitiva si lega inoltre alla trasformazione della sovranità. Nell'ordine westfaliano, la sovranità era associata al controllo del territorio e al monopolio della forza legittima. Nell'ordine digitale, uno Stato può conservare formalmente i propri confini e perdere comunque parte della propria autonomia decisionale se il suo spazio informativo è sistematicamente penetrato, se le sue infrastrutture cognitive dipendono da piattaforme esterne, se il dibattito pubblico è manipolabile da attori stranieri, se le sue élite politiche reagiscono più agli

shock narrativi che a valutazioni strategiche. La sovranità cognitiva non significa autarchia informativa; significa capacità di preservare autonomia di giudizio in un ambiente aperto e interdipendente.

Questa trasformazione riguarda anche la competizione tra modelli politici. Le potenze autoritarie tendono a considerare lo spazio informativo come un'estensione della sicurezza del regime. La gestione delle percezioni interne ed esterne diventa parte integrante della sopravvivenza politica. Le democrazie, invece, si muovono in una tensione più complessa: devono difendere lo spazio pubblico senza chiuderlo, contrastare interferenze ostili senza compromettere libertà civili, aumentare la capacità di risposta senza centralizzare eccessivamente il controllo dell'informazione. La competizione tra modelli non si gioca quindi soltanto sull'efficienza economica o sulla capacità militare, ma sulla capacità di produrre fiducia, adattamento e legittimità sotto stress.

In questa prospettiva, il dominio cognitivo diventa il luogo in cui si decide la sostenibilità politica della potenza. Una grande potenza può disporre di capacità militari avanzate, ma fallire nel mantenere consenso interno o credibilità esterna. Può vincere una battaglia informativa di breve periodo e perdere reputazione strategica nel lungo periodo. Può produrre deterrenza attraverso la minaccia, ma indebolirla se i suoi segnali vengono percepiti come incoerenti. La potenza contemporanea richiede continuità tra risorse, narrazioni e comportamenti. La credibilità non è un attributo retorico; è un moltiplicatore strategico.

Questo aspetto è evidente nelle alleanze. La NATO e l'UE non sono soltanto aggregati di capacità materiali. Sono comunità politico-strategiche che dipendono dalla percezione condivisa della minaccia, dalla fiducia reciproca, dalla coerenza delle decisioni e dalla capacità di comunicare ai cittadini il senso degli impegni comuni. Un avversario che riesca a indebolire la fiducia tra alleati, a far apparire i costi della solidarietà come insostenibili, a presentare la deterrenza come escalation o l'assistenza militare come inutile spreco di risorse, può ottenere risultati strategici senza sconfiggere militarmente l'alleanza. La disgregazione cognitiva può precedere quella politica.

Il potere nelle transizioni è quindi anche potere di temporalità. Gli attori strategici competono per imporre il ritmo degli eventi. Chi accelera può costringere l'avversario a reagire senza deliberare. Chi rallenta può logorare la volontà politica dell'altro. Chi moltiplica crisi simultanee può saturare la capacità decisionale di governi e opinioni pubbliche. Nel dominio cognitivo, il tempo è una risorsa es-

senziale: la velocità della disinformazione tende a superare quella della verifica; l'emozione precede spesso la valutazione; la semplificazione narrativa si diffonde più rapidamente dell'analisi complessa. La competizione strategica diventa allora anche competizione sul tempo dell'attenzione.

La centralità dell'attenzione è uno degli elementi più sottovalutati della potenza contemporanea. In un ambiente informativo saturo, il problema non è soltanto accedere all'informazione, ma stabilire ciò che merita attenzione. La scarsità non riguarda più il contenuto, ma la capacità cognitiva di selezionarlo e interpretarlo. Gli attori strategici competono per definire priorità, frame, crisi dominanti e categorie interpretative. In questo senso, *agenda-setting*, *framing* e *narrative power* non sono strumenti secondari: sono forme di potere che orientano il modo in cui una società percepisce ciò che è urgente, ciò che è legittimo, ciò che è minaccioso e ciò che è possibile.

Ne deriva una trasformazione della stessa nozione di *battlefield*. Il campo di battaglia resta terrestre, marittimo, aereo, spaziale e cibernetico, ma si estende anche alla mente dei decisori e delle popolazioni. Questo non significa militarizzare ogni aspetto della vita sociale. Significa riconoscere che le società sono parte del teatro strategico quando diventano bersaglio di campagne volte a modificarne orientamenti, fiducia e comportamenti. La sfida teorica consiste nel conciliare questa consapevolezza con la tutela dello spazio civile. La sicurezza cognitiva deve evitare due errori opposti: ignorare la dimensione ostile della manipolazione o trasformare ogni conflitto discorsivo in minaccia alla sicurezza nazionale.

L'approccio più solido consiste nel pensare il dominio cognitivo come infrastruttura democratica. Così come le infrastrutture energetiche, digitali e logistiche richiedono protezione, manutenzione e ridondanza, anche l'infrastruttura cognitiva di una società richiede investimenti. Essa comprende istruzione, ricerca, media, comunicazione pubblica, archivi, cultura istituzionale, competenze digitali e capacità analitiche. La resilienza non nasce da una risposta emergenziale a singole campagne ostili, ma da un ecosistema capace di assorbire shock informativi senza perdere orientamento strategico.

Per gli Stati europei, questa è una sfida particolarmente urgente. L'Europa è esposta a pressioni ibride provenienti dal vicinato orientale e meridionale, alla competizione tecnologica tra Stati Uniti e Cina, alla dipendenza da piattaforme digitali extraeuropee, alla vulnerabilità delle infrastrutture critiche e alla frammen-

tazione dei dibattiti pubblici nazionali. La sua risposta non può limitarsi alla regolazione delle piattaforme o al contrasto tecnico alla disinformazione. Deve includere una riflessione più ampia sulla capacità europea di produrre conoscenza strategica, comunicazione credibile e cultura della sicurezza democratica.

La potenza europea, in particolare, è storicamente associata a strumenti normativi, economici e regolatori. Questo resta un vantaggio, ma non basta se non viene integrato con capacità operative, tecnologiche e cognitive. La regolazione può creare standard, ma deve essere accompagnata da capacità di enforcement. La comunicazione istituzionale può denunciare la manipolazione, ma deve essere tempestiva e comprensibile. La resilienza democratica può essere proclamata, ma richiede politiche educative e sociali. La transizione della potenza europea dipende dalla capacità di trasformare il proprio modello regolatorio in una postura strategica più integrata.

Le trasformazioni della potenza nella competizione strategica contemporanea non possono essere comprese attraverso una semplice opposizione tra *hard power* e *soft power*. Il potere opera oggi come combinazione di coercizione, attrazione, interdipendenza, controllo tecnologico, capacità narrativa e resilienza cognitiva. La centralità del dominio cognitivo non sostituisce le dimensioni materiali della potenza, ma le attraversa e ne condiziona l'efficacia. La forza militare ha bisogno di credibilità politica. La deterrenza ha bisogno di percezione. L'autonomia strategica ha bisogno di capacità decisionale. La sicurezza ha bisogno di fiducia.

"Power in transitions" significa allora comprendere che la potenza si esercita dentro transizioni multiple: geopolitiche, tecnologiche, industriali, informative e sociali. In ciascuna di queste transizioni, il dominio cognitivo rappresenta lo spazio in cui si decide se una società riesce a interpretare il cambiamento, sostenere decisioni difficili, riconoscere minacce reali e resistere alla manipolazione. La competizione strategica del XXI secolo non sarà vinta soltanto da chi dispone di più risorse, ma da chi saprà trasformarle in orientamento, coerenza e capacità collettiva di decisione. In questo senso, la cognizione non è un livello secondario della potenza. È la condizione attraverso cui la potenza diventa politicamente efficace.

2

La guerra cognitiva e la costruzione della resilienza dei militari

A cura di Antonio Venci

© 2026 Antonio Venci. Tutti i diritti riservati.

Nota di Riserva dei Diritti e Licenza d'Uso

Proprietà Intellettuale: Antonio Venci – Tutti i diritti riservati.

La concessione dei diritti avviene a titolo di permuta a fronte della fornitura dei servizi da parte dell'Esercito Italiano, quali la disponibilità di spazi e sale conferenze attrezzati con i dispositivi correntemente utilizzati (arredi, microfoni, schermi digitali, collegamenti internet, ecc.), destinati alla presentazione dei lavori intellettuali del Centro Studi Esercito (CSE EPS). L'Autore concede al Centro Studi Esercito (CSE EPS), di cui è socio, e all'Esercito Italiano una licenza d'uso **non esclusiva e non trasferibile** relativa all'opera intitolata *La Guerra Cognitiva e la costruzione della resilienza dei militari*, limitatamente all'uso interno. È consentito il caricamento del testo sulla rete Intranet dell'Amministrazione, purché protetta da credenziali e non accessibile al pubblico esterno. L'Autore conserva la piena ed esclusiva titolarità di tutti i diritti di sfruttamento economico del-

l'opera nei confronti del pubblico e di terzi, restando libero di pubblicarla in qualsiasi forma, cartacea o digitale, anche tramite case editrici, senza alcuna limitazione. La presente licenza non conferisce al Centro Studi Esercito né all'Esercito Italiano alcun diritto di prelazione o di esclusiva editoriale.

2.1 Abstract

Cognitive Warfare (cogwar, ovvero guerra cognitiva) è uno strumento di egemonia che si inquadra nella strategia globale. In ambito militare, seguendo la dottrina NATO, si considererebbero gli effetti prodotti sulle opinioni, sulle emozioni e sui sentimenti in conseguenza delle operazioni condotte nei cinque domini canonici: terrestre, marittimo, aereo, cibernetico e spaziale. Per altro verso, in un quadro di «guerra ibrida» la *cogwar* è una forma di propaganda nella società bersaglio per degradarne la tenuta valoriale e renderla arrendevole o, più pragmaticamente orientarla, nel quadro di una più ampia manovra strategica con finalità egemoniche. Nonostante la caratterizzazione semantica l'avvicini alla strategia militare qui non si tratta di operazioni di guerra psicologica, che attengono invece al livello tattico, al massimo operativo. Viceversa, la guerra cognitiva è un fenomeno da gestire a livello politico, utilizzando strutture ad hoc.

La *cogwar* è di interesse dei militari perché l'azione di un singolo combattente, in un mondo interconnesso da internet, può assumere valore strategico nel campo della comunicazione (concetto di «caporale strategico»). Quindi, il personale militare a tutti i livelli gerarchici deve essere in grado di gestire le proprie emozioni e cognizioni (mentalizzazione) per mantenere in ogni circostanza un comportamento rispondente ai dettami dei codici etici della condizione militare e della missione ricevuta. La cultura militare opera a tale scopo.

Nel confronto politico-militare moderno, prima con la Guerra Fredda e ora tra autocrazie che abitano il «cuore della terra», l'Heartland e i Paesi democratici dell'Occidente, fenomeni d'influenza ci sono sempre stati e in questo documento si argomenta sulla propaganda dell'URSS verso l'Alleanza Atlantica e, segnatamente, in Italia, richiamandone gli effetti tuttora osservabili. Sembra allora che attraverso le generazioni si siano strutturate credenze, se non veri bias cognitivi, che condizionano ancora la percezione dell'Occidente non come ecume-

ne di civiltà e valori, ma quale portatrice di colpe ancestrali cui fare ammenda. Dunque, il concetto della guerra cognitiva chiama in causa processi psicologici che occorre esaminare per comprendere come pensiamo e quali influenze ci plasmino. Quest'orientamento è vieppiù urgente ora che la comunicazione è diventata digitale. In tale prospettiva vengono qui chiamati in causa numerosi pensatori del nostro tempo che con le loro intuizioni spiegano come e perché il nostro mondo fenomenico abbia assunto la forma che ha.

Si richiama poi il paradigma della Cultura organizzativa militare, elaborato in un precedente documento dall'Autore, per dimostrare l'assunto secondo cui la resilienza dei militari dell'Esercito di fronte al fenomeno delle influenze malevoli della *cogwar* si neutralizzi di fronte alla loro cultura organizzativa, ma solo se ben assimilata e quotidianamente confermata. Nella circostanza si considerano anche le possibili vulnerabilità derivanti dai condizionamenti imposti da fattori contingenti alla condizione militare, come le influenze all'imborghesimento insite nell'antimilitarismo militante.

Un riferimento alla Psicologia del profondo, richiamando il concetto di archetipo dell'inconscio collettivo (C.G. Jung), evidenzia le connessioni tra propaganda polarizzazione delle masse.

Completa il lavoro un riepilogo dei moderni strumenti della comunicazione di propaganda quali post-verità, narrazioni, spin doctor, piattaforme *social*, *troll*, *bot*, *meme*, algoritmi, uso nella propaganda degli archetipi dell'inconscio collettivo, ponendo in evidenza come la conoscenza di queste strutture assieme alle capacità critiche che una buona cultura può fornire rendono gli individui meno influenzabili e la società più resiliente.

3

La guerra cognitiva nell'era digitale Basi neurobiologiche della vulnerabilità cognitiva e implicazioni per la sicurezza

A cura di Alessia Dorigoni

3.1 Abstract

La guerra cognitiva contemporanea si dispiega al di sotto della soglia della violenza armata convenzionale, avvalendosi di strumenti che agiscono sulla percezione, sul giudizio e sulla fiducia prima ancora che sulle infrastrutture fisiche. A differenza delle tradizionali operazioni psicologiche, che mirano a cambiare ciò che le persone pensano, la guerra cognitiva mira ad alterare come le persone pensano, intervenendo sull'architettura stessa dell'elaborazione cognitiva. Il presente lavoro analizza le basi neurobiologiche di questa vulnerabilità attraverso una revisione della letteratura su neuroscienze, psicologia cogniti-

va e studi strategici. Si identificano cinque vettori principali di influenza cognitiva: (1) informazionale-contenutistico, mediato dall'effetto di verità illusoria e dalla persistenza della disinformazione (CIEM); (2) mnestico, attraverso la generazione di false memorie neurologicamente indistinguibili da quelle vere; (3) digitale-algoritmico, attraverso l'amplificazione del sistema di ricompensa dopaminergico e la polarizzazione indotta dalle architetture di *engagement*; (4) attentivo-cognitivo, attraverso il sovraccarico informativo e lo sfruttamento dei bias strutturali del sistema attentivo umano; (5) formale-trasmissivo, attraverso la selezione del formato e del canale di trasmissione come strumenti di influenza emotiva autonomi dal contenuto. La comprensione integrata di questi meccanismi è indispensabile per sviluppare strategie di resilienza cognitiva adeguate alle sfide della sicurezza contemporanea.

Parole chiave: guerra cognitiva, neuroscienze cognitive, disinformazione, effetto di verità illusoria, false memorie, formato dell'informazione, resilienza cognitiva, guerra ibrida

3.2 Introduzione

Nell'attuale panorama geopolitico, il confine tra guerra e pace non è più netto. Russo (2026) ha mostrato come i conflitti contemporanei si dispieghino deliberatamente al di sotto della soglia della violenza armata convenzionale, operando attraverso l'influenza, la disruption e l'ambiguità: ciò che Hasselbladh chiama '*shadow of war*', una condizione in cui i segnali sostituiscono gli eventi verificabili e l'incertezza diventa principio organizzativo delle istituzioni. In questo scenario, la domanda 'siamo in guerra?' non è retorica ma strutturalmente irrisolvibile, e la plausibilità prende il posto della verità come criterio orientativo dell'azione. Questa opacità deliberata non è un'anomalia: è la caratteristica funzionale della guerra cognitiva. Come sottolinea Hoffman (2025), il campo di questo tipo di conflitto è ancora privo di una definizione condivisa, densamente popolato da concetti sovrapposti come operazioni psicologiche, guerra dell'informazione e operazioni di influenza, e questa stessa vaghezza costituisce un vantaggio operativo per chi agisce nell'ombra. L'analisi bibliometrica di Prébot (2026) su 187 fonti dedicate alla guerra cognitiva rivela che il 44,9% delle pubblicazioni si concentra sull'influenza informazionale, il 37,4% su questioni definitive generali, e le neuroscienze cognitive vengono identificate come un 'angolo

cieco' del corpus: presenti come fondamento teorico, ma raramente integrate nelle dottrine operative. Il 46% delle pubblicazioni analizzate è stato prodotto nel solo 2025, segnale di un'accelerazione senza precedenti che rende urgente colmare proprio questo vuoto. L'obiettivo del presente lavoro è analizzare le basi neurobiologiche della vulnerabilità cognitiva nell'era della guerra cognitiva digitale, esaminando i molteplici vettori attraverso cui il cervello umano può essere influenzato strategicamente: dalla disinformazione e dalla generazione di false memorie, all'amplificazione algoritmica dei circuiti di ricompensa, fino alla manipolazione del formato e del canale di trasmissione come strumenti di influenza emotiva autonomi rispetto al contenuto informativo.

3.3 La guerra cognitiva: definizione, perimetro e specificità

La distinzione concettuale tra guerra psicologica e guerra cognitiva è più di un esercizio tassonomico: è una questione operativa. Russo e Peteva (2025) la formulano con precisione: la guerra psicologica mira a cambiare ciò che le persone pensano, la guerra cognitiva mira a cambiare come le persone pensano. La prima agisce sui contenuti delle credenze; la seconda sull'architettura sottostante attraverso cui qualsiasi informazione viene elaborata, valutata e integrata. Dal panorama definitorio analizzato dagli autori emergono quattro convergenze fondamentali: la cognizione come bersaglio primario; l'azione sub-soglia che attraversa il confine pace-guerra senza mai esplicitarlo; un'intenzionalità strategica bidirezionale, che include sia la degradazione cognitiva del nemico sia il potenziamento cognitivo delle proprie forze; e un'architettura multi-vettoriale che integra componenti tecnologiche, neurobiologiche e psicologiche. Hoffman (2025) traduce questa cornice analitica in termini operativi, definendo la guerra cognitiva come 'l'applicazione dell'informazione e delle scienze cognitive per migliorare o degradare il processo decisionale di leader politici e militari e della società civile'. La Cina ha declinato questa logica nelle '*Cognitive Domain Operations*', considerate un campo di battaglia complementare a quelli fisici, con l'obiettivo di 'colpire, indebolire e smantellare la volontà di combattere del nemico'; la Russia impiega invece il 'controllo riflessivo', finalizzato a trasmettere alla controparte basi decisionali false che la inducano a prendere decisioni a sé sfavorevoli, manipolando i frame emotivi, psicologici e culturali entro cui le decisioni vengono prese. Ciò che rende questa competizione par-

ticolarmente insidiosa è la sua invisibilità: come nota van der Linden e Cohen (2025), i meccanismi attraverso cui il cervello elabora e valuta le informazioni non sono progettati per resistere a manipolazioni sistematiche e scalabili. La neuroscienza della disinformazione, proseguono gli autori, è dunque non solo una disciplina accademica, ma uno strumento necessario per comprendere cosa rende il cervello vulnerabile, come la disinformazione si propaga e come può essere contrastata. Prébot (2026) segnala però che questa integrazione rimane in larga misura un'aspirazione: la frammentazione terminologica del campo costituisce essa stessa una vulnerabilità strategica, poiché non si può difendere ciò che non si riesce a definire.

3.4 Tassonomia dell'informazione falsa e diffusione nei media sociali

Se la guerra cognitiva si avvale dell'informazione come vettore di attacco, una precisione concettuale sul tipo di informazione impiegata è necessaria prima di esaminare i meccanismi neurali che la rendono efficace. Hussain e Soomro (2023) offrono la tripartizione fondamentale: la misinformazione è informazione falsa diffusa senza consapevolezza della propria falsità; la disinformazione è informazione deliberatamente falsa diffusa con intento di ingannare; la malinformazione è informazione vera utilizzata per causare danno. La distinzione è fondata sul criterio dell'intenzionalità, il che ha conseguenze dirette sul piano operativo: la disinformazione istituzionale, coordinata e intenzionale, è qualitativamente diversa dalla propagazione spontanea di notizie false, e richiede risorse, organizzazione e tempo. Questa tripartizione, tuttavia, non cattura la piena complessità del fenomeno. Santos-D'Amorim e Miranda (2021) identificano sedici tipologie di contenuti fuorvianti: dalla propaganda alle teorie del complotto, dal clickbait alla satira, dai siti web impostori alle camere d'eco e alle bolle di filtraggio. La diversificazione delle forme non è casuale: risposte appropriate a una tipologia possono risultare inefficaci o controproducenti per un'altra, il che rende l'arsenale informativo della guerra cognitiva intrinsecamente adattivo. Ma perché questa varietà di forme è così efficace? La risposta, come mostra Allen (2020) analizzando l'infodemia da COVID-19, risiede in vulnerabilità psicologiche e neurobiologiche preesistenti: il bias di conferma porta le persone ad accettare preferenzialmente le informazioni in linea con le credenze preesisten-

ti; la tendenza evolutiva a cercare cause 'grandi' per eventi rilevanti rende fertile il terreno per le teorie del complotto; l'attenzione evolutivamente programmata verso le notizie negative o minacciose favorisce la propagazione virale dei contenuti allarmistici. Gli algoritmi dei social media, conclude Allen, non creano queste vulnerabilità ma le amplificano sistematicamente, costruendo bolle informative sempre più ristrette ed estreme. Si capisce così come la tassonomia dell'informazione distorta non sia un esercizio classificatorio, ma la mappa delle linee di attacco disponibili alla guerra cognitiva.

3.5 Il cervello di fronte alla disinformazione: circuiti della ricompensa ed effetto di verità illusoria

Comprendere perché la disinformazione funziona richiede di guardare dentro il cervello che la riceve. Grignolio, Morelli e Tamietto (2022) documentano come le notizie false attivino il sistema mesolimbico della ricompensa, in particolare il nucleo accumbens e le vie dopaminergiche, grazie alla loro salienza emotiva e alla novità dei contenuti. L'amigdala elabora gli stimoli minacciosi o sorprendenti che connotano tipicamente la disinformazione, mentre la corteccia prefrontale laterale, associata alla valutazione critica, risulta meno attiva durante i giudizi distorti. Una breve esposizione di cinque minuti a contenuti falsi è sufficiente a modificare significativamente gli atteggiamenti dei partecipanti: la vulnerabilità non è dunque un esito di un'esposizione prolungata, ma una caratteristica della prima risposta cerebrale. Questo dato acquista piena portata se considerato insieme alle evidenze raccolte da Cohen e Decety (2026) sul comportamento di condivisione sui social media. Attraverso studi fMRI, gli autori mostrano che l'attivazione del sistema di ricompensa, striato ventrale e corteccia prefrontale ventromediale, si verifica sia quando si ricevono 'like' sia quando si condividono contenuti. La distinzione cruciale è tra 'wanting' e 'liking': il sistema dopaminergico motiva la condivisione anche in assenza di un'esperienza piacevole consapevole, secondo il meccanismo dell'apprendimento per rinforzo. Ne consegue che i contenuti che stimolano l'indignazione morale o l'identità di gruppo vengono condivisi più dei contenuti accurati non perché piacciono di più, ma perché attivano la spinta a diffonderli. Studi su Twitter citati dagli autori confermano che il *feedback* positivo alle espressioni di indignazione rinforza la tendenza a produrne ulteriori, creando un circuito che premia la radicalizzazione emotiva

indipendentemente dalla verità del contenuto. Se l'attivazione del sistema di ricompensa spiega l'attrattiva iniziale e la diffusione della disinformazione, un secondo meccanismo ne garantisce la persistenza nel tempo: l'effetto di verità illusoria. Van der Linden e Cohen (2025) identificano la corteccia peririnale (PRC) del lobo temporale mediale come il substrato neurobiologico principale di questo fenomeno: la sua funzione critica nella memoria di riconoscimento e nei giudizi di familiarità implica che la semplice ripetizione di un'affermazione, indipendentemente dalla sua veridicità, ne aumenti la credibilità percepita. Studi fMRI citati dagli autori mostrano che l'attività della PRC aumenta linearmente con la verità percepita per le affermazioni ripetute. Cohen e Decety (2026) documentano che anche una singola esposizione a notizie false su *Facebook* è sufficiente a incrementare le percezioni di accuratezza, con effetti persistenti a distanza di una settimana, anche per storie contraddette dai *fact-checker*. La conseguenza logica di questi meccanismi è confermata dallo studio EEG di Arisoy, Mandal e Saxena (2022): il cervello umano non presenta differenze statisticamente significative nell'elaborazione neurale di notizie vere rispetto a quelle false. Su 19 partecipanti, l'accuratezza di identificazione è risultata prossima al caso (53,09%); nemmeno algoritmi di *machine learning* addestrati sui dati EEG hanno superato questa soglia (F-measure tra 47 e 61%). La vulnerabilità alla disinformazione non è un difetto individuale correggibile con la sola consapevolezza: è una caratteristica strutturale del cervello umano.

3.6 Le basi neurali dell'influenza persistente: CIEM e memoria falsa

Se il cervello è strutturalmente incapace di distinguere il vero dal falso, sorge una domanda ancora più urgente: cosa succede quando si tenta di correggere l'informazione falsa già acquisita? La risposta di Ecker, Swire e Lewandowsky (2014) è scomoda: le semplici rettifiche non funzionano. Il fenomeno del *continued influence effect of misinformation* (CIEM) descrive la persistenza dell'influenza di un'informazione falsa sul ragionamento e sul comportamento anche dopo la sua esplicita smentita. La smentita senza narrazione alternativa lascia un vuoto cognitivo che il sistema tende a colmare con l'informazione originale. Peggio ancora, il *familiarity backfire effect* mostra che la ripetizione del contenuto falso durante la rettifica può aumentarne paradossalmente la credibilità per

effetto della familiarizzazione; il *worldview backfire effect* mostra che le correzioni che contraddicono le credenze identitarie di una persona possono rafforzarle anziché indebolirle. Solo i testi di refutazione strutturati, che esplicitano la tecnica di manipolazione usata e offrono una narrazione alternativa coerente, si rivelano efficaci. Le ragioni neurobiologiche di questo pattern sono state chiarite da Gordon et al. (2017) attraverso uno studio fMRI su 26 partecipanti: la regione precuneo/corteccia cingolata posteriore (PrC/PCC) mostra una minore attivazione durante la codifica delle rettifiche rispetto alle affermazioni non rettificate, suggerendo che le correzioni interrompano i processi di costruzione della coerenza narrativa nel cervello. Le rettifiche risultano strutturalmente meno integrate nella rappresentazione mentale complessiva dell'evento, mentre l'attività del giro frontale mediale (MFG) predice la risposta accurata, in linea con il ruolo delle aree prefrontali nel recupero strategico delle informazioni. Il cervello, in altri termini, aggiorna i propri modelli del mondo in modo conservativo, resistendo ai cambiamenti che richiedono la revisione di narrazioni già integrate. La ragione profonda di questa resistenza risiede nel processo stesso di formazione della memoria. Lentoer (2023) mostra che tutte e tre le fasi della memoria, codifica, consolidamento e recupero, sono vulnerabili all'effetto della disinformazione. L'ippocampo è coinvolto nel consolidamento, mentre la corteccia prefrontale dorso- e anterolaterale e la vmPFC partecipano alla formazione di false memorie durante la codifica. La *Fuzzy Trace Theory*, discussa da Lentoer, distingue tra tracce verbatim (dettagliate e accurate) e tracce di *gist* (semplificate e schematiche): quando le prime decadono nel tempo, le seconde diventano il substrato per le false memorie. La ricerca di Elizabeth Loftus, richiamata dallo stesso autore, ha mostrato che informazioni fuorvianti presentate dopo un evento possono letteralmente sovrascrivere la memoria originale, rendendola non recuperabile nella sua forma autentica. Queste dinamiche assumono un rilievo ancora maggiore nel dominio politico, dove le loro implicazioni sono state investigate da Coronel e Bucy (s.d.) attraverso i potenziali evento-correlati (ERP). Applicando il framework dei sistemi mnestici multipli, gli autori dimostrano che le false memorie su posizioni di candidati politici generano pattern cerebrali, N400 e LPC, indistinguibili da quelli delle vere memorie. Le 'false alarms' mostrano profili ERP simili agli '*hits*', accompagnati da alti livelli di confidenza soggettiva. Ne consegue che la disinformazione politica, una volta consolidata in falsa memoria, è strutturalmente più difficile da correggere di

qualsiasi altro tipo di errore cognitivo: il soggetto non ha accesso alla distinzione tra ciò che ha realmente vissuto e ciò che gli è stato fatto credere.

3.7 Meccanismi cognitivi della vulnerabilità: *bias*, cecità attenzionale e cognizione motivata

I fenomeni descritti nei capitoli precedenti, dall'effetto di verità illusoria alla formazione di false memorie, non sono isolati: sono radicati in una struttura più ampia di vulnerabilità cognitiva che opera stabilmente al di sotto della soglia della consapevolezza. Alexander, Macknik e Martinez-Conde (2022) ne tracciano i contorni attraverso il prisma della neuroscienza e della psicologia della magia. Il sistema attentivo umano è altamente selettivo e sopprime attivamente le informazioni non attese: la cecità attenzionale e la cecità al cambiamento mostrano come il cervello perda consistenti porzioni di informazioni visibili quando l'attenzione è diretta altrove. Il sovraccarico informativo, caratteristico degli ambienti digitali contemporanei, amplifica questi effetti, rendendo l'individuo più vulnerabile a contenuti costruiti per intercettare l'attenzione attraverso la salienza emotiva o la novità. Gli autori documentano inoltre che l'effetto di verità illusoria persiste per mesi e che la memoria è particolarmente malleabile nel momento del recupero. A questo limite attentivo si aggiunge un secondo fattore, altrettanto strutturale: la cognizione motivata. Van der Linden e Cohen (2025) mostrano come gli obiettivi, i valori e l'identità preesistenti modulino i processi cognitivi di base, portando a preferire, interpretare e ricordare le informazioni congruenti con le credenze preesistenti. Quando la disinformazione è altamente congruente con le credenze identitarie, le correzioni producono disagio cognitivo che predice il ricorso persistente all'informazione falsa come base per le inferenze. La segnalazione dopaminergica supporta l'elaborazione di informazioni confermate, mentre l'attivazione della corteccia cingolata anteriore nel rilevamento del conflitto cognitivo può precedere la soppressione dell'informazione discordante anziché la sua integrazione. È precisamente su queste vulnerabilità che agisce il design dei social media. Allen (2020) mostra come le piattaforme creino bolle di filtraggio che espongono gli utenti in modo progressivamente più selettivo a informazioni congruenti con le credenze preesistenti, amplificando la radicalizzazione delle posizioni e rendendo le democrazie più vulnerabili alle campagne di disinformazione sistematica. E Santos-D'Amorim e

Miranda (2021) chiariscono che si tratta di un effetto progettato, non emergente: le camere d'eco e le bolle di filtraggio possono essere deliberatamente costruite attraverso architetture algoritmiche che massimizzano il coinvolgimento a scapito della qualità informativa. La vulnerabilità cognitiva individuale diventa così una risorsa strategica sfruttabile su scala.

3.8 Amplificazione algoritmica e guerra cognitiva digitale

Se i capitoli precedenti hanno descritto le vulnerabilità neurobiologiche e cognitive del singolo individuo, questo capitolo mostra come tali vulnerabilità vengano trasformate in leva strategica attraverso l'architettura digitale. Il punto di partenza è la convergenza documentata da Cohen e Decety (2026) tra il meccanismo del 'wanting' dopaminergico e il design degli algoritmi di engagement: questi ultimi privilegiano sistematicamente i contenuti che evocano indignazione morale, sorpresa o identità di gruppo, non perché siano più accurati, ma perché generano più condivisioni. Ne emerge un circuito di retroazione: l'indignazione attiva il sistema di ricompensa, promuove la condivisione, guida la prioritizzazione algoritmica, che a sua volta rinforza la produzione di contenuti analoghi. La disinformazione emotivamente attivante non si diffonde nonostante le piattaforme: si diffonde grazie alla loro logica interna. Questa vulnerabilità sistemica non è passata inosservata agli attori della guerra cognitiva. Hoffman (2025) documenta come Cina e Russia abbiano sviluppato strategie sistematiche per sfruttare questi circuiti algoritmici. Il 'controllo riflessivo' russo mira a trasmettere alla controparte basi decisionali false che la inducano a scelte sfavorevoli, manipolando i frame emotivi entro cui quelle decisioni vengono prese, e l'ambiente digitale offre il canale di distribuzione ideale per farlo su scala. La strategia è resa ancora più efficace dal fatto che, come ha dimostrato Arisoy et al. (2022), il cervello non dispone di strumenti neurali per distinguere il falso dal vero: la suscettibilità alla disinformazione è una vulnerabilità sistemica, non individuale, e non può essere risolta attraverso la sola educazione critica del singolo utente. Grignolio et al. (2022) sintetizzano il risultato complessivo: la combinazione tra architetture algoritmiche ottimizzate per il coinvolgimento e la propensione evolutiva del cervello verso la novità e la salienza emotiva crea un ambiente informativo strutturalmente ostile alla verità fattuale e alla deliberazione democratica. La veloce amplificazione virale delle notizie false non è

un'anomalia del sistema: è una conseguenza neurobiologicamente prevedibile del suo funzionamento ordinario.

3.9 Il formato come dimensione strategica: non solo cosa, ma come

La letteratura esaminata finora si concentra su ciò che viene trasmesso e sui meccanismi con cui il cervello lo elabora. Rimane però sistematicamente sotto-splorata una dimensione ulteriore: il formato attraverso cui l'informazione viene trasmessa. McLuhan (1964) aveva formulato questa intuizione nella proposizione '*the medium is the message*': il mezzo di comunicazione non trasporta passivamente un contenuto, ma modifica la struttura cognitiva ed emotiva entro cui quel contenuto viene ricevuto, elaborato e ricordato. Applicata alla guerra cognitiva, questa prospettiva apre uno spazio d'azione che la letteratura neuroscientifico-strategica stenta ancora ad affrontare sistematicamente (Prébot, 2026): la selezione del formato non è una scelta stilistica, ma una decisione operativa con effetti neurobiologici misurabili. Un'evidenza empirica diretta di questo principio proviene dallo studio di Dorigoni e Bonini (2023), condotto nel contesto dell'infodemia da COVID-19. I ricercatori hanno esposto 161 partecipanti a cinque formati numericamente equivalenti dello stesso dato di mortalità: valore assoluto ('133.177 persone sono morte'), frequenza relativa ('uno ogni 445 abitanti è morto'), rapporto grezzo, percentuale ('0,23%') e probabilità ('0,0023'). Le risposte sono state misurate attraverso il questionario TRIRISK, che distingue tra componenti deliberativa, affettiva ed esperienziale del rischio percepito, la scala PANAS per l'affettività negativa, la conduttanza cutanea (EDA) come misura di arousal autonomico, e l'analisi delle espressioni facciali tramite OpenFace 2.2.0. I formati di frequenza producono significativamente maggiore percezione affettiva del rischio (ZAR: $\beta = .507$, $p = .017$) e maggiore affettività negativa (PANAS: β fino a 8.44, $p < .01$) rispetto ai formati di probabilità, nonostante la totale equivalenza matematica dei valori. Il formato X/Y produce il maggiore arousal fisiologico misurato dall'EDA. Il risultato più rilevante per la guerra cognitiva riguarda però la **numeracy**: la capacità individuale di elaborare informazioni numeriche modera l'effetto del formato solo sulla componente deliberativa del rischio, ma non sulle componenti affettiva ed esperienziale. Anche i partecipanti con alta capacità numerica sono ugualmente vulnerabili all'impatto emotivo del

formato di frequenza. L'effetto opera attraverso il Sistema 1, rapido, automatico, affettivo, indipendentemente dal livello di attivazione del Sistema 2, lento, analitico, deliberativo. Questo dato si raccorda direttamente con le evidenze descritte nei capitoli precedenti: le vulnerabilità emotive documentate da Grignolio et al. (2022) e Cohen e Decety (2026) non si limitano alla selezione dei contenuti, ma si estendono al formato in cui qualsiasi contenuto viene presentato. Un attore che voglia amplificare il senso di minaccia, ridurre la volontà di combattere di una popolazione o incrementare la percezione di vulnerabilità ha a disposizione uno strumento che non richiede la falsificazione dei dati: è sufficiente scegliere il formato di presentazione più emotivamente attivante. Questo meccanismo è perfettamente coerente con la logica del 'controllo riflessivo' descritto da Hoffman (2025): manipolare il frame, non i fatti. Altre tre dimensioni del formato meritano attenzione. Il formato audiovisivo sfrutta circuiti cerebrali evolutivamente più antichi rispetto al testo: l'area fusiforme facciale e le aree uditive superiori attribuiscono credibilità agli stimoli incarnati, volti, voci, movimenti, prima ancora che intervenga la valutazione critica prefrontale. Le tecnologie deepfake sfruttano esattamente questo substrato: un volto noto che pronuncia un contenuto falso è neurologicamente più convincente dello stesso testo scritto. Poiché Arisoy et al. (2022) hanno utilizzato esclusivamente stimoli testuali, rimane aperta la domanda empirica se il cervello riesca a distinguere la disinformazione multimodale con un'accuratezza anche solo lontanamente superiore al caso. Altrettanto rilevante è il *design* della piattaforma come tecnica di influenza che precede l'arrivo del contenuto: lo *scroll* infinito e le notifiche a rinforzo variabile, strutturalmente identiche al meccanismo delle slot machine nel mantenere attivo il sistema di '*wanting*' dopaminergico documentato da Cohen e Decety (2026), condizionano lo stato cognitivo del ricevente prima ancora che l'informazione arrivi. Un cervello stanco, in modalità automatica, con le risorse deliberative impoverite è strutturalmente più permeabile all'elaborazione affettiva non critica. Infine, il ritmo e la frammentazione dei contenuti brevi non lasciano il tempo necessario perché il Sistema 2 intervenga: l'effetto di verità illusoria documentato da van der Linden e Cohen (2025) si amplifica quando la ripetizione avviene attraverso formati che rendono strutturalmente impossibile la riflessione deliberativa. Ne consegue che la tassonomia della guerra cognitiva non può limitarsi alla distinzione tra misinformazione, disinformazione e malinformazione basata sull'intenzionalità (Hussain & Soomro, 2023; Santos-

D'Amorim & Miranda, 2021). Il formato e il canale di trasmissione costituiscono una quarta dimensione, con effetti neurobiologici misurabili sulla percezione del rischio, sull'arousal autonomico e sulla codifica mnestica, indipendenti dalla verità o falsità del contenuto veicolato.

3.10 Strategie di contrasto: *debunking*, *prebunking* e resilienza cognitiva

Prima ancora di chiedersi come contrastare la guerra cognitiva, è necessario affrontare una condizione preliminare: il pericolo deve essere percepito. Un intervento, per quanto efficace sul piano neurobiologico e comunicativo, non viene attivato se il rischio che intende fronteggiare è invisibile, negato o semplicemente non riconosciuto come tale. L'analogia con il fumo passivo è illuminante: i danni del fumo passivo erano reali da decenni prima che diventassero oggetto di consenso scientifico condiviso e regolamentazione pubblica; finché il rischio non fu percepito come concreto e misurabile, nessuna difesa fu attivata, né individuale né collettiva. La guerra cognitiva presenta una difficoltà analoga, aggravata da un elemento strutturale: essa è progettata per essere impercettibile. I conflitti sub-soglia operano nell'ambiguità deliberata, sostituendo la plausibilità alla verità verificabile; la *shadow of war* funziona proprio perché non è riconoscibile come guerra, e l'incertezza che genera è il suo principale strumento offensivo. A livello individuale, questa invisibilità è neurobiologicamente fondata: un individuo esposto a contenuti che hanno indotto false memorie, come documentato da Coronel e Bucy (s.d.), non ha accesso soggettivo alla distinzione tra la propria opinione autentica e quella indotta dall'esterno, e si percepisce come libero e autonomo nel proprio giudizio. La cognizione motivata descritta da van der Linden e Cohen (2025) opera anch'essa sotto la soglia della consapevolezza: il bias di conferma non produce disagio cognitivo, ma conforto; non avvisa l'individuo di essere manipolato, lo rassicura che sta pensando correttamente. Ne consegue che la costruzione di una percezione condivisa del rischio, a livello individuale, istituzionale e politico, è la precondizione epistemica di qualsiasi contromisura. Senza di essa, le strategie discusse nei paragrafi seguenti rimarranno strumenti disponibili ma non adottati, esattamente come le indicazioni sanitarie sul fumo passivo prima che il pericolo fosse socialmente riconosciuto. È questa la sfida più profonda che la guerra cognitiva

pone alle democrazie contemporanee: non solo difendersi da un attacco, ma riconoscere che l'attacco è in corso. La comprensione neuroscientifica della vulnerabilità cognitiva non ha solo valore descrittivo: indica con precisione dove e come intervenire. Il primo principio che emerge dalla letteratura è che il debunking reagisce troppo tardi. Ecker, Swire e Lewandowsky (2014) mostrano che le semplici rettifiche sono inefficaci perché lasciano un vuoto narrativo che il sistema cognitivo tende a colmare con l'informazione originale: la smentita senza narrazione alternativa ripropone il falso che intende eliminare. Solo i testi di refutazione strutturati, che esplicitano la tecnica di manipolazione e offrono una narrazione sostitutiva coerente, producono effetti duraturi. Questo dato trova conferma nelle evidenze di Cohen e Decety (2026): la semplice esposizione a etichette di **fact-checking** riduce solo marginalmente l'effetto di verità illusoria, mentre gli interventi che aumentano la motivazione all'accuratezza prima della lettura producono effetti più consistenti. La radice del problema è neurobiologica: Gordon et al. (2017) hanno mostrato che le correzioni interrompono la costruzione della coerenza narrativa nel cervello e risultano strutturalmente meno integrate nella rappresentazione mentale dell'evento rispetto all'informazione originale. Correggere è difficile non perché le persone siano irrazionali, ma perché il cervello aggiorna i modelli del mondo in modo conservativo. Se il **debunking** reagisce dopo il danno, il prebunking tenta di prevenirlo. Van der Linden e Cohen (2025) propongono l'inoculazione psicologica: esporre le persone a versioni indebolite delle tecniche di manipolazione, appelli alla paura, capro espiatorio, falsa attribuzione di autorità, polarizzazione artificiale, in un contesto controllato, sviluppa 'anticorpi cognitivi' efficaci quando le stesse tecniche vengono incontrate nella realtà. Studi in campo reale su **YouTube** hanno raggiunto centinaia di milioni di spettatori con riduzioni significative della suscettibilità alle tecniche testate. Sul piano neurobiologico, la corteccia prefrontale dorsolaterale e la rete di controllo frontoparietale sembrano mediare la resistenza alla persuasione che l'inoculazione rafforza. La tecnica del **neuroforecasting**, che utilizza l'attivazione cerebrale di campioni ridotti per predire le preferenze a livello di popolazione, rappresenta uno strumento promettente per ottimizzare questi interventi su larga scala. Tuttavia, intervenire solo sulla resilienza individuale è insufficiente se l'ambiente rimane strutturalmente ostile. Cohen e Decety (2026) propongono la regolamentazione degli algoritmi come intervento sistemico fondamentale: il **Digital Services Act** dell'Unione Europea,

con gli articoli 34-35 che impongono audit algoritmici per i rischi sistemici, viene indicato come modello regolatorio; la modifica della struttura di *feedback*, sostituendo *'like/dislike'* con valutazioni di affidabilità, può migliorare la qualità dei contenuti condivisi. È in questa prospettiva che Prébot (2026) identifica la *'sicurezza cognitiva'* (*cognitive security*) come obiettivo sistemico emergente: non più solo *fact-checking*, ma risposte strutturate alle minacce ibride. Russo e Peteva (2025) completano il quadro con il concetto di *'cognitive literacy'* come competenza strategica fondamentale per i leader: la capacità di riconoscere i meccanismi di manipolazione cognitiva, di comprendere come l'influenza operi negli ambienti organizzativi e informativi, e di mantenere coerenza e fiducia sotto pressione cognitiva. Difendersi dalla guerra cognitiva richiede, in sintesi, interventi a tutti e tre i livelli in cui essa opera: individuale (prebunking, media literacy), algoritmico (regolamentazione delle piattaforme) e culturale (sviluppo di una cognitive literacy diffusa).

3.11 Conclusioni

Il presente lavoro ha illustrato come la guerra cognitiva si avvalga sistematicamente dei meccanismi neurobiologici fondamentali del cervello umano per produrre effetti strategici al di sotto della soglia del conflitto armato. Il campo di azione non si limita alla disinformazione: comprende la manipolazione del sistema di ricompensa dopaminergico attraverso architetture algoritmiche di *engagement*, lo sfruttamento del sovraccarico attentivo, la selezione strategica del formato di trasmissione per massimizzare l'impatto emotivo, e la generazione di false memorie neurologicamente indistinguibili da quelle vere. Questi vettori convergono verso un obiettivo comune: non cambiare cosa le persone pensano, ma come le persone pensano, alterando l'architettura stessa della valutazione cognitiva. La convergenza tra queste vulnerabilità strutturali e le architetture digitali progettate per massimizzare il coinvolgimento crea un ambiente di elevata fragilità per le democrazie contemporanee. La domanda "siamo in guerra?" è diventata strutturalmente irrisolvibile: i conflitti contemporanei operano attraverso segnali piuttosto che eventi, attraverso l'ambiguità piuttosto che la dichiarazione, sfruttando la plausibilità come principio organizzativo in sostituzione della verità verificabile. L'assenza di chiarezza dottrinale sul concetto di guerra cognitiva, documentata da Russo e Peteva (2025), Hoffman (2025) e Prébot

(2026), non è solo un problema accademico, ma una vulnerabilità strategica: non si può difendere ciò che non si riesce a definire. Le neuroscienze offrono strumenti potenti tanto per comprendere le vulnerabilità quanto per sviluppare contromisure più efficaci. Van der Linden e Cohen (2025) indicano come obiettivi prioritari per la ricerca la comprensione dei correlati neurali dell'effetto di verità illusoria (PRC), della propagazione della disinformazione (circuiti di ricompensa e mentalizzazione) e degli interventi di inoculazione (dlPFC e rete frontoparietale). Arisoy et al. (2022) hanno dimostrato che la vulnerabilità alla disinformazione è una caratteristica dell'elaborazione neuronale umana, non un difetto individuale: questo implica che le strategie di contrasto efficaci devono agire sull'ambiente informativo e algoritmico, non solo sulla formazione individuale. Coronel e Bucy (s.d.) hanno mostrato che le false memorie politiche sono neurologicamente indistinguibili dalle memorie vere, il che rende la prevenzione strutturalmente superiore alla correzione post-hoc. La costruzione di una cultura della resilienza cognitiva è oggi un imperativo di sicurezza nazionale e democratica. Analogamente a quanto avvenuto con le campagne di salute pubblica contro il tabagismo, che non hanno reso il tabacco meno attraente, ma hanno aumentato la consapevolezza dei rischi e modificato le norme sociali, il contrasto alla guerra cognitiva richiede interventi su più livelli: educazione critica ai media e al formato dell'informazione, regolamentazione algoritmica basata su prove neuroscientifiche, sviluppo di 'vaccini cognitivi' attraverso il *prebunking*, e investimento in ricerca neuroscientifica applicata ai contesti operativi e strategici. Il cervello umano non è solo il bersaglio della guerra cognitiva: è anche il terreno in cui le contromisure devono essere progettate, testate e validate. Solo attraverso questa comprensione integrata, che unisce neuroscienze cognitive, psicologia, studi strategici e politiche della comunicazione, sarà possibile preservare le condizioni epistemiche minime necessarie per il funzionamento delle democrazie nel XXI secolo.

4

Neurotecnologie applicate

A cura di Giulio Chiarantoni

4.1 Nuove, vecchie tecnologie

Le Forze Armate si trovano oggi ad operare in scenari iper-complessi, caratterizzati da un sovraccarico informativo multidimensionale, in cui analisti d'intelligence, decisori politici e operatori sul campo devono processare flussi sterminati di dati in frazioni di secondo. E sebbene la maggior parte delle informazioni sia processata da *computer* sempre più potenti, alla fine la decisione spetta sempre all'essere umano, la cui evoluzione biologica ha dotato il cervello di limiti intrinseci e invalicabili nell'elaborazione parallela e ultrarapida degli stimoli, l'insorgenza di fatica mentale, *bias* cognitivi ed euristiche fallaci. In questa cornice, le neuroscienze e le neurotecnologie si rivelano per la loro natura intrinsecamente *dual-use*: i medesimi protocolli sviluppati per alleviare determinate patologie, infatti, possono essere specularmente traslati in ambito militare per l'*enhancement* cognitivo e fisico di soggetti sani. Le tecnologie usate in ambito di Ricerca si suddividono principalmente in due macro-categorie: tecniche di

neuroimaging, come l'Elettroencefalografia (EEG), la Risonanza Magnetica Funzionale (fMRI) e la Spettroscopia Visiva vicino all'Infrarosso (fNIRS), e le tecniche di neuromodulazione, come la Stimolazione transcranica a Corrente (tCS) e la Stimolazione Magnetica Transcranica (TMS). Queste ultime, in particolare, negli ultimi decenni stanno ricevendo una notevole risonanza in ambito accademico a causa dei risultati sperimentali, ma non c'è nulla di nuovo nel loro principio fisico il cui funzionamento è noto da tempo. L'uso dell'elettricità sul cranio, ad esempio, non deve sorprendere; basti pensare al tristemente noto elettroshock, o, andando ancora più indietro, all'uso che facevano gli Antichi Romani del pesce torpedine, i quali lo piazzavano sullo scalpo e ne sfruttavano le funzionalità bio-elettriche per curare il mal di testa. E l'invenzione della TMS, che ad oggi viene venduta come una tecnologia innovativa semplicemente perchè ci sono abbastanza risorse per riprodurre dispositivi in massa, in realtà risale agli anni '80, grazie ai lavori di Anthony Barker. In questo scenario, le scoperte fatte e le scoperte che si faranno possono rappresentare un bene comune se usate eticamente, ma anche un pericolo se sfruttate per un uso malevolo volto a modulare i processi cognitivi. In tal senso, le Forze Armate dovranno sempre più includere, nella valutazione e gestione dei rischi correlati alla dimensione cognitiva, la cosiddetta "*neurosecurity*". Ci si chiede, infatti, se le traiettorie di evoluzione di questi studi avanzati, che hanno permesso di sviluppare procedure e terapie per curare malattie e patologie, costituiscano nuove fonti di minaccia.

4.2 Funzionamento della tCS

La tCS (*transcranial Current Stimulation*), nota anche come tES (*transcranial Electrical Stimulation*), è una tecnica di neuromodulazione non invasiva basata sulla somministrazione controllata di correnti elettriche a bassissima intensità (tipicamente comprese tra 0,5 e 2,0 mA) mediante elettrodi posizionati sullo scalpo e opportunamente bagnati con soluzione salina. Assolutamente sicuro come dispositivo (la potenza erogata è centinaia di volte inferiore a quella che serve per iniziare a bruciare la popolazione di neuroni più superficiale), è presente sul mercato sotto forma di vari modelli, da quelli più rudimentali a quelli di ultima generazione, e a seconda della forma d'onda data si distingue in: - tDCS (*transcranial Direct Current Stimulation*), caratterizzata dall'erogazione di corrente continua. Si basa sul principio secondo il quale i neuroni, per poter-

si attivare, hanno bisogno di un certo potenziale d'azione. Tramite una piccola quantità di elettricità, di conseguenza, è possibile modulare la soglia di attivazione a proprio piacimento. A seconda del polo d'interesse che può essere "positivo" o "negativo" (come una pila), si è in grado di potenziare o de-potenziare il cervello, motivo per il quale in genere uno dei due è posto su un lobo neutro o sulla spalla più distante (cosa che in genere non si fa con le altre tecniche, tipo la tRNS), così da avere un unico effetto senza inificiare un'altra parte del cervello. I risultati sperimentali evidenziano quello che viene chiamato "*after effect*", ovvero una modifica funzionante non tanto durante la scarica vera e propria quanto durante le ore successive al trattamento. - tACS (*transcranial Alternating Current Stimulation*), caratterizzata dall'erogazione di corrente alternata definita. Essendo sprovvista di anodo e catodo, il suo obiettivo primario è la sincronizzazione forzata dei *network* neurali su una determinata frequenza di scarica per potenziarne la connettività funzionale, come se facesse fare stretching al cervello. Al contrario del modello a Corrente Continua, i risultati sperimentali indicano generalmente un effetto "*Online*", ovvero un maggior potenziamento delle facoltà cognitive durante la scarica, piuttosto che "*Offline*" (che corrisponderebbe al cosiddetto "*after effect*" della tDCS citato prima). - tRNS (*transcranial Random Noise Stimulation*), caratterizzata dall'erogazione di corrente alternata casuale. Può essere vista come una degenerazione della tACS (è utile lì dove non si conosce la frequenza con cui agisce la popolazione di neuroni scelta), ed immette un rumore di fondo controllato che, anziché disturbare, ottimizza il rapporto segnale-rumore all'interno dei circuiti neurali deboli o parzialmente attivati, accelerando i processi di plasticità del cervello. Inoltre, a queste si aggiunge una tecnica completamente diversa che prende il nome di "*closed-loop stimulation*". Questo approccio configura un ecosistema simbiotico che unisce sulla medesima cuffia sensori EEG e moduli di stimolazione elettrica. Attraverso algoritmi di intelligenza artificiale e *machine learning*, il sistema analizza in tempo reale i flussi bio-elettrici del soggetto; nel momento esatto in cui l'algoritmo rileva un'anomalia, un calo di performance o l'insorgenza di onde lente associate alla fatica mentale, l'IA attiva istantaneamente una stimolazione mirata per risonare o de-sincronizzare il *network* deficitario, personalizzando l'output in base allo stato cerebrale del millisecondo precedente. Gli effetti collaterali sono generalmente di natura transitoria e circoscritti all'area cutanea sottostante gli elettrodi. Essi includono sensazioni di prurito, pizzico-

re, lieve bruciore locale ed eritema cutaneo passeggero indotto dalla vasodilatazione periferica. In rari casi si registrano effetti sistemici lievi quali cefalee post-trattamento, nausea, vomito o stanchezza transitoria, che recedono spontaneamente entro pochi minuti dal termine della sessione di stimolazione. Sono da chiarire ancora gli effetti dell'uso a lungo termine.

4.3 Applicazioni militari della tCS

In ambito militare, l'interesse verso la tCS è guidato dalla necessità di ottimizzare le prestazioni psicofisiche del personale operativo senza ricorrere ad agenti chimici o farmacologici. L'applicazione di maggiore rilevanza strategica concerne la Target Acquisition e la vigilanza visiva in compiti d'*intelligence*. Gli analisti deputati allo screening prolungato di immagini satellitari, tracciati radar o flussi video da droni operano in condizioni di estrema saturazione sensoriale. Gli esperimenti pregressi condotti dall'*Air Force Research Laboratory* (AFRL) negli Stati Uniti hanno dimostrato che l'applicazione di un protocollo di tDCS anodica sulla corteccia parieto-frontale destra raddoppia l'accuratezza nell'identificazione di minacce mimetizzate o obiettivi strategici nascosti rispetto ai gruppi di controllo, mantenendo inalterata la performance anche dopo ore di attività ripetitiva. Un secondo asse di applicazione critica riguarda la resilienza alla privazione di sonno e la fatica operativa. Nelle missioni prolungate, il personale delle Forze Speciali o i piloti di velivoli a lungo raggio subiscono crolli drastici nei tempi di reazione e nella memoria di lavoro. Gli studi AFRL hanno accertato che una stimolazione anodica della corteccia prefrontale dorso-laterale (DLPFC) è in grado di neutralizzare i deficit cognitivi causati da oltre 30 ore di veglia forzata. Rispetto alle sostanze stimolanti tradizionali (come il modafinil o le anfetamine), la tCS offre il vantaggio monumentale di non alterare il profilo emotivo del soldato, non indurre tolleranza o dipendenza e azzerare i fenomeni di "*rebound*" neuropsicologico al termine dell'effetto. I risultati sperimentali, però, indicano spesso cambiamenti modesti delle performance, motivo per cui la "soluzione chimica" resta ancora una valida alternativa. Tuttavia, va considerato come questi apparecchi non solo abbiano un costo monetario, ma che necessitano di personale specializzato per piazzare gli elettrodi che non si devono spostare durante la stimolazione, motivo per il cui si sconsiglia di impiegare personale sul campo con questi dispositivi addosso funzionanti. In più, visto l'ambiente militare connotato

da determinate caratteristiche, è da considerare il rischio che qualcuno minimizzi o nasconda proprio del tutto gli effetti collaterali. In questo caso si evidenzia come, sotto il profilo della "*neurosecurity*", il rischio non derivi da eventuali attori ostili che vogliono usare la tCS per scopi nocivi, vista la necessità di una certa vicinanza al cranio per essere impiegata, quanto da un uso improprio del nostro stesso personale.

4.4 Funzionamento della TMS

La TMS (*Transcranial Magnetic Stimulation*) è un'altra tecnica di neuromodulazione non invasiva il cui funzionamento biofisico si fonda sulla legge dell'induzione elettromagnetica di Faraday. La strumentazione comprende un generatore di impulsi ad alta intensità collegato ad una bobina isolata (coil), comunemente sagomata a forma di otto per garantire una focalizzazione geometrica ottimale del campo. Quando un impulso elettrico ad altissimo voltaggio attraversa la bobina per una frazione di millisecondo, si è in grado di creare una temporanea lesione virtuale del cervello. I risultati sperimentali in ambito clinico collocano questo come uno degli strumenti più rivoluzionari ed efficaci della neuropsichiatria moderna, in particolare grazie alla sua capacità di indurre modificazioni plastiche durature nei circuiti cerebrali disfunzionali. Tra i risultati clinici più interessanti si evidenziano il trattamento della Depressione Maggiore Farmaco-Resistente, il trattamento del Disturbo Ossessivo-Compulsivo, delle Dipendenze, della Malattia di Alzheimer, del Dolore Cronico Neuropatico e la Riabilitazione Neurologica Post-Ictus. Tra gli effetti collaterali più comuni e di natura benigna si comprendono cefalee di tipo tensivo (provocate dalla contrazione involontaria dei muscoli pericranici e facciali stimolati dal campo magnetico), dolore o fastidio localizzato sullo scalpo e fastidio acustico indotto dal forte "click" metallico emesso dal coil ad ogni scarica. Tra i rischi più severi, sebbene estremamente rari in assenza di fattori predisponenti, si evidenzia l'induzione di crisi convulsive epilettiformi ed ictus. La presenza di frammenti metallici o impianti ferromagnetici intracranici, clip vascolari per aneurismi o pacemaker cardiaci costituisce una controindicazione assoluta al trattamento.

4.5 Applicazioni militari della TMS

A causa della mole fisica della strumentazione, dei requisiti di alimentazione elettrica e della necessità di un posizionamento millimetrico del coil assistito da sistemi di neuronavigazione stereotassica computerizzata, l'impiego della TMS in ambito Difesa trova allocazione esclusivamente nelle retrovie, nei centri di comando tattico e nelle strutture sanitarie militari, escludendone per il momento l'impiego diretto sulla linea del fronte. I destinatari principali di questa tecnologia possono essere operatori sottoposti a stress cognitivo cronico, quali i piloti di sistemi aeromobili a pilotaggio remoto (UAV) o gli analisti di *cyber-defense*, per non parlare dei pianificatori strategici. L'applicazione di protocolli facilitatori sulla corteccia prefrontale dorso-laterale ha mostrato, ad esempio, di amplificare la memoria di lavoro, ottimizzare i processi di controllo inibitorio e incrementare la flessibilità decisionale in contesti di forte pressione temporale. Un secondo pilastro applicativo riguarda la medicina riabilitativa e il recupero psicofisico accelerato delle truppe di rientro da contesti operativi ad alta intensità. Il personale presenta frequentemente quadri complessi di Disturbo Post-Traumatico da Stress (PTSD) o esiti di traumi cranici lievi causati dall'esposizione ad onde d'urto ed esplosioni. La TMS si è dimostrata uno strumento eccellente per ripristinare l'omeostasi corticale, disattivando i circuiti iper-funzionanti associati all'iperattività dell'amigdala e accelerando il recupero clinico del soldato per il suo reinserimento operativo. Come per la tCS, sotto il profilo della "*neuro-security*" il rischio deriva più che altro da un uso improprio del nostro stesso personale, specie visto gli effetti collaterali molto più intensi e rischiosi; tuttavia, l'abilità intrinseca della TMS di inibire temporaneamente specifiche aree cerebrali solleva inquietanti interrogativi bioetici e dottrinali. Tramite l'applicazione mirata di protocolli inibitori sulla corteccia prefrontale (deputata al controllo esecutivo e alla dissimulazione), infatti, si potrebbe teoricamente indurre uno stato di disinibizione cognitiva forzata. Un simile approccio potrebbe essere sfruttato da attori ostili su soggetti caduti in stato di cattura per facilitare l'estrazione di informazioni classificate o segrete, configurando una modalità di interrogatorio e tortura neurotecnologica subdola, efficace e quasi totalmente priva di tracce fisiche o biologiche visibili.

4.6 Funzionamento delle BCI

Tra le neurotecnologie moderne più di interesse, infine, rientrano anche le BCI (*Brain-Computer Interfaces*), le quali rappresentano lo zenit della convergenza tra neuroscienze computazionali, ingegneria biomedica ed intelligenza artificiale. Una BCI è un sistema di comunicazione diretto ed invasivo che connette il cervello a supporti di calcolo esterni tramite un chip posto su di esso. Il flusso di elaborazione si articola generalmente in quattro macro-fasi sequenziali: l'acquisizione dei segnali neurali, la pre-elaborazione e il filtraggio degli artefatti biologici (come i movimenti oculari o i battiti cardiaci), l'estrazione delle feature corticali tramite algoritmi avanzati di *Machine Learning* per decodificare l'intenzione del soggetto, ed infine la traduzione di tali *feature* in comandi esecutivi per un software o un attuatore robotico esterno. A livello popolare e commerciale Neuralink è sicuramente la più nota, ma in realtà *Blackrock Neurotechnologies* vanta già una più ampia validazione scientifica, con risultati che hanno permesso a pazienti tetraplegici di controllare bracci robotici complessi e ricevere feedback sensoriali tattili artificiali ricreati tramite micro-stimolazione intracorticale a circuito chiuso. L'approccio invasivo di queste tecnologie comporta tuttavia severi limiti fisiologici e rischi biologici intrinseci. Oltre al pericolo immediato di infezioni batteriche intracraniche (meningiti o encefaliti) indotte dalla violazione permanente della barriera cutanea e durale, sul lungo periodo il tessuto cerebrale reagisce alla presenza del corpo estraneo attivando una risposta immunitaria nota come "gliosi reattiva". La formazione di una cicatrice gliale densa attorno ai micro-ago isola elettricamente gli elettrodi dai neuroni circostanti, provocando un progressivo e inesorabile degrado del rapporto segnale-rumore (SNR) e sollevando la necessità di continue ricalibrature algoritmiche o di complessi interventi neurochirurgici di espanto e sostituzione.

4.7 Applicazioni militari delle BCI

Viste le recenti ideazioni di queste tecnologie, è attualmente molto difficile capire quali possano essere le potenziali applicazioni delle BCI nell'ambito Difesa. Certamente l'idea di un dispositivo collegato direttamente al cervello introduce una vulnerabilità cyber-biologica catastrofica: il *neuro-hacking*. Tuttavia, essendo allo stato attuale sostanzialmente degli EEG ad altissima risoluzione, in cui c'è una forma di comunicazione unidirezionale che parte dal cervello verso

il dispositivo, ma non viceversa, ci si può momentaneamente tranquillizzare sul fatto che non ci sarebbe nulla di "*neuro*" in caso di "*hacking*" di questi dispositivi, dato che non vanno direttamente nè a modificare nè ad alterare costantemente la struttura encefalica. In futuro, per giunta, questi potrebbero essere addirittura presentati con o in dei modelli non invasivi, modificando radicalmente lo scenario della sicurezza associata ad essi.

4.8 Direzioni future

Allo stato attuale, quindi, c'è ancora molto da capire sulle tecniche di neuromodulazione e su come esse possano essere integrate in ambito Difesa. Soltanto attraverso una mappatura rigorosa degli effetti a lungo termine e su una necessaria sincronizzazione tra Università e Difesa, si potrà andare avanti. Per fare piena luce sulle reali capacità, stabilità e limiti della neuromodulazione e del *neuroimaging* applicati, si rimanda in modo perentorio ad ulteriori e più approfonditi studi sperimentali integrati.

Bibliografia

Stato Maggiore della Difesa (2023). *Cognitive Warfare. La competizione nella dimensione cognitiva.*

NATO Chief Scientist Research Reports. *Cognitive Warfare.* Disponibile online: <https://www.sto.nato.int/wp-content/uploads/chief-scientist-report-cognitive-warfare-final.pdf>.

Lopez T. (2018). *Contrastare le operazioni di disinformazione russe richiede un approccio che coinvolga l'intero governo.* U.S. Joint Chiefs of Staff. Disponibile online: <https://www.jcs.mil/Media/News/News-Display/Article/1785644/challenging-russian-information-operations-requires-whole-of-government-approach/>.

Williams B. T. (2002). *Operazioni basate sugli effetti.* Army War College.

Mearsheimer J. J. (2019). *La grande illusione.* LUISS University Press.

Saletta M., Stearne R., Ebbott E. (2021). *Understanding Mass Influence. A case study of IRA.* University of Melbourne.

Rojas C. A. (2024). *Lezioni di Teoria Critica.* Aracne.

AA.VV. (2023). *Wokeismo, cancel culture, oicofobia. Tre minacce alla nostra società.* Historica Edizioni.

Heyriès H. (2026). *Storia dell'Esercito Italiano.* LEG Edizioni.

- Spengler O. (2008).** *Il tramonto dell'Occidente*. Longanesi.
- Heidegger M. (2020).** *Essere e Tempo*. Oscar Mondadori Cult.
- Galimberti U. (2005).** *Il tramonto dell'Occidente*. Feltrinelli.
- Jung C. G.** *Psicologia dell'inconscio. Edizione integrale*. Bollati Boringhieri.
- McIntyre L. (2024).** *Disinformazione. Combattere la verità e difendere la democrazia*. UTET Università.
- Sunstein C. R. (2026).** *Manipolazione. Cos'è, perché è un problema e come difendersi*. Raffaello Cortina.
- Arendt H. (1951).** *Le origini del totalitarismo*.
- Arendt H. (1967).** *Verità e politica*.
- Lyotard J. F. (1979).** *La condizione postmoderna*.
- Heidegger M.** *La poesia di Hölderlin*. Adelphi Edizioni, Milano.
- Veneziani M. (2025).** *Nietzsche e Marx si davano la mano. Vita, intrecci e pensiero dei due profeti che sconvolsero il mondo*. Marsilio Editore.
- Bernays E. (2020).** *Propaganda*. ShaKe Edizioni.
- Weil S. (1950).** *Attesa di Dio*. Gli Adelphi.
- Foucault M. (1977).** *Microfisica del potere*. Einaudi.
- Boco F. (2025).** *Accelerazionismo eretico*. Passaggio al Bosco.
- Minuz A. (2026).** *Egemonia senza cultura*. Silvio Berlusconi Editore.
- Shultz R. H., Godson R. (1984).** *Dezinformatsia: Active Measures in Soviet Strategy*. Potomac Books.
- Andrew C., Mitrokhin V. (2007).** *The Mitrokhin Archive*. Rizzoli.
- Bentivegna S., Boccia Artieri G.** *Le teorie della comunicazione di massa e la sfida digitale*. Laterza.
- Jung C. G. (1977).** *Gli archetipi dell'inconscio collettivo*. Bollati Boringhieri.

Benjamin W. (1936). *L'opera d'arte nell'epoca della sua riproducibilità tecnica*.

Alexander R. G., Macknik S. L., Martinez-Conde S. (2022). *What the Neuroscience and Psychology of Magic Reveal about Misinformation*. Publications, 10, 33. DOI: <https://doi.org/10.3390/publications10040033>.

Allen E. (2020). *Why We Believe: Disinformation, Misinformation, and Neuroscience*. Security Nexus Perspectives.

Arisoy A., Mandal S., Saxena R. (2022). *Human Brains Can't Detect Fake News: A Neuro-Cognitive Study of Textual Disinformation Susceptibility*. arXiv:2207.08376.

Ecker U. K. H., Swire B., Lewandowsky S. (2014). *Correcting Misinformation—A Challenge for Education and Cognitive Science*. In Rapp D. N., Braasch J. L. G. (eds.), *Processing Inaccurate Information*. MIT Press.

Gordon et al. (2017). *Exploring the neural substrates of misinformation processing*. Neuropsychologia, 106, 216–224.

Grignolio A., Morelli M., Tamietto M. (2022). *Why is fake news so fascinating to the brain?*. European Journal of Neuroscience.

Hoffman F. (2025). *Assessing Cognitive Warfare*. Small Wars Journal.

Hussain A., Soomro M. T. (2023). *Social Media: An Exploratory Study of Information, Misinformation, Disinformation, and Malinformation*. Applied Computer Systems, 28(1), 13–20.

Lentoor A. G. (2023). *Cognitive and neural mechanisms underlying false memories*. AIMS Neuroscience, 10(3), 255–268.

van der Linden S., Cohen M. S. (2025). *The neuroscience of misinformation: A research agenda*. Neuron, 113, 2225–2229.

Dando M. (2015). *Neuroscience and the future of chemical-biological weapons*. Springer.

Dando M. R. (2020). *Neuroscience and the problem of dual use.* Springer International Publishing.

Evans N. G. (2021). *The ethics of neuroscience and national security.* Routledge.

Hartley D. S., Jobson K. O. (2021). *Cognitive Superiority.* Springer International Publishing.

Moreno J. D., Schulkin J. (2020). *The brain in context: A pragmatic guide to neuroscience.* Columbia University Press.

NATO (2022). *Strategic Concept.*

Romeo G. (2021). *Guerre ibride. I volti nuovi del conflitto.*

Stato Maggiore della Difesa (2022). *Approccio della Difesa alle Operazioni Multidominio.*

Stato Maggiore della Difesa (2022). *L'impatto delle Emerging & Disruptive Technologies (EDTs) sulla Difesa.*

Stato Maggiore della Difesa (2023). *Cognitive Warfare. La competizione nella dimensione cognitiva.*

Bauman Z. (2002). *Modernità liquida.* Laterza, Roma-Bari.

Clark C. (2013). *I sonnambuli.* Laterza, Roma-Bari.

Clausewitz C. von (1997). *Della guerra.* Mondadori, Milano. (Prima edizione a cura dello Stato Maggiore dell'Esercito, 1970).

De Tocqueville A. (2020). *La democrazia in America.* UTET, Roma.

Durkheim E. (1996). *Le regole del metodo sociologico.* Editori Riuniti, Roma.

McLuhan M. (1990). *Gli strumenti del comunicare.* Mondadori, Milano.

Merton R. K. (2000). *Teoria e struttura sociale* (Vol. II). Il Mulino, Bologna.

Nisbet R. A. (1977). *La tradizione sociologica.* La Nuova Italia Editrice, Firenze.

Jomini A. (2026). *The Art of War*. Xpress, Chambersburg (PA). (Prima edizione in lingua francese, 1862).

Sun Tzu (2011). *L'arte della guerra*. Feltrinelli, Milano.

Keegan J. (2001). *Il volto della battaglia*. Il Saggiatore, Milano.

Whittam J. (1979). *Storia dell'esercito italiano*. Rizzoli, Milano.

Glossario degli Acronimi

2A/AD	<i>Anti-Access / Area Denial</i>
AI	<i>Artificial Intelligence</i> (Intelligenza Artificiale)
BCI	<i>Brain-Computer Interface</i> (Interfaccia Cervello-Computer)
BRICS	Brasile, Russia, India, Cina, Sudafrica (e Paesi aderenti)
CCRU	<i>Cybernetic Culture Research Unit</i>
CIEM	<i>Continued Influence of Misinformation / Persistent Misinformation Effect</i>
CIMIC	<i>Civil-Military Cooperation</i> (Cooperazione Civile-Militare)
Cogwar	<i>Cognitive Warfare</i> (Guerra Cognitiva)
CSE	Centro Studi Esercito
DDR	<i>Deutsche Demokratische Republik</i> (Repubblica Democratica Tedesca)
EDA	<i>Electrodermal Activity</i> (Conduttanza Cutanea)
EEG	Elettroencefalogramma / Elettroencefalografia
FIMI	<i>Foreign Information Manipulation and Interference</i>
FLN	<i>Front de Libération Nationale</i> (Fronte di Liberazione Nazionale - Algeria)

FRELIMO	<i>Frente de Libertação de Moçambique</i> (Fronte di Liberazione del Mozambico)
GPS	<i>Global Positioning System</i>
IA	Intelligenza Artificiale
InfoOps	<i>Information Operations</i> (Operazioni Informative)
IRA	<i>Internet Research Agency</i>
KGB	<i>Komitet Gosudarstvennoj Bezopasnosti</i> (Comitato per la Sicurezza dello Stato dell'URSS)
MDO	<i>Multi-Domain Operations</i> (Operazioni Multidominio)
NATO	<i>North Atlantic Treaty Organization</i> (Organizzazione del Trattato dell'Atlantico del Nord)
ONG	Organizzazione Non Governativa
ONU	Organizzazione delle Nazioni Unite
PANAS	<i>Positive and Negative Affect Schedule</i>
PSYOPS	<i>Psychological Operations</i> (Operazioni Psicologiche)
PTSD	<i>Post-Traumatic Stress Disorder</i> (Disturbo Post-Traumatico da Stress)
S.M.E.	Stato Maggiore dell'Esercito
STO	<i>Science and Technology Organization</i> (NATO STO)
StratCom	<i>Strategic Communications</i> (Comunicazioni Strategiche)
tACS	<i>Transcranial Alternating Current Stimulation</i> (Stimolazione Transcranica a Corrente Alternata)
tDCS	<i>Transcranial Direct Current Stimulation</i> (Stimolazione Transcranica a Corrente Continua)
TMS	<i>Transcranial Magnetic Stimulation</i> (Stimolazione Magnetica Transcranica)

tRNS	<i>Transcranial Random Noise Stimulation</i> (Stimolazione Transcranica a Rumore Casuale)
UAV	<i>Aerial Vehicle</i> (Sistemi Aeromobili a Pilotaggio Remoto / Droni)
UE	Unione Europea
URSS	Unione delle Repubbliche Socialiste Sovietiche



CSE
CENTRO STUDI ESERCITO

Email

info@centrostudiesercito.it

Indirizzo

Viale Bruno Buozzi 47,
Roma, 00197

Sito web

www.centrostudiesercito.it