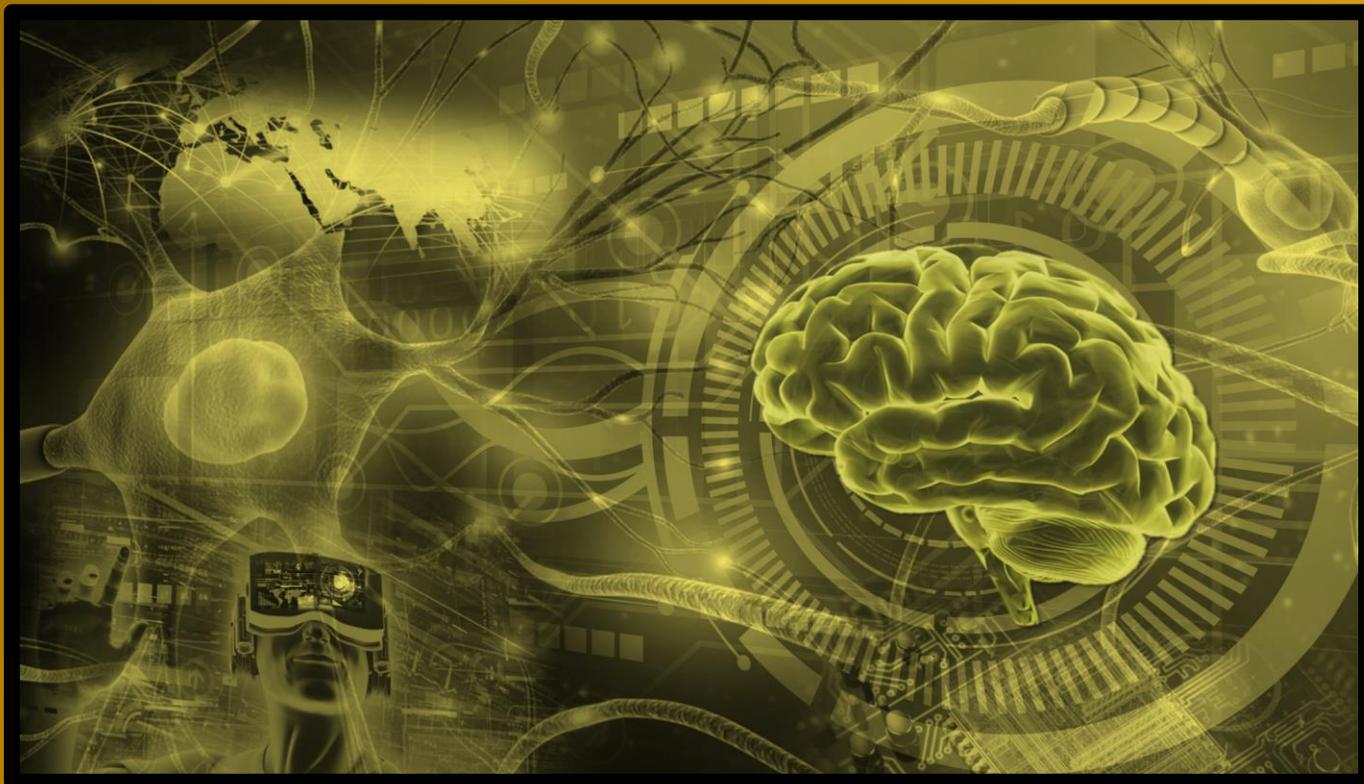


STATO MAGGIORE DELLA DIFESA



COGNITIVE WARFARE

La competizione nella dimensione cognitiva

Edizione 2023

© Tutti i diritti riservati – MINISTERO DELLA DIFESA - Stato Maggiore della Difesa
Titolo: “*Cognitive Warfare*. La competizione nella dimensione cognitiva”.

PREFAZIONE DEL CAPO DI STATO MAGGIORE DELLA DIFESA



La Difesa è da tempo consapevole della necessità di dover affrontare in modo sistemico e lungimirante le sfide poste da tecnologie ed ambienti emergenti, come quelle derivanti dalla dimensione cognitiva.

Una dimensione parte integrante del “campo di battaglia” nel quale operiamo quotidianamente, basata su armi contemporanee capaci di condizionare l’opinione comune, e, in ultima analisi, manipolare le decisioni, influenzando, interferendo e alterando le dinamiche cognitive ad ogni livello, nel quadro di strategie comunicative invasive e destabilizzanti.

La capacità di generare effetti sfruttando i limiti e le vulnerabilità della mente umana per influenzare e, potenzialmente, manipolare il comportamento umano costituisce, quindi, una nuova frontiera di competizione per il perseguimento del vantaggio strategico, con minaccia diretta alla stessa Sicurezza Nazionale.

Tale estensione del campo di battaglia, con i correlati sviluppi delle tecnologie emergenti e nel settore delle neuroscienze, rappresenta un’evoluzione immateriale del confronto che assume rilevanza assoluta in tempi di incertezza come quelli attuali, rispetto ai quali le relazioni internazionali registrano rinnovata competizione tra sistemi valoriali concorrenti, anche attraverso una violenta guerra di narrative sulle reti di comunicazione.

Tutto ciò, alimenta suggestioni e distorsioni a premessa di una sempre maggiore polarizzazione sociale e geopolitica, confermando come la capacità di generare effetti nella dimensione cognitiva esprima la sua valenza strategica nell'intero spettro della competizione (continuum of competition), estendendo la portata della sua azione alle situazioni di conflitto, anche grazie alla capacità di amplificare gli effetti dell'azione cinetica.

In tale quadro, anche alla luce degli effetti della cosiddetta “guerra ibrida” che si sviluppa secondo dinamiche sempre più letali, il Cognitive Warfare (competizione cognitiva) può essere definito come un'operazione multidominio (o parte di essa) che impiega mezzi, azioni e strumenti attraverso le connessioni tra i domini classici (terrestre, aereo, navale), i domini spazio e cyber, l'ambiente informativo e lo spettro elettromagnetico influenzando il comportamento umano e generando effetti nella dimensione cognitiva, con l'obiettivo di ottenere un vantaggio sull'avversario.

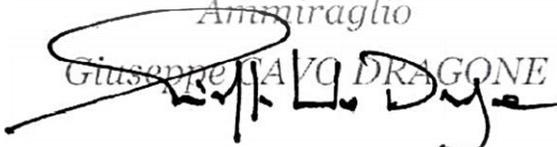
Emerge quindi la necessità di farci trovare pronti, in sinergia con le Istituzioni, per fornire risposte di sistema anche in ragione del fatto che il Cognitive Warfare e le sfide derivanti dalla portata del fenomeno, esulano da competenze esclusive di un unico Dicastero, richiedendo un'azione corale, sia a livello nazionale che internazionale, attraverso un processo di crescente responsabilizzazione degli stakeholder, anche privati.

Come Difesa, con questo documento, abbracciando il paradigma dell'Open Innovation abbiamo affrontato il tema della competizione cognitiva in ottica multidisciplinare, cercando di inquadrare il tema ed identificarne le possibili linee di indirizzo, attraverso un network di esperti militari e civili provenienti dal mondo accademico, industriale e della ricerca.

Per essere all'altezza delle sfide del futuro occorrerà, innanzitutto, accrescere la nostra consapevolezza, informando, formando ed educando il personale militare, con particolare focus sulla leadership. In parallelo, si dovrà valorizzare il ruolo della Difesa e garantirne il pieno coinvolgimento ab initio, migliorare la comprensione della minaccia, rafforzare i progetti di ricerca e sviluppo tecnologico di settore, raggiungere una concreta capacità di integrare e sincronizzare effetti cinetici e non cinetici, in primis con il potenziamento della capacità di comunicazione. Tutto questo, nella cornice di un coerente progetto di sistema che punti ad adeguare – in linea con l'evoluzione internazionale – il quadro giuridico funzionale ad abilitare l'azione dello Strumento Militare.

La Difesa, come sempre, intende quindi fare la sua parte, mettendo a disposizione delle Istituzioni, del Paese e delle Organizzazioni Internazionali di riferimento la sua professionalità, la sua visione e le sue capacità, a tutela degli interessi nazionali, a protezione dei nostri cittadini ed a salvaguardia del perimetro di valori condivisi nei quali crediamo.

Buona Lettura!

Ammiraglio
Giuseppe LAURO DRAGONE


INDICE

CAPITOLO 1 – IL CONTESTO STRATEGICO	1
1.1 LA PROSPETTIVA RUSSA.....	3
1.2 LA PROSPETTIVA CINESE.....	3
CAPITOLO 2 – LA COMPETIZIONE COGNITIVA	5
2.1 RILEVANZA DELLA DIMENSIONE COGNITIVA.....	8
2.2 GLI STRUMENTI DEL <i>COGNITIVE WARFARE</i>	10
2.3 DEFINIZIONE DEL PROBLEMA MILITARE	11
CAPITOLO 3 – NUOVI STRUMENTI DI INFLUENZA.....	13
3.1 FATTORI CONCORRENTI	14
3.2 <i>SOCIAL MEDIA E MARKETING</i>	17
3.3 STRATEGIE DI INFLUENZA	18
3.4 IL <i>GAMING</i> COME ANTEPRIMA DELLO SPAZIO DIGITALE	20
3.5 FORME DI CONTRASTO.....	22
3.6 INQUADRAMENTO GIURIDICO	24
CAPITOLO 4 – NUOVI STRUMENTI DI INTERFERENZA	27
4.1 POTENZIALI APPLICAZIONI MILITARI.....	28
4.2 ASPETTI ETICO-GIURIDICI.....	33
CAPITOLO 5 – NUOVI STRUMENTI DI ALTERAZIONE.....	35
5.1 LA COMUNICAZIONE UOMO-MACCHINA	36
5.2 LA <i>HUMAN COMPUTER CONFLUENCE</i>	37
5.3 L' <i>HACKING</i> COGNITIVO	38
5.4 PRINCIPI ETICO-GIURIDICI DI RIFERIMENTO.....	39
5.5 L'ESIGENZA DI UN COMITATO ETICO.....	41
CONCLUSIONI	45
IL <i>COGNITIVE WARFARE</i> NEL CONTESTO MULTIDOMINIO.....	45
LINEE DI INDIRIZZO	47

ALLEGATI

Allegato A - LE OPERAZIONI INFORMATIVE RUSSE.....	57
Allegato B - LA GUERRA COGNITIVA CINESE.....	61
Allegato C - RECIPROCIÀ E NORME SOCIALI.....	65
Allegato D - METODOLOGIA DI LAVORO E BIBLIOGRAFIA.....	67

CAPITOLO 1

IL CONTESTO STRATEGICO

L'attuale contesto internazionale è caratterizzato dall'acuirsi della competizione tra sistemi valoriali concorrenti che si esprime anche attraverso una violenta guerra di narrative sulle reti di comunicazione. Tale situazione ha contribuito ad alimentare suggestioni e percezioni foriere di una sempre maggiore polarizzazione sociale e geopolitica, confermando come la capacità di generare effetti nella dimensione cognitiva esprima la sua valenza strategica nell'intero spettro della competizione (*continuum of competition*), estendendo la portata della sua azione alle situazioni di conflitto grazie alla capacità di amplificare anche gli effetti dell'azione cinetica.

In tale contesto, la Federazione Russa prosegue la sua sfida all'Occidente violando apertamente l'ordine liberale internazionale con l'obiettivo di porsi quale valida alternativa, utilizzando, tra l'altro, strategie di disinformazione per creare confusione, dividere e impedire ai propri avversari di organizzare una risposta alla propria azione. La Cina, invece, persegue la sua linea di affermazione egemonica e di occupazione della rete mondiale di infrastrutture critiche, anche in aperta sfida al diritto internazionale, nel tentativo di ottenere la superiorità tecnologica e il controllo delle comunicazioni per estendere la propria sfera di influenza attraverso strategie più a lungo termine e il pieno sfruttamento di tutti gli aspetti cognitivi al punto da riconoscergli una centralità strategica.

Parallelamente, in Occidente si è andata diffondendo una sempre maggiore consapevolezza della portata del fenomeno e, con livelli e profondità differenti, si stanno elaborando studi e strategie per affrontare le future sfide sia a livello nazionale che internazionale. In ambito NATO il progetto di sviluppare un *Cognitive Warfare Concept* entro il 2024 si inquadra quale elemento prodromico al *Warfare Development Imperative (WDI)*¹ "*Cognitive Superiority*". In ambito europeo, gli sforzi condivisi nello *Strategic Compass*² per il contrasto alla disinformazione hanno l'obiettivo di sviluppare un pacchetto di strumenti contro la manipolazione delle informazioni e le ingerenze da parte di attori stranieri.

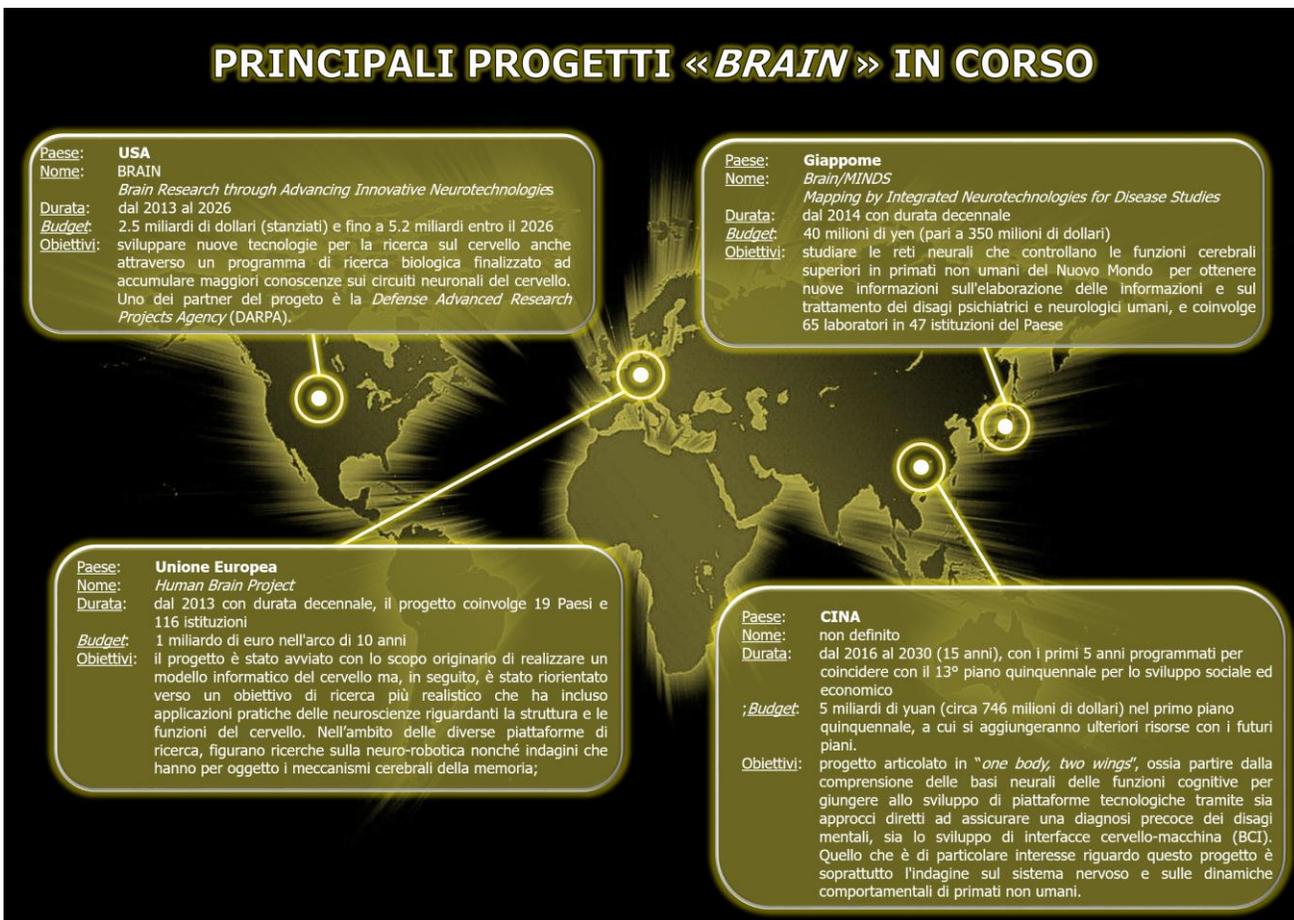
Dopo l'esperienza della pandemia e ancor di più con il conflitto russo-ucraino, anche a livello nazionale si è cominciata a diffondere una maggiore consapevolezza della portata del fenomeno riconoscendo la disinformazione quale sfida da fronteggiare nell'ambito della "Strategia Nazionale di Cybersicurezza" e nel sotteso "Piano di implementazione".

¹ Nell'ambito del processo di implementazione del NATO *Warfighting Capstone Concept* (concetto "*Capstone*" volto a delineare la traiettoria per la modernizzazione delle strutture, delle capacità e della dottrina militare al fine di incrementare l'efficienza militare), l'Alleanza ha sviluppato un ambizioso piano di sviluppo attraverso la *Warfare Development Agenda* che si compone di 5 pilastri principali indicati quali *Warfare Development Imperatives (WDI)*.

² Documento strategico dell'Unione Europea che mira a definire una visione strategica comune per la politica di sicurezza e di difesa dell'UE nei prossimi 5-10 anni.

Per analizzare compiutamente le attuali e le future sfide della dimensione cognitiva, occorre comprendere come questa si estenda ben oltre la portata della disinformazione *on-line* coinvolgendo:

- aspetti di reciprocità che si basano su vincoli etici e giuridici diversi e sistemi nazionali che consentono ai *competitors* di perseguire comportamenti aggressivi attraverso le reti globali negando la possibilità di risposta con l'implementazione di reti sovrane interne (come nel caso della rete cinese o il tentativo della Federazione Russa di attivare la propria rete RuNet);
- aspetti di superiorità tecnologica relativi alle reti di comunicazione, alle tecnologie interattive di persuasione, alla fusione civile-militare e alla crescente militarizzazione delle neuroscienze attraverso progetti "*brain*" che sono oggetto di una sempre maggiore attenzione anche per applicazioni militari.



1.1 LA PROSPETTIVA RUSSA

Nella prospettiva della Federazione Russa (approfondimento in Allegato A) non viene mai fatto esplicito riferimento agli aspetti cognitivi. Il controllo e l'influenza della sfera informativa sono emersi nella discussione strategica russa a partire della metà degli anni '90 e si sono consolidati con il passaggio al “*Non-contact warfare*” attraverso azioni informative volte a rafforzare e accompagnare le operazioni convenzionali.

L'approccio operativo russo, maturato poi nel 2014 in Ucraina, è infatti quello di utilizzare la disinformazione con l'obiettivo di favorire le operazioni militari, massimizzando la disorganizzazione dell'avversario e creando una situazione di incertezza permanente attraverso il concetto di controllo della reazione (*reflexive control*). L'interferenza nei flussi informativi avversari diviene un approccio sistemico e le operazioni informative sono state progressivamente percepite come uno strumento politico con il tentativo di utilizzarle anche a livello strategico. Nonostante le imponenti campagne di disinformazione, tuttavia, i risultati in Europa sono stati per lo più modesti e legati a situazioni politiche locali attraverso l'amplificazione di posizioni polarizzate già presenti nell'ecosistema informativo. La capacità di inserirsi in conflitti e narrazioni preesistenti, come l'ostilità nei confronti dei Paesi europei (e, in particolare, verso la Francia) ha però permesso alla Russia, grazie al supporto dei regimi e dei governi locali, di guadagnare una buona reputazione nel continente africano dove le operazioni informative *on-line* hanno grandemente favorito le manifestazioni dell'*hard power* russo.

Nonostante non siano attualmente note iniziative analoghe ai progetti “*brain*” nel contesto russo, la convergenza civile-militare ha permesso di sviluppare piani centralizzati per lo sviluppo dell'Intelligenza Artificiale con la creazione di un dipartimento della Difesa per implementazione dell'IA nello sviluppo di sistemi d'arma attraverso lo sviluppo di sistemi autonomi (RAS) ai quali potrebbero essere correlati anche progetti per lo sviluppo di reti neurali e interfacce cerebrali³.

1.2 LA PROSPETTIVA CINESE

Nell'ambito della propria “Dottrina delle Tre Guerre” (psicologica, dell'opinione pubblica e legale), la prospettiva della Repubblica Popolare Cinese (approfondimento in Allegato B) riconosce una centralità strategica al dominio cognitivo che si può esplicitare attraverso il ricorso a “stratagemmi” e fattori intangibili (morale, coesione, ruolo dell'opinione pubblica) per influenzare e manipolare l'avversario, ma che assume un ulteriore livello attraverso lo sviluppo tecnologico e, in particolare, dell'Intelligenza Artificiale. Tramite la strategia della “fusione civile-militare”, la Cina mira, infatti, ad acquisire una *leadership* nella corsa all'IA e, al contempo, a darvi applicazione in ambito militare con un progressivo processo di “intelligentizzazione” della guerra e l'accelerazione dei processi decisionali e di elaborazione delle informazioni. In tal senso, l'approccio cinese alla guerra cognitiva si può

³ US Center for Naval Analyses, *Russia Studied Program “Artificial Intelligence and Autonomy in Russia: A Year’s Reflection”*, Settembre 2022 (<https://www.cna.org/centers-and-divisions/cna/sppp/russia-studies>).

esprimere più nella ricerca di un vantaggio futuro rispetto all'Occidente, che nel tentativo di colmare il *gap* attualmente esistente. L'attenzione alla crescita esponenziale del ritmo e della complessità delle operazioni militari potrà richiedere anche un potenziamento dell'intelligenza umana, attraverso lo sviluppo di nuove forme di "intelligenza ibrida", che potrebbe tradursi nello sviluppo di interfacce neurali molto spinte, già oggetto di studi a livello scientifico in Cina tramite un progetto *brain* dedicato (vds. figura dei principali progetti "*brain*" in corso).

CAPITOLO 2

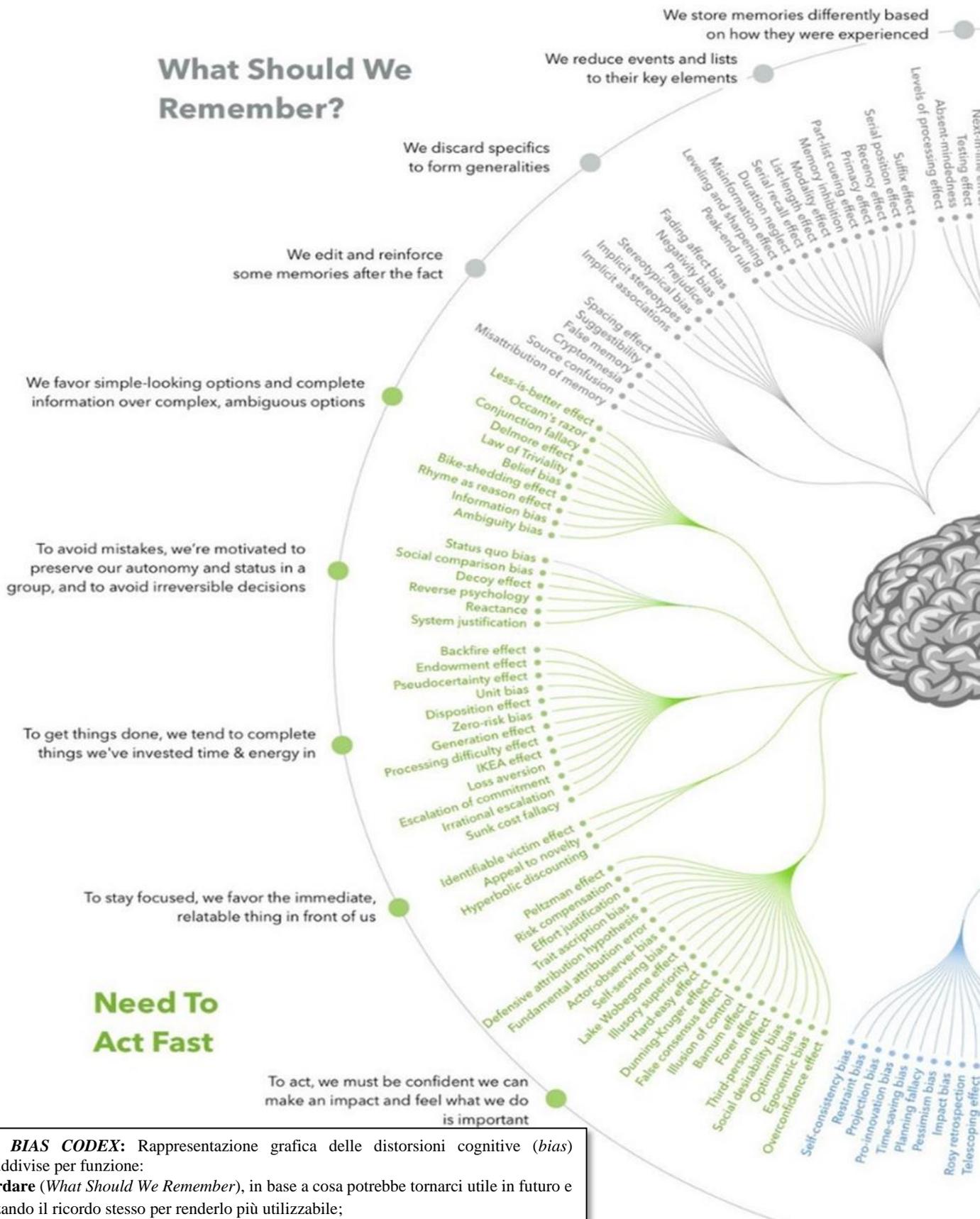
LA COMPETIZIONE COGNITIVA

Descrivere la portata della competizione per la dimensione cognitiva necessita preliminarmente di una comprensione generale del funzionamento della mente umana e delle sue vulnerabilità, che alcuni *competitors* stanno imparando a conoscere e sfruttare a proprio vantaggio. Benché spesso considerata quale elemento prevalentemente astratto, nella mente umana confluiscono elementi psicologici, legati ai processi mediante i quali ogni individuo acquisisce, elabora e dà significato a stimoli e informazioni provenienti dall'ambiente in funzione del proprio comportamento (percezione, immaginazione, simbolizzazione, formazione di concetti, soluzione di problemi), ed elementi neurologici, costituiti dall'insieme delle strutture specializzate del cervello responsabili di molteplici funzioni - consce ed inconsce - tra le quali l'elaborazione del pensiero, il linguaggio, la memoria e il controllo delle emozioni. Tutti questi processi sono prevedibili e manipolabili. È altresì noto che la quantità di funzioni assolve dalla mente umana ne rappresenti tuttavia uno dei principali limiti poiché, al di fuori delle situazioni di estremo rischio per la stessa esistenza (situazioni "lotta o fuggi"), la nostra parte cosciente è responsabile solo del 5-10% del processo decisionale e all'incirca del 5% dell'interpretazione delle informazioni (*sense-making*) e della memoria. Tutto il resto dei processi di elaborazione del pensiero avviene attraverso la parte inconscia della mente umana che diviene, quindi, il *target* delle possibili azioni avversarie. Tale prevalenza inconscia rappresenta, inoltre, la chiave per comprendere il funzionamento dei *bias*⁴ e quindi di come gli esseri umani siano naturalmente portati a non considerare informazioni razionali o logiche che pongono a rischio i loro elementi identitari (valori, credenze, cultura, ecc.), privilegiando piuttosto informazioni che si allineano a sentimenti ed emozioni che risiedono nella parte inconscia.

I *bias*, considerati quali deviazioni dal normale processo razionale e che ci spingono a ricreare una visione soggettiva della realtà, vengono naturalmente sviluppati in quanto costituiscono scorciatoie mentali che ci consentono di risparmiare energia (approccio euristico), permettono all'individuo di proteggere il proprio ego e la propria identità, rappresentano un *framework* familiare che ci rassicura in situazioni di incertezza.

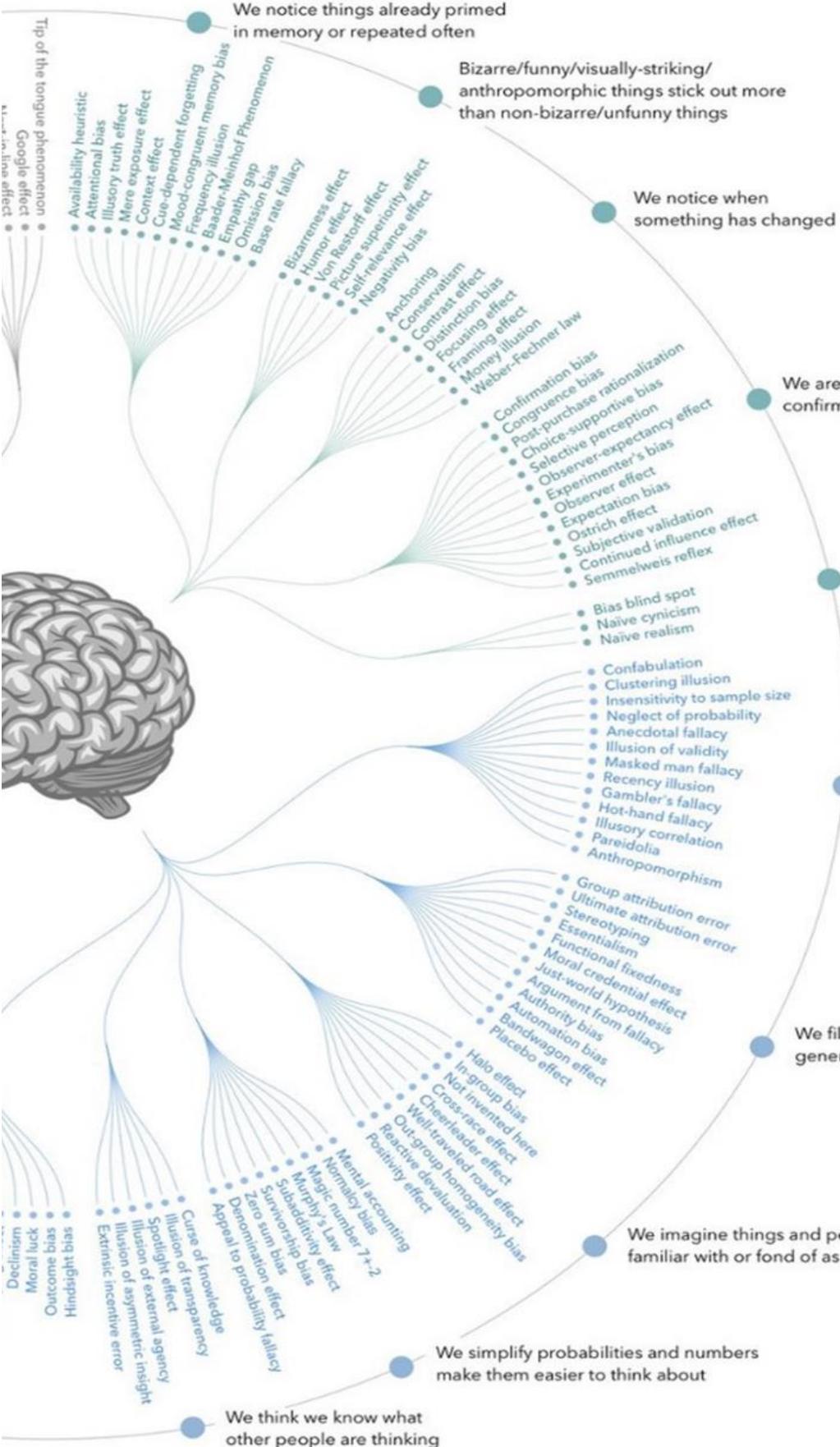
⁴ Distorsioni nelle valutazioni di fatti e avvenimenti per effetto delle scorciatoie euristiche sviluppate dal cervello umano.

What Should We Remember?



COGNITIVE BIAS CODEX: Rappresentazione grafica delle distorsioni cognitive (*bias*) conosciute, suddivise per funzione:

- **cosa ricordare** (*What Should We Remember*), in base a cosa potrebbe tornarci utile in futuro e generalizzando il ricordo stesso per renderlo più utilizzabile;
- **filtrare informazioni** (*Too Much Information*), per rispondere all'impossibilità di processare tutte le informazioni oggi disponibili;
- **dare un senso** (*Not Enough Meaning*), mettendo a sistema informazioni sparse;
- **agire velocemente** (*Need to Act Fast*), prendendo una decisione anche in assenza di tutte le informazioni necessarie.

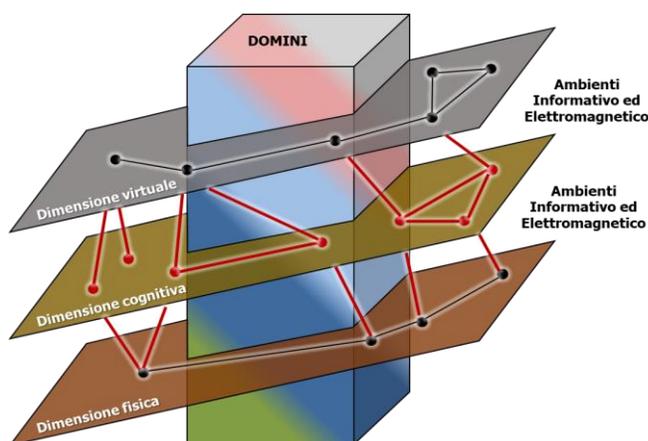


Too Much Information

Not Enough Meaning

2.1 RILEVANZA DELLA DIMENSIONE COGNITIVA

Il contesto operativo Multidominio è un sistema complesso in continua evoluzione in cui le singole variazioni che agiscono lo modificano portandolo ad un nuovo stato, diverso da quello iniziale. In tale sistema complesso, i domini (terrestre, marittimo, aereo, spaziale e cibernetico), le dimensioni degli effetti (fisica, virtuale e cognitiva), i sistemi (politico, militare, economico, sociale, informativo e infrastrutturale) e gli ulteriori ambienti (informativo ed elettromagnetico) concorrono a generare un unico sistema di sistemi in cui tutti gli aspetti sono legati da una serie di interrelazioni attraverso una serie di nodi collocati su più piani differenti⁵.

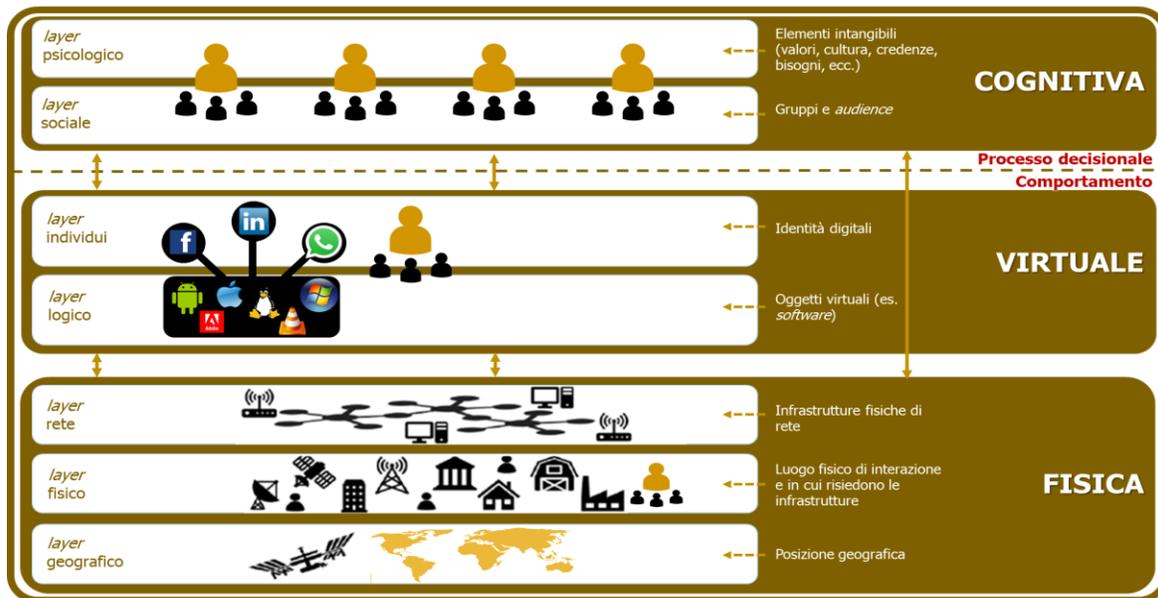


Pertanto, particolare rilevanza assume la competizione nella dimensione cognitiva (*Cognitive Warfare*) che, nella sua dimensione intangibile, prende di mira ideologie, valori e società attraverso un uso sempre più esteso di mezzi di comunicazione e nuove soluzioni tecnologiche e la crescente attenzione militare al settore delle neuroscienze e alle sue applicazioni.

Il *Cognitive Warfare* può quindi essere definito come un'operazione Multidominio (o parte di essa) che impiega mezzi, azioni e strumenti attraverso le connessioni esistenti tra i domini (terrestre, marittimo, aereo, spaziale e cyber), l'ambiente informativo e lo spettro elettromagnetico per generare effetti nella dimensione cognitiva e influenzare il comportamento umano per ottenere un vantaggio sull'avversario.

Rappresentare schematicamente le complesse relazioni esistenti tra le differenti dimensioni degli effetti e come esse contribuiscano ad influenzare il pensiero umano richiede uno sforzo di semplificazione che, pur non risultando pienamente esplicativo, consente di comprendere la portata del concetto di *Cognitive Warfare*, attraverso la rappresentazione dell'ambiente informativo. In tale schematizzazione, le dimensioni sono suddivise in differenti *layer*:

⁵ Cfr. SMD – “Approccio della Difesa alle Operazioni Multidominio” (2022).



a. La dimensione cognitiva

Rappresenta il luogo intangibile in cui le decisioni vengono assunte e vengono indirizzati i comportamenti degli individui, anche attraverso le azioni condotte nelle altre dimensioni. Si distingue nei *layer*:

- **psicologico**, che comprende l'insieme intangibile degli elementi che rappresentano l'identità del pensiero umano (valori, cultura, credenze, volontà, aspirazioni, bisogni, ecc.) ed in cui le informazioni vengono interpretate, ma non trasmesse;
- **sociale**, che comprende il sistema di relazioni tra il singolo e i gruppi sociali di cui fa o si sente parte e rappresenta il livello in cui l'interpretazione delle informazioni, il comportamento e le decisioni vengono influenzati dall'ambiente sociale e culturale.

b. La dimensione virtuale

È lo spazio virtuale in cui le *audience* (individui, comunità e organizzazioni) sempre più spesso interagiscono. Può essere schematizzata attraverso i due *layer*:

- **individui**, che comprende l'insieme dei profili che interagiscono con meccanismi di influenza sul modello *leader-followers* attraverso contenuti digitali. Tali profili possono essere pubblici, istituzionali, di singoli individui (anche attraverso multiple proiezioni) o fittizi (*bot*⁶ che operano attraverso l'impiego di algoritmi di Intelligenza Artificiale);
- **logico**, contiene l'insieme delle attività non direttamente percepite nella creazione, trasmissione e memorizzazione di contenuti digitali e costituisce l'infrastruttura digitale di relazioni, servizi e altre risorse che consentono lo scambio di contenuti. Comprendendo anche la configurazione delle reti, i dati e i protocolli di trasferimento, nonché i processi virtuali ed elettromagnetici correlati, sono quasi esclusivamente

⁶ Abbreviazione di *robot*, è un programma che accede alla rete attraverso lo stesso tipo di canali utilizzati dagli utenti che fa credere all'altro utente di comunicare con una persona.

collocati nell'ambiente cibernetico in cui eventuali azioni possono inficiare e/o alterare l'integrità e l'accessibilità dei dati.

c. La dimensione fisica

Rappresenta l'insieme delle aree geografiche in cui individui, nazioni, culture e società interagiscono e degli oggetti e infrastrutture che consentono tali interazioni. Può essere suddivisa in tre differenti *layer*:

- **rete**, costituisce la “topologia” del *network* e comprende l'insieme delle infrastrutture fisiche sottese ai *layer* virtuali attraverso cui avviene la trasmissione e ricezione di dati mediante la conversione da *bit* digitali in segnali radio, elettrici e ottici;
- **fisico**, che rappresenta il luogo in cui le *audience* interagiscono e in cui risiedono le infrastrutture (umane e di comunicazione);
- **geografico**, che rappresenta il loro posizionamento geografico.

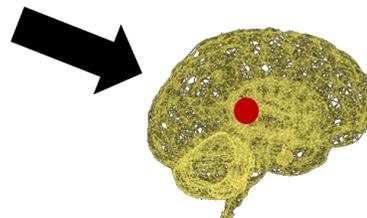
2.2 GLI STRUMENTI DEL COGNITIVE WARFARE

In considerazione delle vulnerabilità insite nella mente umana, alcuni attori hanno sviluppato strategie sempre più sofisticate ed efficaci per generare effetti nella dimensione cognitiva e manipolare le scelte di una determinata *target audience*, sia attraverso il ricorso a strumenti atti a influenzare le percezioni e i comportamenti degli individui, sia attraverso il ricorso a nuove soluzioni tecnologiche per migliorare o degradare funzioni e/o capacità del nostro cervello.

L'innovazione portata dall'impiego di questi nuovi strumenti si aggiunge agli effetti sulla dimensione cognitiva delle azioni classiche di tipo cinetico (quali ad esempio la paura generata da un bombardamento o la motivazione di una compagine militare a continuare a combattere dopo una sonora sconfitta) o non cinetico (quali la diffusione di un sentimento di gratitudine e di consenso per la realizzazione di un progetto CIMIC⁷ a favore di una comunità o l'effetto di una campagna informativa). L'esperienza del conflitto russo-ucraino è un chiaro esempio di come si possa amplificare esponenzialmente gli effetti dello scontro attraverso il potenziamento delle percezioni e suggestioni correlate.

L'azione diretta o indiretta di questi nuovi strumenti può essere suddivisa in tre differenti macro-aree:

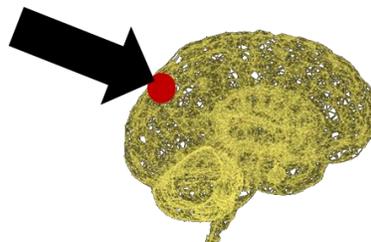
- **influenza**: è l'insieme degli strumenti e delle metodologie impiegabili per influenzare e manipolare, direttamente o indirettamente, il pensiero umano. Tali strumenti operano al di fuori della mente umana e generano effetti attraverso i processi cognitivi di interpretazione delle informazioni secondo gli schemi culturali e valoriali di riferimento e i *bias* personali. Essi operano prevalentemente, ma non esclusivamente, attraverso la dimensione digitale e le reti sociali dell'ambiente informativo tramite l'utilizzo di tecnologie interattive di persuasione che consentono di sviluppare strategie a breve-



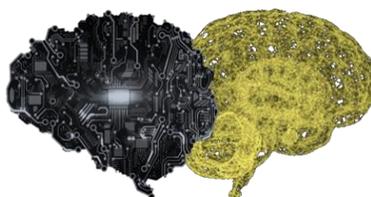
⁷ Cooperazione Civile-Militare: funzione operativa che integra la comprensione dei fattori civili dell'ambiente operativo per supportare il conseguimento degli obiettivi strategici della missione.

medio termine di disinformazione per orientare, dividere, polarizzare, sovvertire e radicalizzare ovvero, guardando in prospettiva, anche potenziali strategie più a lungo termine per influenzare e manipolare persino usi, credenze, costumi e abitudini di una specifica *audience*;

➤ **interferenza:** è l'insieme degli strumenti e delle tecnologie che, attraverso la profonda conoscenza del funzionamento del cervello, operano sulle sue dinamiche fisiologiche e biochimiche per interferire con il processo cognitivo. Tali strumenti operano direttamente sul cervello umano e possono essere impiegati per migliorare (*enhancement*) o degradare (mediante le cosiddette *neuroweapons*) specifiche funzioni e/o capacità del cervello. In tale insieme possono essere ricompresi anche principi attivi presenti in farmaci, sostanze stupefacenti, alimenti, impulsi elettrici e onde elettromagnetiche che interagiscono sui processi cognitivi;



➤ **alterazione:** è l'insieme degli strumenti e delle tecnologie che, attraverso l'utilizzo di interfacce più o meno invasive, permettono l'interazione tra il cervello umano e le macchine e che possono essere impiegati per incrementare, anche significativamente e attraverso un contributo esterno, le capacità della mente umana (*augmentation*), ma le cui vulnerabilità potrebbero anche essere impiegate in chiave offensiva per degradare le capacità dell'avversario. In tale insieme, possono essere ricomprese le tecnologie di confluenza e ibridazione tra uomo e macchina e spaziano dalla realtà virtuale/aumentata alle interfacce cervello-macchina (*Brain Computer Interface-BCI*) e cervello-cervello (*Brain-to-Brain Interface-B2BI*), fino alle potenziali soluzioni di ibridazione più avanzate verso il modello *Cyborg*.



2.3 DEFINIZIONE DEL PROBLEMA MILITARE

La sfida di questa nuova frontiera di competizione cognitiva si estende a livello globale (individui, gruppi e comunità) con potenziali impatti dirompenti sia in termini di Sicurezza Nazionale che di stabilità internazionale, e richiede necessariamente risposte a livello *Whole of Society*. In particolare, tenuto conto che anche lo Strumento Militare può essere oggetto di azioni malevole condotte sul piano cognitivo, con potenziali impatti sulla capacità decisionale (*decision-making*), sulla piena comprensione del contesto operativo (*situational understanding*) e sull'efficacia delle operazioni e sulla sicurezza/protezione del personale, risulta necessario comprendere il ruolo della Difesa nella dimensione cognitiva, contribuire a definire il quadro etico-giuridico di riferimento e definire le linee di indirizzo per la trasformazione e l'innovazione dello Strumento Militare.

CAPITOLO 3

NUOVI STRUMENTI DI INFLUENZA



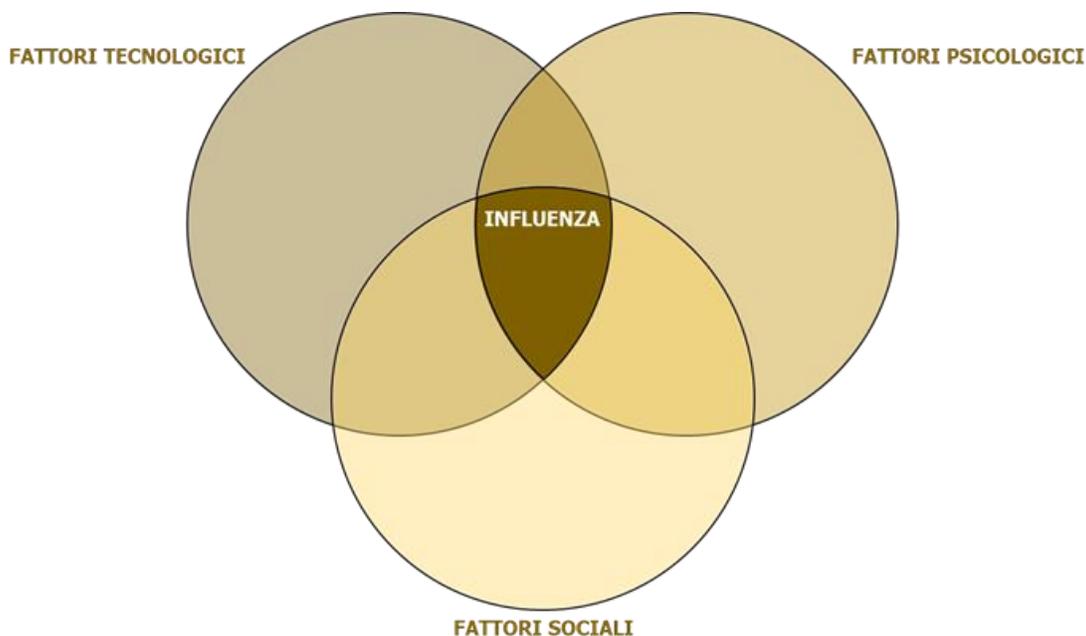
L'evoluzione nel tempo del mezzo di comunicazione (dalla carta stampata alla radio, dalla televisione ai computer/internet) ha modificato il mondo dell'informazione e della comunicazione, grazie alla crescente capacità di trasmettere messaggi "immediati" ad *audience* sempre più ampie. La rivoluzione digitale, l'avvento dei *social media* e di tutti gli altri canali di comunicazione digitale hanno ulteriormente trasformato questa realtà, soppiantando, di fatto, tutti gli strumenti precedenti ed aprendo il mondo della comunicazione a una nuova schiera di attori che veicolano i loro messaggi e contribuiscono, talvolta in maniera determinante, a orientare l'opinione pubblica e manipolare il dibattito socio-politico. Tale cambiamento ha contribuito significativamente a modificare i nostri usi e le nostre abitudini, proiettandoci in una realtà iperconnessa in cui siamo destinatari di una quantità senza precedenti di contenuti e costantemente in contatto con un numero crescente di attori. Conseguentemente, si assiste sempre più al passaggio da sistemi basati su modelli di interazione tra utenti, verso modelli di intrattenimento (*infotainment*⁸) che incoraggiano una propensione alla fruizione passiva di contenuti. L'impossibilità di processare l'immensa mole di informazioni trasporta il singolo individuo in un sistema di *overflow* di contenuti in cui i meccanismi di affiliazione di tipo *leader-follower* e le comunità digitali contribuiscono a costituire un sistema di riferimento per la formulazione dell'opinione del singolo.

Parallelamente, con l'implementazione e la distribuzione dell'IoT (*Internet of Things*) e, in prospettiva dell'IoE (*Internet of Everything*), assistiamo a un moltiplicarsi di dispositivi interattivi sempre più indossabili (*smartphone*, *smartwatch*, ecc.) e vicini a noi (es. assistenti vocali) cui affidiamo funzioni di consulenza e supporto, attraverso i quali è già possibile influenzare i comportamenti del singolo utilizzando tecnologie interattive di persuasione sempre più efficaci.

⁸ Termine derivato dalla fusione di *information* ed *entertainment* che indica l'ibridazione tra informazione e intrattenimento.

3.1 FATTORI CONCORRENTI

Nel contesto generale descritto, attraverso la combinazione di fattori tecnologici, sociali e psicologici, alcuni attori stanno sviluppando comportamenti e strategie sempre più invasivi e tesi a influenzare l'avversario.



a. Fattori tecnologici

Tra i fattori tecnologici che concorrono allo sviluppo delle nuove strategie di influenza, particolare significatività assumono le **tecnologie interattive di persuasione**. Queste tecnologie – che rientrano nell'ambito della captologia⁹ quale branca delle scienze sociologiche che studia l'impatto delle tecnologie interattive su comportamenti, abitudini e convinzioni di chi naviga in rete – possono essere suddivise in **macro-persuasione** (*macrosuasione*), quando l'intero prodotto (es. oggetti, *software* o pagine web) viene concepito per motivare e persuadere l'utente a effettuare una determinata azione, e **micro-persuasione** (*microsuasione*), quando all'interno di un prodotto concepito per proprie finalità possono essere inseriti singoli elementi di persuasione (es. singole funzioni degli *smart device*).

In ragione della funzione cui sono destinate e del ruolo che possono assumere possono essere catalogate come:

- **strumenti di persuasione**: supportano l'utente in determinate funzioni per incentivarne un determinato comportamento (rientrano in tale categoria gli strumenti di profilazione dei contenuti, la stimolazione tramite notifiche e *reminder*, il monitoraggio delle prestazioni sportive, ecc.);
- **simulazioni persuasive**: attraverso la capacità di mostrare l'effetto di un'azione o di vivere una determinata esperienza, inducono l'utente ad adottare un determinato

⁹ Termine coniato nel 1996 da Brian Jeffrey Fogg, direttore del Laboratorio di Tecnologia Persuasiva della *Stanford University*, e la cui etimologia deriva dall'acronimo CAPT (*Computers As Persuasive Technologies*).

comportamento (rientrano in tale categoria le simulazioni di relazioni causa-effetto, di ambienti e oggetti);

- **attori sociali:** attraverso il monitoraggio dei comportamenti e l'uso di incentivi quali ricompense o raccomandazioni l'utente viene indotto ad intraprendere o abbandonare determinate azioni/comportamenti (rientrano in tali categoria, ad esempio, alcune funzioni dei dispositivi di *e-fitness* che incentivano ad adottare comportamenti più sani).

Tali tecnologie, inizialmente sviluppate per finalità prevalentemente commerciali, oggi costituiscono l'ossatura dei *digital media*, delle piattaforme di *e-commerce*, del *marketing* digitale e dell'*e-fitness*, trovando sempre più ampia diffusione nella vita quotidiana di tutti noi.

b. Fattori psicologici

Tra i numerosi fattori psicologici che entrano in gioco quando pensiamo al possibile effetto delle strategie di influenza, particolare significatività possono assumere alcuni aspetti che riguardano il nostro modo di percepire e interpretare il mondo esterno. In particolare, tra i fattori di cui tenere conto rientrano:

- **bias cognitivi:** il cervello umano è costantemente sottoposto a un eccesso di informazioni che lo portano a sviluppare apposite scorciatoie euristiche che gli consentono di risparmiare tempo, ma possono indurre in errori di valutazione (*bias*). Tra queste, particolare rilevanza assumono i *confirmation bias* che attraverso un effetto c.d. *anchoring*, ci portano a prediligere e valorizzare quelle informazioni che confermano la nostra prospettiva/visione;
- **riconoscimento nella proiezione digitale di sé:** gli esseri umani si proiettano nell'universo digitale attraverso identità multiple (profili, *account*, *avatar*, ecc.) che possono essere anche fortemente differenti dalla realtà in relazione alla possibilità di selezionare una diversa identità da adoperare in differenti contesti. Le ricerche in questo settore confermano come il riconoscimento di sé nella propria identità digitale abbia significativi impatti in termini comportamentali evidenziando, in particolare, come al venir meno del pieno riconoscimento si configuri una maggiore attitudine a fingere/mentire per ottenere un vantaggio (approfondimento in Allegato C);
- **fiducia (*trust*):** particolare rilevanza nel contesto dell'influenza riveste il fattore fiducia, inteso sia come credibilità, attendibilità e affidabilità (*reputation*) che noi riconosciamo a determinati soggetti in funzione di fattori quali ruolo, familiarità, professionalità, modello, sia come riconoscimento della validità dei loro consigli (*advising*). In tal senso, si evidenzia la maggiore propensione alla fiducia nei rapporti tra essere umani che tra essere umano e macchine e, in quest'ultimo caso, all'aumentare dell'accettazione in funzione della vicinanza. Tuttavia, l'evoluzione descritta conferma come, per sopperire a questa propensione umana, si ricorra sempre più a una personalizzazione o prossimità delle macchine (profili *fake* gestiti da bot sui

social media, wearable smart device, umanizzazione e prossimità degli assistenti vocali quali Alexa, Google Assistant, Siri, ecc);

- **memoria emotiva**: il cervello umano apprende attraverso un processo episodico cui vengono associate le emozioni provate. In tal senso, particolarmente significativi sono gli eventi traumatici che, rispetto agli eventi positivi, hanno un potere immediato di indurre la modifica di determinati atteggiamenti e comportamenti allo scopo di preservare l'individuo dal rivivere la stessa esperienza.

c. Fattori sociali

Rispetto alle dinamiche sociali della vita reale, il funzionamento dei *digital media* porta a incoraggiare l'instaurazione di innumerevoli connessioni sociali anche in considerazione del fatto che il numero di amici/*follower* costituisce un fattore di riconoscimento sociale. Tuttavia, come nel mondo reale, anche nell'universo digitale emergono dinamiche sociali che privilegiano alcune relazioni forti rispetto alla moltitudine di relazioni deboli instaurate. In tal senso, le relazioni forti che contribuiscono maggiormente e gli effetti che ne possono discendere, possono essere descritti come segue:

- **relazioni Leader-Follower**: costituiscono il modello di relazione degli *influencer*, ma anche di tutti quei soggetti che, attraverso efficaci strategie comunicative e la creazione di contenuti, riescono a influenzare l'opinione del loro pubblico (*followers*);
- **dinamiche di gruppo**: gli esseri umani sono naturalmente portati a riunirsi in gruppi, pagine, *communities*, ecc. in cui si condividono interessi e nelle quali possono instaurarsi efficaci dinamiche di influenza. In tal senso, la capacità di influenzare un solo soggetto del gruppo può assicurare l'amplificazione dell'effetto all'intera comunità;
- **effetto ingroup-outgroup**: uno dei risvolti correlati alle dinamiche di influenza e rafforzamento delle dinamiche di gruppo è l'instaurarsi dei conflitti *ingroup – outgroup*. In altri termini atteggiamenti positivi, lealtà, fiducia, coesione o favoritismo verso il proprio gruppo di appartenenza (*ingroup love*) che spesso è associato a sentimenti di ostilità sfiducia, pregiudizio, addirittura odio, creazione di stereotipi verso chi non vi appartiene (*outgroup hate*);
- **disimpegno morale selettivo**: il risultato di un insieme di meccanismi psicologici di relazioni personali, comunicazione di massa e categorizzazioni che inducono a commettere, tollerare o fiancheggiare comportamenti moralmente condannabili, disattivando temporaneamente o selettivamente alcune funzioni cognitive-emotive del sistema di autoregolazione morale. Connesso quindi ad una deresponsabilizzazione nel comportamento sociale ed individuale (riscontrato anche in ambito internazionale in contesti legati alla guerra e al terrorismo), amplificati attraverso i *social*, si evidenziano comportamenti di deumanizzazione della vittima, attribuzione della colpa, dislocamento e diffusione di responsabilità, giustificazione morale, etichettamento eufemistico.

3.2 SOCIAL MEDIA E MARKETING

Il successo delle piattaforme di *social media* è stato assicurato dalla possibilità di accesso diretto a una quantità senza precedenti di contenuti e all'interazione con un numero sempre maggiore di utenti. Tuttavia, gli algoritmi di profilazione¹⁰ del *feed*¹¹, sviluppati prevalentemente per fini commerciali, personalizzano l'offerta dei contenuti tenendo conto delle preferenze e degli atteggiamenti degli utenti. In questo sistema, in cui gli utenti prediligono contenuti e informazioni che aderiscono alle loro visioni del mondo, il rischio diretto è che non vengano più offerte informazioni divergenti, dando vita a gruppi polarizzati attorno a narrazioni condivise. Attraverso questi meccanismi, e ancor di più attraverso l'azione di potenziali *influencer*, così come all'interno delle *communities* in rete, si formano delle camere di risonanza (c.d. "*echo chamber*") in cui l'opinione, l'inclinazione politica o la convinzione degli utenti su un tema vengono rafforzate da interazioni ripetute quasi esclusivamente con altri utenti o fonti che hanno tendenze e atteggiamenti simili. I *confirmation bias* – la tendenza a cercare informazioni aderendo a opinioni preesistenti – sono direttamente correlati all'emergere di *echo chamber* sui *social media* e, secondo le dinamiche della polarizzazione di gruppo, queste possono fungere da meccanismo per amplificare un'azione di influenza contribuendo a spostare l'opinione dell'intero gruppo verso posizioni più estreme o radicali.

Parallelamente, l'aumento esponenziale di utenti dei *social media* ha offerto crescenti opportunità per attori economici e relativi modelli di *business*. Sono infatti stati sviluppati strumenti innovativi di **Social Media Marketing** che, attraverso lo sfruttamento dei meccanismi di funzionamento propri dei *digital media*, possono consentire di ottimizzare l'offerta commerciale degli attori economici.

Tali strumenti consentono, attraverso la selezione di una specifica *target audience* (funzione *engage*) – determinata in relazione a differenti parametri (età, sesso, posizione geografica, ecc.) – di effettuare differenti funzioni:

- **monitoring**: nella quale vengono raccolte le informazioni relative all'efficacia dei contenuti/prodotti, attraverso il monitoraggio delle interazioni degli utenti (condivisioni, reazioni, *like*, sentimenti, ecc.);
- **listening**: nella quale vengono identificati e analizzati i modelli di diffusione di un contenuto con evoluzione del sentimento generato e identificazione degli *influencer*, intesi quali attori che contribuiscono alla diffusione/promozione del contenuto influenzando il sentimento correlato.

Inoltre, al fine di comprendere le strutture (gruppi e organizzazioni) sottostanti alla diffusione di contenuti, sono stati sviluppati ulteriori strumenti di **Social Network Analysis** per analizzare e comprendere le dinamiche di interazione dei gruppi sociali al fine di mappare i modelli di relazione, misurare le interazioni ed evidenziare modelli e

¹⁰ Per profilazione si intende l'insieme delle attività di raccolta ed elaborazione dei dati inerenti agli utenti di un servizio, al fine di suddividerli in gruppi a seconda del loro comportamento (segmentazione).

¹¹ Un *feed* è un algoritmo, uno *script*, che permette ad un utente di avere costantemente e automaticamente contenuti aggiornati attraverso un'applicazione.

comportamenti dei gruppi in determinati contesti. Al fine di supportare campagne promozionali di un determinato prodotto o contenuto, sono anche stati sviluppati strumenti che consentono di gestire *account* multipli che concorrono alla diffusione del messaggio voluto, all'atteggiamento del gruppo *target* e all'orientamento del sentimento sottostante.

STRATEGIE DI *MARKETING* IMPIEGATE ANCHE QUALE VEICOLO DI INFLUENZA

Alcune classiche tecniche di *marketing*, già note dagli anni '60 ma ulteriormente raffinate e potenziate tramite algoritmi IA per il loro utilizzo sul mercato digitale, sono:

- **Viral Marketing:** si sfrutta la possibilità offerta dal web di veicolare in maniera massiva un messaggio. Si tratta sostanzialmente del *Word of Mouth* (passaparola) ed è una delle strategie più usate da cellule terroristiche;
- **Effetto *decoy*:** si valuta il costo in base alle scelte che si hanno davanti, non in base ad un reale ragionamento;
- **Effetto di mera esposizione:** si sceglie in base a ciò che si reputa familiare. La ripetizione di parole, concetti o immagini rende questi familiari e quindi più accettabili. È tipico della propaganda;
- **Avversione alla perdita:** il senso di urgenza o di perdita stimola l'azione, la scelta;
- **Effetto inquadramento (*Framing bias*):** la medesima informazione ha effetti diversi a seconda del modo di comunicare gli aspetti positivi o negativi. Una sconfitta non deve essere chiamata «sconfitta»;
- **Effetto Ikea:** partecipare alla creazione di qualcosa (un'idea, un progetto ecc.) gli fa assumere più valore;
- **Ambush marketing:** utilizzare un dato evento e appropriarsi della visibilità offerta per promuovere una certa comunicazione, senza però che ciò sia regolarmente organizzato;
- **Influencer Marketing:** si sfrutta la visibilità di un *influencer* per veicolare un messaggio.

3.3 STRATEGIE DI INFLUENZA

La costruzione delle percezioni sociali e l'inquadramento delle narrazioni possono influenzare il processo decisionale e l'evoluzione del dibattito pubblico, in particolare su argomenti polarizzanti.

Attraverso l'azione combinata dei fattori concorrenti e degli strumenti finora descritti, è possibile sviluppare strategie di influenza diverse in funzione dell'obiettivo e del relativo orizzonte temporale, che possono essere distinte in due categorie principali: disinformazione e persuasione.

a. Disinformazione

La fiducia (nei processi elettorali, nelle istituzioni nazionali, negli alleati, nella classe politica) può diventare l'obiettivo delle strategie di disinformazione perpetrate dai *competitors* che, avvalendosi dei modelli di interazione tra gruppi sociali e delle vulnerabilità proprie dei *digital media*, possono promuovere la diffusione di contenuti finalizzati a generare un determinato effetto e “manipolare” le reazioni e il comportamento di uno specifico gruppo di persone.

Tali strategie possono impiegare robuste campagne di disinformazione ed immensi flussi di *fake news* attraverso la manipolazione di contenuti reali o la creazione artificiale di contenuti quali i *deepfakes*¹² e sfruttando anche la spettacolarizzazione di eventi traumatici per deviare un processo decisionale, indebolire la coesione interna, erodere la fiducia nelle istituzioni democratiche e generare dubbi e indecisione, al fine di perseguire un proprio disegno strategico che svuota di significato elementi identitari della popolazione. Tali strategie sfruttano il modo in cui pensano gli individui e le comunità attraverso l'utilizzo di tecniche di disinformazione e misinformazione. Mentre la disinformazione afferisce alla diffusione deliberata di informazioni false con l'intento di ingannare (*deception*), costituendo quindi un'azione esterna diretta, la misinformazione rientra nel campo della libertà di espressione e si riferisce alla divulgazione inconsapevole o involontaria di contenuti non veritieri inquadrandosi quale azione interna al sistema. Quest'ultima rappresenta un amplificatore dell'azione disinformativa esterna, soprattutto quando eseguita attraverso i *social media*, dove tutti possono condividere liberamente i propri pensieri, e anche i media tradizionali sono chiamati a rispondere ad esigenze di informazione *real time*, e dove si privilegia la tempestività rispetto alla veridicità.

L'obiettivo di tali strategie è il caos, la confusione generata dalla estrema polarizzazione che rallenta fino a immobilizzare l'azione decisionale del soggetto *target* e consente il perseguimento dei propri obiettivi strategici. Le strategie di disinformazione, sfruttando e amplificando le divisioni già esistenti all'interno di un sistema, non possono garantire risultati durevoli nel tempo e, pertanto, hanno solitamente obiettivi di breve-medio termine e vengono prevalentemente usate a livello operativo a supporto di altre azioni (economiche, diplomatiche, militari, ecc.) sia nella fase di preparazione, sia a supporto dell'azione principale.

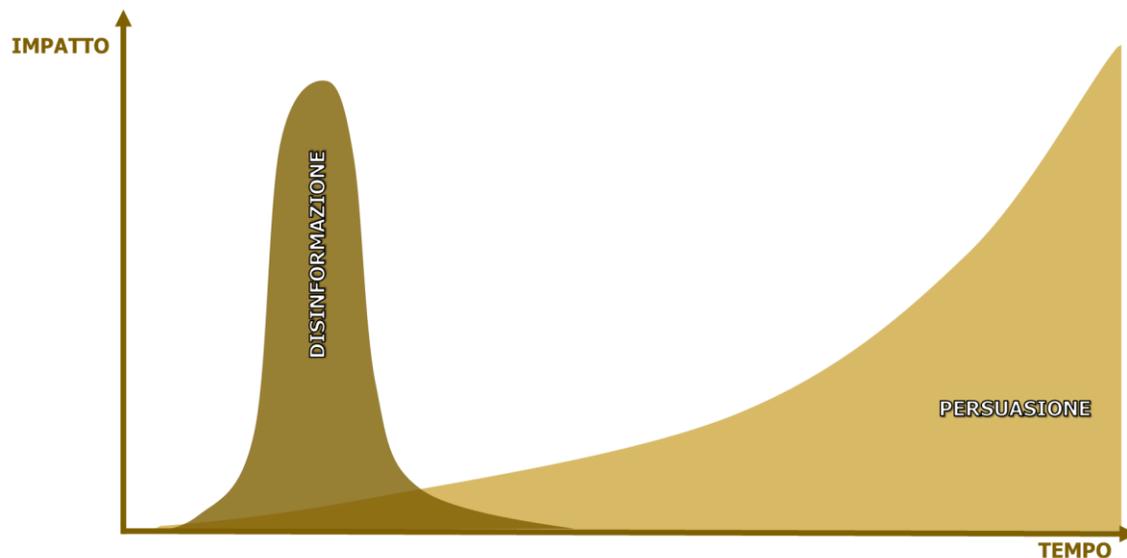
b. Persuasione

Nel contesto di una competizione permanente nella dimensione cognitiva particolare rilevanza riveste la capacità di persuadere un avversario attraverso la possibilità di influenzarne il modo di pensare per fargli scegliere spontaneamente di adottare determinati comportamenti. Questa scelta dell'avversario non avviene nella normale dialettica fra attori politici e seguendo una libera analisi costi-benefici, pur distorta da *bias* cognitivi, ma piuttosto in un contesto di scontro e senza che l'avversario sia consciamente coinvolto in un'interazione con l'attore che adotta la misura di influenza. Anche le strategie di persuasione utilizzano i modelli di interazione tra gruppi sociali e le vulnerabilità proprie dei *digital media*, cui si possono però aggiungere tutti gli ulteriori elementi che impiegano tecnologie interattive di persuasione e che operano su tutti i fattori psicologici e sociali per proporre nuovi modelli comportamentali ad una determinata *target audience* attraverso un'azione costante, positiva e propositiva che può

¹² Contenuti (foto, video e audio) creati grazie a *software* di IA che, partendo da contenuti reali, riescono a modificare o ricreare in modo realistico le caratteristiche e i movimenti di un volto o di un corpo.

anche essere interpretata come semplice proiezione di *soft power*, ma che opera, invece, anche a livello subliminale.

Tali strategie modificano il modo in cui pensano gli individui e le comunità per influenzarne abitudini e comportamenti potendo garantire il conseguimento di risultati duraturi. Hanno solitamente obiettivi di lungo termine, vengono utilizzate prevalentemente a livello strategico e costituiscono l'azione principale che può essere supportata da azioni di supporto (economiche, diplomatiche, industriali, ecc.).



Rappresentazione grafica delle strategie di influenza attraverso l'utilizzo di un diagramma cartesiano sui cui assi vengono riportati l'impatto dell'azione e la persistenza nel tempo degli effetti.

3.4 IL GAMING COME ANTEPRIMA DELLO SPAZIO DIGITALE

L'evoluzione delle dimensioni digitali verso uno spazio immersivo (metaverso¹³) identifica il passaggio da un modello di condivisione di contenuti verso un modello partecipativo che ha le potenzialità di costituire un fattore di amplificazione delle azioni di influenza. La possibilità offerta dall'utilizzo di strumenti di simulazione di vivere un'esperienza virtuale percepibile come reale, la proiezione nello spazio digitale attraverso un *avatar* personalizzabile, la selezione di un differente mondo virtuale in cui immergersi secondo preferenze e valori personali ed in cui interagire con altri soggetti senza alcuna possibilità di distinguere tra individui reali e artificiali, sono tutti fattori che potrebbero contribuire ad amplificare esponenzialmente la portata degli effetti generabili attraverso strategie di influenza e che, oggi, possono già essere parzialmente riscontrati nell'ambiente dei videogiochi (*gaming*).

¹³ Termine coniato da Neal Stephenson nel romanzo "*Cyberpunk Snow Crash*" (1992) per indicare uno spazio virtuale tridimensionale all'interno del quale persone fisiche possono muoversi, condividere e interagire attraverso *avatar* personalizzati. In linea con la visione originale e grazie allo sviluppo tecnologico e agli investimenti privati nel settore, oggi il metaverso, inteso quale fusione tra mondo fisico e virtuale, viene considerato quale verosimile evoluzione futura della rete *internet* globale.

Negli ultimi anni l'universo del *gaming* ha subito una fortissima espansione grazie alla possibilità offerta dallo *streaming*¹⁴. Rispetto alle comunità ristrette che un tempo costituivano l'utenza dei *videogames* e che tendevano ad adottare comportamenti di isolamento per trascorrere molte ore davanti ad uno schermo interagendo con pochi individui, oggi la possibilità di trasmettere *live* le proprie sessioni di gioco e di condividere l'esperienza sia con altri giocatori, sia con un numero crescente di spettatori, ha esteso la portata delle *communities* contribuendo ad accrescerne visibilità ed influenza.

Inoltre, utilizzando strumenti di simulazione particolarmente realistici e guidando l'utente ad effettuare una serie di azioni tramite l'*interactive storytelling*¹⁵, il mondo del *gaming* offre ulteriori possibilità. Solo per citare un esempio, rispetto allo *storytelling* classico che ha una sequenza lineare di eventi dall'inizio alla fine e tempi predefiniti come al cinema, nel mondo dei *videogames* le storie hanno un inizio e una fine, ma l'ordine e la durata degli eventi possono essere modificati secondo la velocità e le azioni dell'utente, omettendo intere sequenze narrative o vivendole seguendo una differente successione (*loop* temporale).

Per le attività di influenza di gruppi di persone e di creazione di forti legami di affiliazione e controllo (modello *leader-follower*) è sempre più evidente l'importanza del ricorso a strumenti di *gamification* (utilizzo di elementi provenienti dai videogiochi, in contesti non ludici) che possano svolgere un ruolo alternativo o sostitutivo per quelle fasi maggiormente complesse della creazione e guida dei gruppi di opinione. Il principale vantaggio del gioco, e conseguentemente degli strumenti di *gaming*, è il coinvolgimento maggiore da parte degli utenti rispetto a qualsiasi altro veicolo di informazione o apprendimento. La *gamification* dei gruppi offre, infatti, dei potenti strumenti per contattare, confrontare e scegliere nello stesso istante migliaia di potenziali utenti afferenti al gruppo, senza essere intrusivi o notati. I videogiochi, soprattutto quelli digitali e *on-line*, portano al loro interno degli strumenti (es. *chat*, tempo di gioco, tempi di reazione, contatti in rete, ecc.) che permettono di analizzare e valutare le competenze e più in generale il profilo degli utenti che vi partecipano, spesso senza che questi nemmeno si accorgano di essere studiati.

Attività come la selezione, indottrinamento e l'affiliazione possono beneficiare molto di più della *gamification* proprio perché il coinvolgimento diventa motivo fondante del rapporto di riconoscimento del "giocatore" verso il gruppo¹⁶. Nel processo di selezione questo stato di coinvolgimento è presente soltanto in misura pertinente alla parte di analisi delle competenze e all'*engagement* dell'utente. In realtà lo strumento dei giochi di per sé non è l'unica modalità con cui si possono sondare le competenze dei potenziali affiliati in modo efficace; è altresì vero che è l'unico che genera un coinvolgimento così elevato da fare in modo che l'utente, mentre gioca, non si senta sotto indagine e si lasci andare nell'esperienza ludica nel modo più naturale possibile. Attraverso la spontaneità si può cercare di capire

¹⁴ Sistema per la trasmissione di segnali audio e video via *Internet*, che permette di ascoltare e visualizzare i segnali provenienti da un *server* via via che questi vengono ricevuti senza dover attendere il *download* completo.

¹⁵ Affabulazione, arte di scrivere o raccontare storie catturando l'attenzione e l'interesse del pubblico.

¹⁶ Andando ad utilizzare le implicazioni studiate da McGonigal (2011) per il coinvolgimento nello stato di *flow* (Csikszentmihalyi, 1990) attraverso il quale si massimizzano le conoscenze apprese e l'obiettivo ricevuto.

quelli che possono essere gli atteggiamenti che una persona poi adotterà nel gruppo, quando gli sarà assegnato un obiettivo reale o semplicemente come condurrà la sua vita quotidiana. Ciò che emerge sull'utilizzo di questo tipo di strumenti nel modo aziendale è, per esempio, la crescita della velocità di *screening* dei profili presentati per la selezione del personale o nella analisi delle competenze dei candidati, grazie ad algoritmi sempre più raffinati afferenti alle logiche del gioco presentato. Alla base di questi sistemi, infatti, vi è una forte strutturazione dell'intera piattaforma con algoritmi estremamente precisi e sessioni di sviluppo molto complesse e strutturate basate su uno *storytelling* di contesto preciso e articolato in grado di analizzare ed evidenziare tutti gli aspetti che si ritengono di interesse. È da sottolineare, inoltre, che sempre più spesso il *target* di riferimento di queste nuove piattaforme di *gaming* è sempre più giovane, proprio perché il linguaggio dei videogiochi si adatta meglio a questo pubblico, ed è quindi più semplice arrivare, per questo tipo di utenza, ad una affiliazione più forte e duratura nel tempo.

Grazie all'utilizzo dell'analisi dei *big data*, dell'Intelligenza Artificiale e delle creazioni di narrazione dedicate ai videogiochi, sono state sviluppate piattaforme di *gaming* estremamente valide, dal punto di vista scientifico, che possono analizzare, tramite l'esperienza ludica, determinate competenze possedute dagli utenti, ritenute importanti dal *leader* della specifica piattaforma. Secondo l'attuale *trend*, si può ipotizzare che in futuro la *gamification* per la creazione di *community* dedicate possa diventare ancora più frequente. L'evoluzione e la diffusione che può prospettarsi per l'applicazione di questi strumenti in ambiti più ampi (es. metaverso) è limitata unicamente dagli alti costi di sviluppo che, al momento, queste piattaforme comportano e che solo le più grandi aziende multinazionali possono sostenere.

3.5 FORME DI CONTRASTO

Nonostante la crescente attenzione posta al tema dell'influenza e gli sforzi per mitigare la portata e gli effetti del fenomeno, le difficoltà di svolgere un'efficace azione di contrasto sono da ricercare principalmente nella natura stessa del terreno in cui tali azioni vengono condotte.

La dimensione digitale degli strumenti di comunicazione e, in particolare, dei *social media* rappresenta per il modello ed i valori occidentali uno spazio pubblico e globale in cui la libertà di espressione del singolo rappresenta un valore democratico irrinunciabile e le possibili forme di controllo statale, a meno di determinate fattispecie giuridiche, costituirebbero una limitazione delle libertà personali. Di contro, gli attori che adottano modelli valoriali concorrenti hanno sviluppato strategie e strumenti sempre più efficaci per sfruttare le caratteristiche di questo spazio e condurre azioni di influenza sempre più pervasive, negando agli avversari la reciprocità dell'azione, mediante l'adozione di modelli di segregazione dello spazio interno dalla rete *internet* globale con fortissime azioni di propaganda interna, lo sviluppo di reti sovrane controllate (emblematico il caso delle reti cinesi come il recente tentativo della Federazione Russa di attivare la propria rete RuNet),

e/o l'utilizzo esclusivo di alcune piattaforme nazionali (pur essendo di proprietà cinese, TikTok è vietato all'interno del Paese¹⁷).

Parallelamente, tale spazio è stato prevalente colonizzato da attori privati quali multinazionali e *corporation* che hanno sviluppato sistemi e piattaforme per finalità prevalentemente commerciali. La diffusione e la portata del fenomeno hanno via via portato gli Stati a compiere innumerevoli sforzi per regolamentare questo spazio, tentando di imporre restrizioni e limitazioni agli attori privati (es. *General Data Protection Regulation-GDPR* dell'Unione Europea) e incontrando fortissime resistenze. Dal lato opposto, il modello di fusione civile-militare cinese o il controllo statale russo hanno consentito di asservire gli attori privati alle finalità strategiche nazionali ricorrendo anche a forme di co-finanziamento statale che potrebbero aver già consentito di raggiungere una superiorità tecnologica in taluni settori quali quello delle tecnologie interattive di persuasione. Solo per citare un esempio, mentre l'algoritmo di profilazione di Facebook richiede circa 200 interazioni attive (*likes*) dell'utente per effettuarne la profilazione, quello di TikTok potrebbe già essere in grado di effettuare la completa profilazione in soli 20 minuti e attraverso la sola fruizione passiva di contenuti.

Le caratteristiche descritte contribuiscono a giustificare gli enormi sforzi attualmente in corso per contrastare il fenomeno della disinformazione e la portata limitata di tali azioni. Nonostante la crescente attenzione del comparto *Intelligence*, oggi il contrasto del fenomeno su larga scala è prevalentemente effettuato attraverso azioni di *fact-checking* che mirano a verificare le informazioni per poi chiederne la rimozione dalla rete attraverso gli strumenti di moderazione delle piattaforme (*debunking*¹⁸). Tali azioni vengono oggi condotte sia a livello privato da cittadini organizzati¹⁹, che a livello nazionale²⁰ e sovranazionale²¹. Tuttavia, l'eliminazione dei contenuti non riduce l'effetto sull'avvenuta esposizione e può comunque generare effetti significativi sull'*audience*. In tal senso, si stanno sviluppando strategie e strumenti di *pre-bunking*²² che, attraverso tecniche che favoriscano la resistenza preventiva, rappresentano lo strumento più efficace a limitare l'estensione della disinformazione.

La proliferazione del fenomeno della disinformazione durante l'emergenza pandemica e, ancor di più, con l'apertura del conflitto russo-ucraino ha contribuito a responsabilizzare talune piattaforme che hanno avviato importanti progetti per lo sviluppo di nuovi strumenti

¹⁷ La versione più diffusa di Tik Tok risulta non disponibile alla popolazione cinese al pari di tutti gli altri *social* occidentali. La versione interna, denominata Douyin, risulta infatti graficamente simile ma molto differente nel funzionamento e totalmente segregata rispetto a quella esterna.

¹⁸ Confutazione di notizie o affermazioni false o antiscientifiche, spesso frutto di credenze, ipotesi, convinzioni, teorie ricevute e trasmesse in modo acritico.

¹⁹ Quale, ad esempio, la "legione degli elfi" in Lituania.

²⁰ Il 1 gennaio 2022 è stata costituita in Svezia l'Agenzia per la Difesa Psicologica, prima agenzia governativa dedicata al contrasto della disinformazione.

²¹ In tal senso, particolarmente rilevante è il progetto europeo dell'*European Digital Media Observatory* (guidata dall'*European University Institute* di Firenze) e degli 8 *hub* regionali (tra i quali l'*Italian Digital Media Observatory* guidato dalla LUISS) che rientrano nel Piano di contrasto alla disinformazione dell'Unione Europea.

²² Gli strumenti oggi disponibili sono costituiti da simulazioni (es. *Bad News Game*) che permettono di comprendere le dinamiche della disinformazione – NATO SG 278 - *Cognitive Augmentation for Military Applications*.

finalizzati all'identificazione e rimozione di contenuti falsi o manipolati²³. In tal senso, risulta evidente come il ruolo degli *stakeholders* privati sia potenzialmente determinante nell'efficacia delle azioni di contrasto e pertanto andrà ricercata una sempre maggiore collaborazione con le piattaforme che si renderanno disponibili ad adottare strumenti di mitigazione del fenomeno, contribuendo, potenzialmente, a identificare le piattaforme malevoli. La sola imposizione di regole particolarmente stringenti a cui non tutte le piattaforme potrebbero adeguarsi o la mancanza di dialogo e cooperazione potrebbero contribuire all'inefficacia delle azioni di contrasto e, all'esacerbarsi della competizione, sfociare in tentativi di esercizio della sovranità sulle reti e di controllo statale che andrebbero contro i valori democratici del mondo occidentale contribuendo a spostare il nostro modello verso quello proprio dei *competitors*.

3.6 INQUADRAMENTO GIURIDICO

a. L'uso della forza e le attività di influenza

La capacità di influenzare il cervello umano si caratterizza per la possibilità di agire sul nesso di causalità azione-evento, contribuendo alla produzione di effetti specifici o, in taluni casi, influenzando su quelli già prodotti.

Gli strumenti di influenza, quindi, rappresentano una forma di supporto alle operazioni che, con lo sviluppo tecnologico, assume un ruolo essenziale nel *warfare* moderno ed è oggetto di continuo dibattito in ambito NATO e UE in merito agli aspetti giuridici ed etici coinvolti.

Sotto il profilo giuridico, gli strumenti di influenza vanno analizzati alla luce del dettato Costituzionale²⁴ e dell'Art. 2 (4) della Carta della Nazioni Unite che afferma, in via generale, che gli Stati membri devono “*astenersi nelle loro relazioni internazionali dalla minaccia o dall'uso della forza*”.

In tale quadro, occorre definire in modo chiaro i margini operativi nell'esercizio delle attività di influenza, restando impregiudicato il limite posto dall'ordinamento giuridico nazionale e internazionale: *self-defense* di cui all'Art. 51²⁵ dello Statuto delle Nazioni Unite o, comunque, uso legittimo della forza di cui al Capo VII dello stesso Statuto.

E' possibile considerare un'azione di influenza come “uso della forza” ricorrendo al cosiddetto criterio dell'*equivalenza cinetica* (spesso utilizzato in ambito *cyber*²⁶) soltanto

²³ <https://jigsaw.google.com/the-current/disinformation/>

²⁴ Art. 11 Cost.: “*L'Italia ripudia la guerra come strumento di offesa alla libertà degli altri popoli e come mezzo di risoluzione delle controversie internazionali; consente, in condizioni di parità con gli altri Stati, alle limitazioni di sovranità necessarie ad un ordinamento che assicuri la pace e la giustizia fra le Nazioni; promuove e favorisce le organizzazioni internazionali rivolte a tale scopo*”.

²⁵ Articolo 51 Carta delle Nazioni Unite: “*Nessuna disposizione del presente Statuto pregiudica il diritto naturale di autotutela individuale o collettiva, nel caso che abbia luogo un attacco armato contro un Membro delle Nazioni Unite, fintantoché il Consiglio di Sicurezza non abbia preso le misure necessarie per mantenere la pace e la sicurezza internazionale. Le misure prese da Membri nell'esercizio di questo diritto di autotutela sono immediatamente portate a conoscenza del Consiglio di Sicurezza e non pregiudicano in alcun modo il potere e il compito spettanti, secondo il presente Statuto, al Consiglio di Sicurezza, di intraprendere in qualsiasi momento quell'azione che esso ritenga necessaria per mantenere o ristabilire la pace e la sicurezza internazionale*”.

²⁶ Il dominio cibernetico, trasversale agli altri domini, presenta caratteristiche analoghe in termini di difficoltà nell'individuare spazio, tempo ed effetti delle operazioni.

quando le dimensioni e gli effetti prodotti sono paragonabili a quelli di un uso della forza convenzionale tipica, appunto, delle operazioni cinetiche²⁷, con conseguente danno fisico a cose, lesioni a persone o perdita di vite umane²⁸.

Tutte le attività che si mantengono, per livello di efficacia, al di sotto di tale soglia (campagne informative, *countering misinformation*, ecc.) e che rientrano nell'alveo delle azioni finalizzate a tutelare le Forze, sono consentite in quanto:

- non costituiscono azioni vietate ai sensi del citato art. 2 (4);
- non rappresentano violazione dei principi ordinamentali nazionali e internazionali.

b. I profili giuridici della reazione

Tradizionalmente, la risposta a campagne informative o attività idonee a influenzare il pensiero delle masse trova una naturale definizione nel concetto di legittima difesa quando si identifica in una reazione proporzionata e temporalmente successiva ad un atto idoneo a produrre effetti analoghi a quelli derivanti dall'uso della forza che raggiunge il livello di attacco armato.

Tale reazione, però, incontra specifiche limitazioni dettate dall'esigenza di evitare di incorrere in eccessi contrari ai principi del diritto internazionale.

Un primo elemento da stabilire è l'*attribution*²⁹ delle attività di influenza ad uno Stato o a un soggetto che al suo interno agisce in nome e per conto dello stesso. Un ulteriore aspetto, per certi versi il più controverso, riguarda il legame azione-reazione. In analogia a quanto avviene nel dominio cibernetico, esistono circostanze all'interno delle attività di influenza per cui la successione temporale tra azione e reazione è difficile da inquadrare in modo chiaro, atteso che gli effetti non si sviluppano necessariamente in concomitanza con l'azione.

In tali casi, per spingersi sino al limite del concetto di *self-defence* con l'intento di tutelare gli interessi nazionali e dei contingenti militari impiegato in teatro operativo, occorre considerare tre aspetti essenziali³⁰ in sede di valutazione della legittimità dell'autodifesa (vds. *Caroline Test*³¹):

²⁷ È importante sottolineare la necessità di distinguere tra le forme più gravi di uso della forza, che, costituendo un attacco armato, legittimano il ricorso alla legittima difesa, dalle forme meno gravi (sul punto CIG, *Attività militari e paramilitari degli Stati Uniti in Nicaragua e contro il Nicaragua*, merito, 27 giugno 1986, § 191, in *ICJ Rep.*, 1986, 101), quali, ad es., incidenti di frontiera di minore entità che, pur costituendo una violazione degli obblighi assunti nelle relazioni internazionali, non sono assimilabili ad un attacco armato.

²⁸ Cfr., sul punto, Repubblica Italiana, *Italian Position Paper On 'International Law And Cyberspace'*, 4 novembre 2021, 8, in *www.esteri.it*.

²⁹ Cfr. AA. VV., *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Rule 15.

³⁰ Quale uso della forza anticipato davanti a un attacco imminente o alla minaccia di esso, qualora esso derivi da un atto di coercizione volto a privare un popolo del diritto all'autodeterminazione e pur non costituendo espressamente aggressione (*ICJ, Nicaragua-Stati Uniti, Reports* 1986, pag. 101).

³¹ H. H. DINNISS, *Cyber Warfare and the Laws of War*, 102-104; H. JONES, *To the Webster-Ashburton Treaty: A Study in Anglo-American Relations*, Chapel Hill, 1977, 1783 ss. Il noto episodio si inquadra nell'insurrezione del Canada contro la Gran Bretagna e si riferisce all'attacco che avvenne nella notte del 29 dicembre 1837 ad opera di alcuni soldati britannici che dal Canada penetrarono in territorio statunitense distruggendo la nave *Caroline* ancorata sulle rive del Niagara da dove essa riforniva di viveri e armi un'isola occupata da canadesi e statunitensi. Nello scambio di lettere tra gli Ambasciatori degli Stati Uniti e della Gran Bretagna rimane celebre la frase del Segretario di Stato americano Daniel Webster che precisò i limiti in cui era giustificato l'uso della forza in legittima difesa per cui andava

- la necessità, ovvero l'impossibilità di perseguire, considerate le condizioni, vie alternative per risolvere politicamente o diplomaticamente la controversia;
- la proporzionalità, intesa come risposta commisurata alla minaccia;
- l'imminenza, per cui, esemplificando, uno Stato ha fondato motivo di ritenere di essere in procinto di essere attaccato.

Tale valutazione, ammette un'azione di risposta legittima se esercitata entro l'ultima finestra utile prima di perdere definitivamente la possibilità di difendersi efficacemente³².

c. Il rispetto del Diritto Internazionale Umanitario

Le attività di influenza in un contesto operativo devono, anche in assenza di conflitto armato internazionale, conformarsi a principi consuetudinari del Diritto Internazionale Umanitario sanciti dal diritto di Ginevra, quali distinzione, umanità, proporzionalità, precauzione e necessità militare. In particolare, nella scelta di mezzi e metodi di combattimento³³ devono essere evitati quelli che possono arrecare mali superflui o sofferenze inutili. Nella condotta delle operazioni di influenza è consentito lo stratagemma³⁴, purché non sfoci in illegittimi atti di perfidia³⁵.

dimostrata «a necessity of self-defence instant, overwhelming, leaving no choice on means and no moment for deliberation»; Cfr. *British and Foreign State Papers, 1840-1841*, XXIX, Londra, 1857, 1138.

³² Cfr. AA. VV., *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Rule 73, punto 4.

³³ Art. 35 del I P.A. alle Convenzioni di Ginevra del 1977: “In ogni conflitto armato, il diritto delle Parti in conflitto di scegliere metodi e mezzi di guerra non è illimitato. E' vietato l'impiego di armi, proiettili e sostanze nonché metodi di guerra capaci di causare mali superflui o sofferenze inutili. E' vietato l'impiego di metodi o mezzi di guerra concepiti con lo scopo di provocare, o dai quali ci si può attendere che provochino, danni estesi, durevoli e gravi all'ambiente naturale”.

³⁴ Art. 37.2 del I P.A. alle Convenzioni di Ginevra del 1977: costituiscono stratagemmi “gli atti che hanno lo scopo di indurre in errore un avversario, o di fargli commettere imprudenze, ma che non violano alcuna regola del diritto internazionale applicabile nei conflitti armati e che, non facendo appello alla buona fede dell'avversario circa la protezione prevista da detto diritto, non sono perfidi”.

³⁵ Art. 37.1 del I P.A. alle Convenzioni di Ginevra del 1977: costituiscono perfidia “gli atti che fanno appello, con l'intenzione di ingannarla, alla buona fede di un avversario per fargli credere che ha il diritto di ricevere o l'obbligo di accordare la protezione prevista dalle regole del diritto internazionale applicabile nei conflitti armati”.

CAPITOLO 4

NUOVI STRUMENTI DI INTERFERENZA



Plasmato da milioni di anni di evoluzione, il cervello umano ha raggiunto una complessità senza pari e lo studio del suo funzionamento presenta crescenti sfide alla scienza, nonché potenziali sorgenti di rischio, anche in considerazione delle ricadute sociali. Infatti, le scoperte nell'ambito delle neuroscienze e delle neurotecnologie possono rappresentare sia un bene comune se usate eticamente, sia un pericolo se sfruttate per un uso malevolo vista la corrispondente possibilità di modulare i processi cognitivi. In tal senso, la *leadership* dovrà sempre più includere, nella valutazione e gestione dei rischi correlati alla dimensione cognitiva, la "*neurosecurity*".

A riprova dell'interesse globale crescente nella *neurosecurity*, gli stanziamenti pubblici in progetti riguardanti le neuroscienze e le neurotecnologie sono sempre più ingenti e numerosi, soprattutto per approfondire le funzioni cognitive principali come l'empatia, la coscienza e il linguaggio, nonché i meccanismi patogeni e gli approcci per intervenire sui disagi mentali.

Le traiettorie di evoluzione di questi studi avanzati, che hanno permesso di sviluppare procedure e terapie per curare malattie e patologie, costituiscono nuove fonti di minaccia a causa del potenziale uso malevolo delle neuroscienze e delle neurotecnologie da parte di attori statuali o non statuali. Le attività di ricerca e sviluppo in tali settori rientrano pertanto a pieno titolo tra le attività che possono dare luogo ad "aree grigie" di impiego e costituire un elemento di *leverage* geopolitico e geoeconomico dei vari attori, ad esempio manipolando i mercati dell'*healthcare* e delle biotecnologie per forzare mutamenti nel *balance of power*.

4.1 POTENZIALI APPLICAZIONI MILITARI

Gli sviluppi nel campo delle neuroscienze e delle neurotecnologie sono così maturi da ipotizzarne il loro utilizzo per applicazioni volte a potenziare e/o degradare le capacità delle forze militari incidendo sulla *performance* fisica, cognitiva, emotiva e/o comportamentale, aumentando, di conseguenza, il proprio vantaggio competitivo nell'ambito del campo di battaglia.

Il tentativo di perseguire una superiorità cognitiva può infatti esprimersi attraverso il **miglioramento** (*enhancement*) di talune abilità cognitive quali la percezione, l'attenzione, o la memoria. In particolare, gli strumenti di interferenza possono essere impiegati per fini di **potenziamento** - accelerando o consolidando specifiche abilità cognitive individuali o le *performance* di gruppo oltre le capacità di picco – ovvero di **ottimizzazione**, mantenendo o conservando delle capacità di picco a fronte di eventi avversi. Gli strumenti di interferenza utilizzati a fini di *enhancement* possono interferire sia con i processi biochimici del cervello attraverso il ricorso ad agenti farmacologici, sia con i processi elettrici del cervello principalmente tramite tecnologie e tecniche di stimolazione cerebrale. Parallelamente, gli sviluppi nel settore permettono di ipotizzare anche l'utilizzo di alcune applicazioni a fini di **degradazione** di abilità cognitive dell'avversario. Tali strumenti di interferenza, che potrebbero configurarsi quali vere e proprie “*neuroweapons*”, possono includere agenti neuro-farmacologici, bioregolatori chimici e sistemi di stimolazione cerebrale, ma anche sistemi ad energia diretta progettati per colpire un soggetto bersaglio, attraverso impulsi ottici, acustici o elettrici che agiscono sul sistema nervoso.

a. Agenti che agiscono sui processi biochimici del cervello

L'uso di principi attivi in ambito bellico non rappresenta un vero elemento di novità. L'impiego di sostanze che inducono alterazioni del sistema cognitivo dei combattenti è, infatti, un fenomeno storicamente noto; i guerrieri vichinghi, ad esempio, assumevano sostanze stupefacenti per entrare in una sorta di *trance* in modo da assumere una postura particolarmente feroce ed innalzare la soglia del dolore, mentre i soldati greci e romani preferivano lanciarsi contro gli avversari in stato di ebbrezza al fine di innalzare la soglia del dolore e inibire la paura³⁶; nel corso del secondo conflitto mondiale, si fece invece uso del farmaco Pervitin[®], una metanfetamina che innalza la soglia del dolore, inducendo stati di euforia e l'abbandono di ogni sorta di inibizione.

Più di recente, nel teatro siriano sono state rinvenute pillole denominate Captagon[®], contenenti un insieme di sostanze stimolanti/psicoattive, tra cui la fenetilina, composto amfetaminico. Questo farmaco è stato utilizzato dai combattenti dell'ISIS per stimolare comportamenti energici e improntati al coraggio, mitigando il dolore e consentendo a questi di restare svegli per giorni.³⁷

³⁶ L'usanza di miscelare vino all'acqua della borraccia sarebbe stata mantenuta dai soldati francesi fino agli 'anni '30 del Novecento.

³⁷ Nel 2018, una formazione alleata con il *Free Syrian Army*, Maghawir al-Thawra, ha rivenuto più di 300mila pillole di Captagon in un'operazione contro lo Stato Islamico nei pressi del confine tra Siria e Iraq.

Oggi, per migliorare le capacità cognitive, fisiche o emotive dei soldati, al fine di garantire migliori capacità di sopravvivenza oltre che maggiori possibilità di successo della missione, esistono molte possibilità tra cui soluzioni farmacologiche e alimentari³⁸. Nel contesto militare, la modulazione degli attributi del soldato tra cui la forza, la capacità mentale, il recupero, la resistenza alla fatica e la capacità di guarigione, assume un'importanza assoluta nel confronto con l'avversario in qualsiasi dominio.

Per il raggiungimento di tali scopi l'approccio farmacologico fornisce innumerevoli possibilità vista la gamma di effetti prodotti dai principi attivi che compongono i farmaci, o le loro associazioni. Infatti, oltre alle indicazioni terapeutiche autorizzate, i farmaci possono essere impiegati in regime di *off label*, ossia per finalità diverse da quelle autorizzate, oppure esaltando i loro effetti collaterali se somministrati in associazione. Inoltre, lo sviluppo di specifiche ricerche sull'ossitocina e sul suo ruolo nei comportamenti sociali indica ciò che potrebbe avere luogo in relazione ad altri neurotrasmettitori che non sono stati ancora oggetto di studio. Molte delle reti neurali e la loro modulazione da parte di bioregolatori chimici che sottendono al nostro comportamento saranno sempre di più oggetto di comprensione ma, in prospettiva, anche di manipolazione, non necessariamente per applicazioni civili.

ESEMPI DI FARMACI CON IMPIEGO “OFF LABEL” E/O ASSOCIAZIONE DI FARMACI CHE POSSONO GENERARE EFFETTI COGNITIVI

Farmaci impiegati per il trattamento di malattie neurodegenerative, come il Donezepil[®]; ***Inibitori della colinesterasi***, impiegati per il potenziamento cognitivo, incidendo sull'elaborazione delle informazioni oltre che sulla memoria spaziale e di lavoro;

Farmaci impiegati per il trattamento della narcolessia, come il Modafinil[®], sperimentato anche in contesti militari al fine di sostenere il personale nei cicli sonno-veglia

Farmaci analgesico oppioidi ad azione centrale, come il Tramadolo[®] che, se associato a farmaci serotoninergici, provoca la sindrome serotoninergica *

Farmaci anticonvulsivanti per il trattamento dell'epilessia, impiegati per ridurre la durata di azione dei farmaci oppioidi ad azione centrale

* Sindrome caratterizzata da stato mentale alterato (come confusione, agitazione, irrequietezza, eccitazione, euforia, insonnia, allucinazioni, e coma).

³⁸ Ad esempio, l'assunzione di funghi o piante che contengono sostanze allucinogene, come il fungo psilocibe, contenente la psilocibina oppure la pianta peyote, contenente mescalina.

b. Dispositivi che agiscono sui processi elettrici del cervello

I dispositivi di stimolazione cerebrale rientrano tra i potenziali strumenti di interferenza utilizzabili in ambito militare per la modulazione del sistema nervoso. L'applicazione invasiva o meno di deboli correnti elettriche indirizzate a zone ben definite del sistema nervoso centrale genera attività elettrica neuronale con una conseguente modifica transitoria nella trasmissione dei segnali generati dai neuroni per comunicare tra loro. Questa attività è nota e stratificata nel tempo per scopi di ricerca sulle funzioni cerebrali o per ottenere un beneficio terapeutico in talune disfunzioni sensoriali, patologie neurologiche e psichiatriche i cui sintomi non sono curabili con i soli farmaci.

Le procedure invasive prevedono un intervento chirurgico per il posizionamento di elettrodi intracerebrali, come avviene con la stimolazione cerebrale profonda (*Deep Brain Stimulation* - DBS) per fini terapeutici. Le procedure meno invasive, invece, attualmente usate in ambito di ricerca, iniziano ad essere applicate anche per il trattamento di talune patologie psichiatriche e neurologiche e come supporto per alcuni trattamenti riabilitativi. Tali procedure comprendono la stimolazione magnetica transcranica (*Transcranial Magnetic Stimulation* - TMS), quella elettrica a correnti dirette (*transcranial Direct Current Stimulation* - tDCS), quella elettrica a corrente alternata (*transcranial Alternating Current Stimulation* - tACS) e quella a rumore casuale (*transcranial Random Noise Stimulation* - tRNS). Un'altra tecnica non invasiva di stimolazione cerebrale quale quella ad ultrasuoni potrebbe offrire alcuni benefici sulla stimolazione cerebrale profonda (DBS). Gli ultrasuoni possono essere generati da dispositivi impiantati in un casco ma, qualora azionati, potenzialmente in grado anche di danneggiare i tessuti racchiusi nel casco stesso con conseguente danno al sistema nervoso centrale, anche irreversibile.

La stimolazione magnetica transcranica (TMS) ha giovato ad alcuni pazienti gravemente depressi, portando a chiedersi se il campo elettromagnetico che produce possa essere utilizzato non solo come terapia, ma anche per il potenziamento cognitivo (*neuro-enhancement*). Tale tipologia di stimolazione potrebbe portare i soggetti con una funzione cognitiva statisticamente e fisiologicamente normale ad un livello intellettuale superiore, ma solo per brevi periodi. Gli effetti della TMS sul cervello sono pertanto altamente transitori e anche con interventi di TMS ad alta frequenza, gli effetti neurali sembrano essere limitati a circa un'ora dopo la stimolazione.³⁹ Tuttavia, qualora sia combinata con l'implementazione di specifici programmi di *training*, la TMS ha dimostrato di poter produrre effetti di più lunga durata in termini di mesi.

La tecnica di stimolazione cerebrale a corrente alternata (tACS), sulla base dei risultati di ricerche recenti, può essere adattata per migliorare la memoria a lungo e/o breve termine, con benefici che sembrano avere una durata più prolungata, fornendo evidenze

³⁹ Cfr. NATO STO HFM-311 on *Cognitive Neuroenhancement: Techniques and Technology* - NATO Science and Technology Organization, "Neuroenhancement in Military Personnel: Conceptual and Methodological Promises and Challenges", 2022, <https://apps.dtic.mil/sti/pdfs/AD1159590.pdf>.

per la prima volta che questo tipo di stimolazione può produrre effetti duraturi sulla memoria umana.⁴⁰

La stimolazione cerebrale a correnti dirette (tDCS), che ha mostrato potenzialità anche per incrementare l'intelligenza fluida ossia la capacità di rispondere adeguatamente a situazioni nuove, non appare invece esente da effetti avversi, inclusi quelli associati ad un suo uso prolungato, tuttora non pienamente compresi. Talune ricerche indicano che i soggetti sottoposti a tDCS hanno accusato cambiamenti temporanei di umore, comportamento e personalità, confermando che in circostanze in cui effetti avversi possono inficiare le capacità del personale militare di assolvere le proprie attività, il potenziale capacitivo dell'individuo o dell'unità potrebbe essere esposto a rischi. L'induzione di cambiamenti comportamentali con il ricorso a tali neurotecnologie⁴¹ potrebbe potenzialmente generare interesse per un loro impiego malevolo.

La stimolazione cerebrale non invasiva (elettrica e magnetica) dimostra di avere delle potenzialità nella prospettiva sia di accelerare le attività di *training* del soldato, sia di ottimizzarne e potenziarne le abilità cognitive. Queste applicazioni, che non comportano particolari problematiche di natura logistica, potrebbero riscuotere interesse anche per un utilizzo militare nella misura in cui tendono a migliorare un certo numero di aspetti cognitivi, tra i quali proprio le facoltà mnesiche, la funzionalità dei canali percettivi nonché l'apprendimento di un'ampia gamma di abilità cognitive (*accelerated learning*). In questo ultimo caso, la finalità sarebbe di ridurre i costi e la durata delle attività di *training*.

Inoltre, la stimolazione cerebrale rappresenta un campo di ricerca scientifica in crescita esponenziale. Questa rivestirà un ruolo sempre più rilevante, anche nella considerazione che l'ambito e le finalità di applicazione non sono ancora regolati da alcuna normativa e che, anche a causa della differente prospettiva etico-giuridica tra i differenti attori, potrebbe portare a sviluppi di tipo asimmetrico.

Un ulteriore fattore di criticità è rappresentato dalla diffusione sul libero mercato di *devices* di stimolazione cerebrale di tipo *do-it-yourself* (DIY) che ne consentono un utilizzo senza alcuna supervisione. In taluni casi, le ripercussioni ipotizzabili sul personale militare, nelle circostanze in cui si riscontrasse una propensione a fare un uso non supervisionato di apparecchiature realizzate in ambiente domestico o acquisite *online*, riguardano la possibile esposizione a rischi di sicurezza per la salute, soprattutto nella forma di effetti collaterali o imprevisti.

⁴⁰ Cfr. Jessica Hamzelou, "La stimolazione cerebrale migliora la memoria degli anziani", MIT Technology Review, ottobre 2022, <https://www.technologyreview.it/la-stimolazione-cerebrale-puo-migliorare-la-memoria-delle-persone-anziane/>; Grover, S., Wen, W., Viswanathan, V., Gill, C. T., & Reinhart, R. M., "Long-lasting, dissociable improvements in working memory and long-term memory in older adults with repetitive neuromodulation". Nature Neuroscience, 2022, <https://www.nature.com/articles/s41593-022-01132-3>.

⁴¹ Anche la stimolazione cerebrale profonda (DBS) potrebbe cambiare la personalità dei soggetti in modi che non sono ancora pienamente compresi, anche spingendo a comportamenti potenzialmente pericolosi, come crescente impulsività e aggressività e ipersessualità. Cfr. Jonathan D. Moreno, Jay Schulkin, "The Brain in Context: A Pragmatic Guide to Neuroscience", Columbia University Press, 2019.

c. Sistemi a energia diretta

Tra gli strumenti di interferenza, sulla base di alcune ipotesi emerse in relazione a circostanze specifiche che hanno coinvolto personale diplomatico occidentale (la cosiddetta “Sindrome dell’Avana”⁴²), possono essere annoverati anche i c.d. sistemi ad energia diretta. Alle microonde pulsate al di sopra di specifiche soglie di energia sono, infatti, stati attribuiti danni cerebrali in taluni modelli animali. Anche se il reale meccanismo fisico che ne sarebbe alla base non è ancora pienamente compreso, le implicazioni cliniche di tali danni restano un tema controverso. In particolare, un *report* pubblicato nel 2020 della *National Academy of Sciences*, pur esprimendo prudenza data la mancanza di evidenze scientifiche, prende le mosse dagli esiti di accertamenti diagnostici condotti sui soggetti che hanno manifestato la “Sindrome dell’Avana” e ipotizza anche il possibile uso di sistemi ad energia diretta ritenendo i sintomi riscontrati compatibili con effetti generati da sistemi a radiofrequenza⁴³.

d. Ulteriori applicazioni combinate

La possibilità che i soldati non controllino più pienamente il proprio comportamento individuale a causa di uno stato cognitivo alterato in seguito all’assunzione di sostanze chimiche è una variabile di potenziale primaria importanza nello sviluppo di alcune alternative tecnologie di *enhancement*, in particolare nel caso in cui queste fossero oggetto di *hacking* da parte dell’avversario. Il riferimento è alla possibile combinazione di farmaci con tecnologie di neurostimolazione e realtà virtuale immersiva a cui si potrebbe ricorrere per finalità addestrative. In questo caso, l’effetto di un’azione ostile potrebbe aumentare il disorientamento cognitivo del soggetto ed amplificare l’esperienza immersiva con conseguente alterazione del comportamento, al punto da stimolare i processi di apprendimento e di neuroplasticità, già utilizzati nell’ambito degli interventi terapeutici e neuro-riabilitativi. Si segnala un’attenzione crescente alla possibile integrazione nell’esperienza virtuale di farmaci allucinogeni, sostanze psichedeliche e psicoattive come la psilocibina, che coincide con il recente aumento di interesse scientifico per le interazioni tra tecnologia, psicofarmacologia e salute mentale.

⁴² La cosiddetta “Sindrome dell’Avana” è una patologia riscontrata in funzionari dell’Ambasciata americana prima a Cuba (2016-2017), poi presso il Consolato degli Stati Uniti a Guangzhou in Cina (2017) e nuovamente nell’estate del 2021 in differenti località (Ginevra, Vienna, Parigi, Russia, Germania, Europa dell’est, Colombia e Washington D.C.). Alla sindrome sono associati disturbi quali anomale percezioni sensoriali e cognitive associate a sintomi come il ronzio auricolare, vertigini, spossatezza, nausea e mal di testa che potrebbero essere dovuti a una disfunzione vestibolare e che evidenziano la successiva comparsa di un *deficit* cognitivo. Cfr. Nicholas Davis, *What is Havana Syndrome?*, American University, <https://www.american.edu/sis/centers/security-technology/havana-syndrome.cfm> (2021); The Washington Post, *Scientists and doctors zap theory that microwave weapon injured Cuba diplomats*, https://www.washingtonpost.com/national/health-science/scientists-and-doctors-zap-theory-that-microwave-weapon-injured-cuba-diplomats/2018/09/06/aa51dcd0-b142-11e8-9a6a-565d92a3585d_story.html (2018).

⁴³ Cfr. National Academies of Sciences, *An Assessment of Illness in U.S. Government Employees and Their Families at Overseas Embassies* (2020), <https://nap.nationalacademies.org/catalog/25889/an-assessment-of-illness-in-us-government-employees-and-their-families-at-overseas-embassies>.

4.2 ASPETTI ETICO-GIURIDICI

L'impiego di agenti farmacologici e dispositivi neurotecnologici potrebbero contribuire a potenziare le *skills* del personale militare accelerando il *training* e migliorando il livello di efficacia e prontezza operativa. Tuttavia, le medesime tecnologie tese ad assicurare un *enhancement* delle performance umane potrebbero essere utilizzate per degradarle modificando selettivamente taluni parametri (ad esempio, la polarità di stimolazione, l'intensità, la frequenza ovvero la durata), aprendo importanti quesiti di ordine etico e giuridico.

Oltre alle questioni etiche e giuridiche generali valide per tutti i sistemi, l'interferenza con i processi biochimici del cervello attraverso l'assunzione di farmaci solleva ulteriori timori per le possibili implicazioni in termini di sicurezza della salute, a causa delle reazioni avverse di breve, medio e lungo termine. Nella fattispecie, l'interrogativo secondo il quale può essere considerato legittimo somministrare farmaci a individui sani nell'ambito dell'organizzazione militare può essere ricondotto quasi esclusivamente a circostanze eccezionali di estremo rischio per il soldato ovvero di assoluta necessità di accelerare il suo recupero psico-fisico in conseguenza dell'assolvimento di specifici *task* operativi⁴⁴.

Da un punto di vista etico, tuttavia, emerge la necessità di interrogarsi circa le possibili conseguenze, derivanti dall'impiego di agenti farmacologici, sulla resistenza e percezione del dolore da parte dell'individuo, nonché sull'assenza di emotività. Dato che l'utilizzo di tali strumenti dovrebbe essere finalizzato a migliorare la resistenza psico-fisica, la capacità di recupero e la velocità di guarigione, ci si chiede cosa accadrebbe al corpo umano qualora in caso di impiego protratto non percepisse gradualmente stanchezza o dolore, con il conseguente rischio che, in assenza di segnali metabolici interni, l'operatore possa andare incontro ad un crollo immediato di capacità. Con riferimento all'emotività, alcune emozioni, se ben gestite, sono in grado di concorrere alla valutazione del contesto da parte del combattente. La paura, ad esempio, in alcuni casi è funzionale a prendere la decisione più costo-efficace. Specularmente, l'inibizione della paura derivante dall'assunzione di agenti farmacologici potrebbe incidere, anche significativamente, sulla capacità di autoconservazione.

Di contro, farmaci normalmente impiegati per il trattamento di patologie mediche e, pertanto, non soggetti ad alcuna restrizione internazionale, possono essere utilizzati per interferire con lo stato cognitivo individuale⁴⁵ da Paesi e organizzazioni che adottano comportamenti più aggressivi. In tali casi, in cui è difficilmente ipotizzabile il contrasto di un soggetto alterato con una sostanza chimica, le possibili azioni di risposta propendono verso condotte preventive volte a contrastare i flussi di tali sostanze verso aree geopolitiche instabili, anche con il supporto del comparto *intelligence*, ritenuto fondamentale in tale ambito. Ad oggi, non sono contemplate alcune norme che possano essere adottate per la

⁴⁴ Cfr. Héloïse Goodley, "Pharmacological performance enhancement and the military. Exploring an ethical and legal framework for "supersoldiers", Chatham House, novembre 2020.

⁴⁵ Ad esempio, la Dopamina[®], il Donezepil[®], la Carbamazepina[®] e il Triesifenidile[®].

predetta azione preventiva. Pertanto, appare opportuno procedere ad un confronto serio e aperto con i Paesi alleati volto a predisporre un quadro giuridico che sia in grado di disciplinare un fenomeno come quello in oggetto dal quale, se non affrontato in modo condiviso e tempestivo, potrebbero derivare rischi per la sicurezza internazionale in generale e per quella nazionale in particolare.

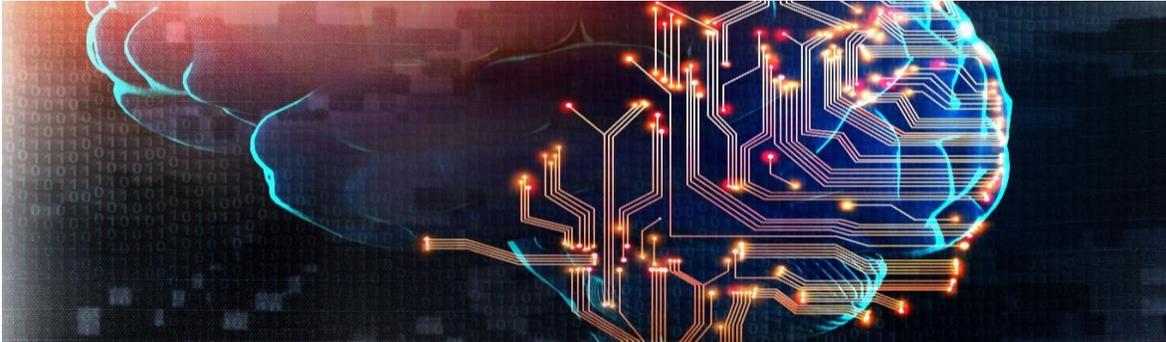
In sintesi, il ricorso a tali strumenti di interferenza cognitiva, nel contesto di una competizione persistente, comporta attente valutazioni di tipo etico-giuridico che taluni attori, in un confronto tra sistemi valoriali concorrenti, potrebbero sfruttare per finalità offensive (*degradation*) nell'ambito delle c.d. azioni "sotto soglia", anche mediante il trasferimento dei predetti valori in politiche di ricerca e sviluppo nazionali. Con riferimento a quest'ultimo aspetto, risulta necessario contribuire a sviluppare una metodologia in grado di realizzare un corretto processo di *attribution* volto ad identificare, al di là di ogni ragionevole dubbio, determinate responsabilità qualora un'eventuale azione, posta in essere attraverso tali strumenti, provocasse conseguenze rilevanti per la Sicurezza e la Difesa.

Per quanto attiene ai casi di conflitto armato convenzionale, non essendo tali strumenti oggetto di specifiche convenzioni, permangono i principi generali del diritto internazionale della *Law of War*, sia in termini di *jus ad bellum* che di *jus in bello*. In tutti gli altri casi, è necessario effettuare specifiche valutazioni atte a verificare i profili di legittimità di impiego.

Infine, considerata la crescente tendenza all'impiego di *devices* tecnologici in grado di realizzare i processi di *enhancement* e/o *degradation* sopra descritti, un ruolo particolarmente rilevante sarà rivestito dalle cd. *tech companies*, le quali acquisiranno un potere significativo (ma anche una rilevante responsabilità) sulla scena internazionale a causa dell'elevata quantità di dati personali e particolari che i relativi dispositivi saranno in grado di trattare. Pertanto, appare opportuno tendere verso un rafforzamento del quadro giuridico in materia di *data protection* e sicurezza cibernetica ponendo, se necessario, parametri internazionalmente condivisi, nonché dei robusti requisiti di sicurezza applicabili ai predetti *devices*, al fine di tutelare la riservatezza, l'integrità e la disponibilità dei dati trattati. Anche in questo caso, infatti, la sicurezza cibernetica assume un ruolo determinante in quanto i dati concernenti le prestazioni cognitive di un soldato, o di un qualsiasi altro soggetto *target*, potrebbero diventare un obiettivo particolarmente remunerativo per un *competitor* in grado di sfruttare tali dati a proprio vantaggio.

CAPITOLO 5

NUOVI STRUMENTI DI ALTERAZIONE



Gli studi scientifici sulla mente umana stanno permettendo di accrescere sempre più la comprensione dei processi cognitivi e dei relativi correlati neurofisiologici del cervello. Parallelamente, l'evoluzione nel campo delle neurotecnologie sta consentendo, anche attraverso l'utilizzo dell'Intelligenza Artificiale, di sviluppare sistemi e dispositivi sempre più efficaci di leggere e interpretare i segnali cerebrali che consentono un'interazione diretta tra il cervello umano e le macchine.

Sviluppate prevalentemente in ambito medico-scientifico per applicazioni terapeutiche e riabilitative, queste interfacce permettono di ripristinare funzioni danneggiate, ma anche di accrescere le capacità cerebrali attraverso un contributo esterno (*augmentation*). Le potenzialità di questi dispositivi sono tali da renderli oggi un elemento cardine dei numerosi progetti *brain* attualmente in corso, ma anche destinatari di un sempre maggiore interesse anche nel settore degli investimenti privati tra i quali, solo per citare un esempio, il progetto *Neuralink*⁴⁶ di Elon Musk.

In un contesto sempre più complesso, conteso e congestionato, in cui aumentano gli *input* provenienti da sensori e sistemi e si comprimono i tempi decisionali per garantire risposte efficaci (*Hyperwar*), particolare rilevanza potrebbero assumere questi nuovi strumenti nell'incrementare le capacità cognitive dei militari e, più in generale, per accrescere la *situational understanding*.

Dalla necessità di una *situational awareness* compiutamente Multidominio a supporto del processo decisionale alla gestione di sciame di sistemi autonomi sul campo di battaglia, queste interfacce hanno innumerevoli possibili applicazioni militari. In tal senso, potrebbero costituire il perno di una vera e propria rivoluzione anche in ambito militare, con il superamento del modello *net*-centrico verso un modello *mind*-centrico con una maggiore centralità della dimensione cognitiva della mente umana.

⁴⁶ Società fondata nel 2016 e specializzata in Intelligenza Artificiale che si pone l'obiettivo di sviluppare un dispositivo che possa collegare direttamente il cervello umano alla macchina.

5.1 LA COMUNICAZIONE UOMO-MACCHINA

L'Intelligenza Artificiale, almeno nelle forme ad oggi disponibili (*macchine/deep learning*), è ormai entrata a far parte della nostra quotidianità attraverso strumenti che ci permettono di impiegarla secondo un rapporto di tipo *master-slave* per delegare alla macchina specifiche funzioni attraverso **interfacce sensoriali** di tipo tattile, acustico o visivo (*devices*). Tali interfacce non costituiscono veri e propri strumenti di alterazione in quanto non permettono di accrescere le capacità cognitive dell'individuo, ma consentono di delegare specifiche funzioni, ottimizzando i tempi necessari, e di concentrare i nostri sforzi sulle attività non delegabili. Tuttavia, queste necessitano di uno stimolo (*input*) di tipo tattile e forniscono un risultato (*output*) che deve comunque essere ricevuto attraverso uno stimolo sensoriale e processato dal cervello.

Le interfacce neurali (*Brain Computer Interface* – BCI) permettono una relazione diretta tra il cervello e il computer attraverso i segnali provenienti dal sistema nervoso centrale. L'acquisizione del segnale cerebrale può avvenire, ad oggi, in modalità non invasive (segnali EEG⁴⁷ registrati sul cuoio capelluto – eBCI, e sistemi di realtà aumentata indossabili), semi-invasive (tecnologie neurali come l'elettrocorticografia) o invasive (*microarray* intracorticali, iBCI)⁴⁸ con risultati ed efficacia differenti. Tuttavia, gli sviluppi nel campo delle nanotecnologie potrebbero consentire di sviluppare nuove ed efficaci modalità di lettura e trasmissione del segnale cerebrale.

Un'interfaccia neurale consente di fatto una comunicazione bidirezionale tra il cervello umano e un dispositivo esterno. Il *teaming* uomo-macchina, inteso in questo caso verso un modello *peer-to-peer*, si configura quindi come parte delle applicazioni di tipo BCI, con la neuro-ergonomia che applicherà le scoperte delle neuroscienze per comprendere la prospettiva umana all'interno della relazione con la macchina. Queste interfacce non devono necessariamente collegare gli esseri umani a elementi *hardware*, ma la connessione può essere stabilita anche con un *software*, un altro operatore umano (*Brain-to-Brain Interface* - B2BI) o semplicemente con un sistema di *output* per svolgere attività di valutazione.

Il potenziale valore aggiunto insito nelle interfacce di tipo BCI è, quindi, da ricondurre non solo alla stretta relazione fra l'operatore umano e la macchina ma, più in generale, alle possibilità di aumentare le capacità umane attraverso il contributo/supporto di un agente esterno. In particolare, le possibili funzioni supportate da tali sistemi di interfaccia sono molteplici e possono essere ricondotte principalmente alle seguenti:

- **lettura di dati dal cervello:** utilizzata per una valutazione della *performance* cognitiva individuale;
- **controllo diretto di un sistema:** l'utente esercita il controllo della macchina *wireless* tramite l'attività cerebrale. Si ritiene ipotizzabile l'utilizzo per una varietà di impieghi,

⁴⁷ Elettroencefalografia.

⁴⁸ Cfr. Jonathan Moreno, Michael L. Gross, Jack Becker, Blake Hereth, Neil D. Shortland III and Nicholas G. Evans, "The ethics of AI-assisted warfighter enhancement research and experimentation: Historical perspectives and ethical challenges", *Front. Big Data*, settembre 2022.

dal controllo di sistemi *unmanned*/autonomi allo svolgimento di attività di ricerca e soccorso ovvero di supporto sanitario;

- **integrazione con dispositivi protesici:** impiegato quale ausilio sanitario;
- **scambio di informazioni:** all'estrazione di dati dal cervello si deve aggiungere specularmente la possibilità di veicolare questi al cervello, mettendo in condizione l'utente di disporre di un *feedback* attraverso informazioni sul sistema oggetto di controllo. Potrebbe essere impiegato per aumentare, ad esempio, la capacità umana di utilizzo della memoria;
- **comunicazione *brain-to-brain*:** sulla base di attività sperimentali già condotte, consentono ad un sistema non invasivo che fa ricorso all'elettroencefalografia (EEG) di leggere i segnali cerebrali, trasmetterli attraverso la rete e, successivamente, trasferire le risposte di tipo motorio ad un secondo utente che si avvale della stimolazione magnetica transcranica;
- **ibridazione** (vds. paragrafo successivo): consente di sviluppare un rapporto più simbiotico tra l'operatore umano e la macchina, permettendo al primo di integrare pensieri e dati nell'ambito dei processi condotti dalla macchina.

5.2 LA HUMAN COMPUTER CONFLUENCE

La confluenza uomo-computer si riferisce a un'interazione trasparente, implicita, e incarnata (o basata su impiantati neurali) tra l'operatore umano e il sistema. Il paradigma emergente della confluenza tra computer ed essere umano (*Human Computer Confluence* – HCC) non può, infatti, essere ridotto ad una sfida puramente tecnologica. Le complessità di questo nuovo paradigma è rappresentato dal fatto che entrambe le parti (essere umano e macchina) interagiscono e si intrecciano a diversi livelli (fisico, comportamentale e cognitivo) sulla base di una comprensione reciproca. In altri termini, non essendovi più la necessità per l'operatore umano di fornire comandi alla macchina, si assiste ad una modellazione reciproca (in senso robotico/cibernetico dell'uomo e delle sue interazioni e, viceversa, in senso antropomorfo della macchina che viene percepita come *partner*). Questa è resa possibile tramite una rete di sensori e attuatori che consentono un'amplificazione della realtà ovvero un'**ibridazione** tra realtà fisica e realtà digitale, impattando in tal modo sulla capacità di gestire la complessità cognitiva e traendo vantaggio da tale stratificazione. In questo quadro di rapporto ormai simbiotico, si va ben oltre la collaborazione tra l'uomo e la macchina nella direzione di un'autentica conversazione tra questi ultimi grazie all'IA e alla robotica antropomorfa.

La confluenza si configura pertanto non solo come forma di *augmentation* per specifiche capacità umane (forza, memoria, concentrazione, percezione o ragionamento), ma come *empowerment* dell'operatore stesso, permettendo a questo di utilizzare le proprie abilità in modi nuovi. Il progressivo *coupling* funzionale a livello neurofisiologico si concretizza in

uno strumento di alterazione delle capacità cognitive umane dalle molteplici applicazioni⁴⁹ e che sono oggi oggetto di studio e ricerca.

L'integrazione tra le interfacce e la realtà virtuale può essere funzionale ad applicazioni volte ad aumentare il controllo delle funzioni cerebrali tramite una tecnica nota come “*neurofeedback*”, in base alla quale l'utente apprende a modulare e autoregolare gli stati cerebrali attraverso un segnale (*feedback*) che informa in tempo reale dei cambiamenti neurofisiologici che stanno avendo luogo. Il *neurofeedback* è già applicato con successo nel trattamento dei disturbi dell'attenzione, dell'ansia, della depressione, dei disturbi del sonno e delle dipendenze. Tale procedura risulta pertanto più efficace grazie alle interfacce neuro-virtuali, mettendo in condizione l'utente di visualizzare il *feedback* direttamente nell'ambiente virtuale.⁵⁰

5.3 L'HACKING COGNITIVO

Accanto agli evidenti vantaggi che l'implementazione di interfacce neurali potrebbe generare anche nel contesto militare, vi sono tuttavia da considerare anche i rischi e le vulnerabilità correlati. Accanto alle vulnerabilità già evidenti, si potrebbero aprire nuove possibilità di aggressione sia sulla funzionalità del *network*, sia sulla sicurezza dello stesso operatore. La possibilità di infiltrare “*malware* neurali” pone evidenti interrogativi sia in termini di *detection* che di protezione⁵¹.

Inoltre, attraverso il superamento della frontiera tecnologica si può arrivare a ipotizzare l'*hacking* cognitivo del soggetto *target*, attraverso l'induzione di una rappresentazione falsata della realtà oggettiva.

Il cervello umano funziona, infatti, attraverso una modalità anticipante della realtà (*predictive coding*⁵²) che viene poi confermata o corretta in funzione degli stimoli sensoriali ricevuti. Nei contesti di relazione simbiotica, il fenomeno dell'*hacking* cognitivo potrebbe essere utilizzato sia operando sulla rete e inducendo una certa previsione, sia operando direttamente sulla risposta sensoriale. Attraverso tali modalità di intervento si potrebbe così arrivare a indurre una rappresentazione alterata della realtà che porterebbe ad un disallineamento dalla realtà oggettiva con evidenti effetti sia sull'azione, sia sulla salute stessa dell'operatore.

Per capire la possibile portata di tali azioni, alcuni esempi possono essere ricercati negli studi attualmente in corso per la valutazione dei rischi del metaverso, tra i quali lo “*human joystick*” (in cui viene indotto uno spostamento fisico reale dell'utente attraverso la

⁴⁹ Cfr. Andrea Gaggioli, Alois Ferscha, Giuseppe Riva, Stephen Dunne, Isabelle Viaud-Delmon, “*Human Computer Confluence. Transforming Human Experience Through Symbiotic Technologies*”, De Gruyter Open Ltd, 2016.

⁵⁰ Cfr. Giuseppe Riva, Andrea Gaggioli, “*Realtà virtuali: Gli aspetti psicologici delle tecnologie simulate e il loro impatto sull'esperienza umana*”, Giunti Psychometrics, 2019.

⁵¹ Cfr. Katrine Nørgaard, Michael Linden-Vørnle, “*Cyborgs, Neuroweapons, and Network Command*”, Scandinavian Journal of Military Studies, 4(1), 2021, <https://doi.org/10.31374/sjms.86>.

⁵² Cfr. Friston, K., & Kiebel, S. (2009). Predictive coding under the free-energy principle. *Philosophical transactions of the Royal Society of London. Series B, Biological sciences*, 364(1521), 1211–1221. <https://doi.org/10.1098/rstb.2008.0300>

manipolazione dell'ambiente virtuale) e l'attacco “*chaperone*” (attraverso la modifica dei confini dell'ambiente virtuale viene portato l'utente in condizioni di rischio nella realtà fisica in cui si trova).

5.4 PRINCIPI ETICO-GIURIDICI DI RIFERIMENTO

Lo sviluppo nel settore delle interfacce cerebrali apre significativi ed irrisolti quesiti di natura etica e giuridica che sono oggi fonte di acceso dibattito nelle comunità internazionali di scienziati e ricercatori. Allo stato attuale, è impossibile definire chiaramente un quadro di riferimento per sviluppi ancora in fase di ricerca sperimentale. Tuttavia, partendo dal necessario assioma che la miglior sicurezza non risiede nel comprendere e possedere la tecnologia più avanzata, ma nel porre le condizioni per un utilizzo “corretto” di tali mezzi, si possono individuare, sin da subito, alcuni parametri che potrebbero contribuire a fornire un possibile riferimento nello sviluppo di programmi di interesse anche militare.

a. Responsabilità

Con l'evoluzione nel settore delle interfacce neurali e il nuovo paradigma della confluenza si aprono importanti riflessioni su quanto l'essere umano possa mantenere la paternità delle proprie decisioni e su quanto queste possano invece essere frutto dell'azione esterna. Al riguardo, è bene ricordare come – in un sistema di diritto – l'atteggiamento psicologico costituisce l'elemento essenziale che connota la condotta del soggetto agente ma, nel caso di specie, ci troviamo davanti a nuove entità, le cui decisioni e risultati non sono pienamente l'effetto di azioni umane, ma derivano da una serie di processi che hanno autonoma capacità decisionale e in alcuni casi non giustificabili a posteriori, in quanto non è sempre possibile comprendere come il sistema sia giunto ad assumere una certa decisione. Ciò posto, seppure il tema della responsabilità giuridica dell'IA sia ampiamente dibattuto in numerosi ambiti come nel caso delle auto a guida autonoma, per lo specifico contesto militare è possibile effettuare alcune precisazioni.

Il tema della confluenza e della robotizzazione degli esseri umani fa da contraltare a quello dell'umanizzazione dei sistemi robotici che in ambito militare possono essere inquadrati nel contesto dei *Lethal Autonomous Weapons System* (LAWS). Facendo un parallelismo è possibile richiamare i principi guida sullo sviluppo di sistemi autonomi della Convenzione su certe armi convenzionali (*Convention on Certain Conventional Weapon* – CCW) che precisa come la piena responsabilità umana sulla decisione di impiego dovrà essere mantenuta finché l'*accountability* non potrà essere trasferita alla macchina.

In tal senso, data la natura del rapporto che si viene a instaurare attraverso soluzioni sempre più tendenti all'ibridazione, potrà essere necessario sviluppare specifiche valutazioni e sperimentazioni preliminari (es. scenario *based*) per valutare il livello di coscienza mantenuto dall'operatore nell'assunzione delle decisioni e riconoscere l'idoneità all'introduzione in servizio delle interfacce.

Ferma la previsione dell'articolo 27, comma 1, della Costituzione⁵³ che ha di fatto impedito, ad oggi, il riconoscimento di responsabilità penali in capo alle persone giuridiche, occorre prevedere, pertanto, l'implementazione di sistemi IA capaci di rispondere, già in sede di progettazione, a dei principi di natura tecnica (tra cui le architetture del sistema, la tracciabilità, le fasi di test e validazione, la possibilità di ottenere una spiegazione delle decisioni adottate) che consentano, qualora fosse necessario, la puntuale identificazione di eventuali responsabilità in capo al produttore, nonché ai programmatori o a coloro che hanno realizzato gli algoritmi decisionali.

Certamente la questione mette in dubbio l'intero concetto di pena e coinvolge nella discussione prospettive filosofico-culturali che trascendono la dogmatica penalistica, innervandosi ancora una volta nel dibattito sul riconoscimento di una soggettività giuridica.

Inoltre, considerato che le decisioni assunte dal combattente nel *battlespace* di riferimento dipendono in larga parte dalla percezione di sé all'interno del contesto operativo, non si può escludere a priori il rischio che un'autonomia, anche solo compartecipata uomo-macchina, possa alterare tale percezione, degradando di conseguenza le abilità decisionali dell'essere umano e la capacità di effettuarne una distinzione dei propri limiti e vincoli.

b. Reversibilità

In chiave etica, il ricorso a tali *devices* impone di assicurare che il progresso tecnologico si svolga in armonia con le esigenze di tutela individuali e collettive, nel rispetto della dimensione antropocentrica e della prevenzione del danno (*primum non nocere*), che rappresentano attualmente l'unico ancoraggio dinanzi a un fenomeno di cui non si conoscono appieno le reali implicazioni.

Tutte le interfacce sin qui descritte, infatti, comportano una crescente dipendenza dell'utente. Già a partire da quelle sensoriali oggi usate quotidianamente ed alle quali siamo soliti delegare alcune funzioni possono comportare la riduzione progressiva fino alla perdita completa di alcune capacità (ad esempio, secondo alcuni studi l'utilizzo costante dei sistemi di navigazione satellitare sta progressivamente comportando una riduzione della capacità di orientamento). Nel caso di interfacce cerebrali, tale dipendenza può essere sviluppata sia a livello psicologico che cognitivo e comportare importanti conseguenze in caso di interruzione del rapporto che si instaura tra il cervello e l'ausilio esterno.

In tal senso, nell'ambito delle possibili applicazioni militari, il tema della reversibilità dovrà essere preventivamente valutato a differenti livelli:

- **operativo:** il disturbo o l'interruzione del rapporto tramite la negazione del supporto esterno potrebbe inficiare, anche significativamente, l'operatività dell'utente. Pertanto, al fine di mantenere una piena capacità operativa, anche in questo caso andrà

⁵³ La responsabilità penale è personale.

attentamente mantenuta e costantemente addestrata la capacità di operare in modalità degradata;

- **sanitario:** oltre agli aspetti legati alla sicurezza, sono da considerare gli effetti sulla salute a breve, medio e lungo termine, dato che le caratteristiche di impiego nel contesto militare potrebbero comportare una tendenza ad optare per sistemi più o meno invasivi che possono avere impatti non pienamente reversibili;
- **psicologico:** poiché tali interfacce comportano una crescente dipendenza soprattutto in contesti di impiego prolungato quali una campagna operativa, l'interruzione del supporto potrebbe avere significativi impatti sulla salute mentale del soggetto. Secondo alcuni studi, infatti, l'utilizzo prolungato potrebbe comportare l'insorgere di patologie simili alla sindrome da stress post-traumatico (PTSD).

5.5 L'ESIGENZA DI UN COMITATO ETICO

Uno degli obiettivi principali della ricerca è la scoperta di nuovi principi e metodi che possono essere applicati a beneficio dell'uomo. I potenziali vantaggi e rischi di una sperimentazione non possono essere accertati fino a quando non è stata ampiamente testata su soggetti umani. Tuttavia, nonostante le misure di salvaguardia stabilite, esiste la possibilità intrinseca che effetti collaterali, imprevisi e a lento sviluppo, possano verificarsi. Infatti, la sperimentazione di nuove tecniche o terapie sull'essere umano implica l'insorgere di una serie di ostacoli e problematiche, alcuni dei quali condivisi con l'etica medica generale e altri più specificamente legati a questioni morali e filosofiche dell'attività mentale.

Una delle principali questioni etiche, nell'ambito della ricerca, è il delicato equilibrio tra scienza, società e i diritti dell'essere umano, nella considerazione che il progresso scientifico e il miglioramento del benessere dell'individuo rappresentano per la società un dovere morale. Quando informazioni mediche importanti possono essere ottenute con rischi trascurabili e senza violare i diritti individuali, lo sperimentatore ha il dovere di utilizzare la sua intelligenza e le sue capacità per questo scopo. Il mancato rispetto di ciò rappresenta una negligenza dei doveri professionali, in qualche modo simile alla negligenza di un medico che non applica tutti i suoi sforzi alla cura di un paziente.

Infatti, quando si testa una nuova terapia, come è stato ad esempio per la penicillina, le prove preliminari volte a verificarne l'efficacia terapeutica, inizialmente sono svolte in laboratorio (per la penicillina, infatti, sono state effettuate *in vitro*). Successivamente, vengono eseguiti test su animali⁵⁴ (per esempio, su diverse specie di mammiferi) e, infine, la dimostrazione conclusiva della sicurezza clinica ed efficacia di un farmaco richiede l'applicazione all'uomo. La ricerca, ovviamente, non si conclude con la verifica dell'immediata efficacia del prodotto, ma prosegue con lo studio degli effetti a lungo termine sull'essere umano⁵⁵.

⁵⁴ Nel senso, la disciplina è stata sancita dal decreto legislativo 4 marzo 2014, n. 26, recante “Attuazione della direttiva 2010/63/UE sulla protezione degli animali utilizzati a fini scientifici”.

⁵⁵ Negli anni 50-60, un farmaco apparentemente innocuo, il Talidomide[®], veniva somministrato in maniera diffusa come sedativo per poi scoprire negli anni successivi che aveva effetti dannosi sullo sviluppo fetale, portando alla nascita di bambini focomelici.

Sebbene nessun codice etico formale sia stato universalmente accettato per lo svolgimento della ricerca sull'uomo, le linee guida di base sono state formulate, ad esempio, dall'*American Psychological Association*, dai giudici dei processi per crimini di guerra di Norimberga, dall'Associazione medica mondiale e dal *Medical Research Council of Britain*. Al riguardo, l'approfondimento delle questioni etiche e la necessità di regolamentazione delle attività sperimentali che implicano il coinvolgimento di esseri umani ha portato alla nascita dei Comitati Etici (EC).

I COMITATI ETICI

I Comitati Etici (CE) sono organismi indipendenti la cui principale funzione è la valutazione degli aspetti etici e scientifici delle sperimentazioni cliniche al fine di tutelare i diritti, la sicurezza e il benessere delle persone coinvolte. I CE sono ampiamente diffusi nel mondo e negli Stati Uniti prendono il nome di *Institutional Review Boards* (IRB).

In Italia non è possibile sperimentare un farmaco sull'uomo senza che prima lo studio abbia ottenuto un parere favorevole da parte di un CE, a garanzia pubblica del fatto che il bene primario che si intende perseguire è, al di sopra di ogni altro, il benessere delle persone. Questi organismi sono presenti anche in alcune strutture sanitarie pubbliche e in alcuni Istituti di Ricovero e Cura a Carattere Scientifico (IRCCS).

I componenti dei CE, generalmente in numero compreso tra 15 e 20, sono selezionati tra esperti in materie medico-scientifiche, sanitarie, infermieristiche, giuridiche e di bioetica. Per l'attività di valutazione e decisione circa l'ammissibilità delle sperimentazioni, i CE fanno riferimento a documenti e strumenti giuridici condivisi a livello internazionale nonché a tutte le normative vigenti in tale ambito a livello nazionale ed internazionale.

I CE italiani sono il risultato di un processo di sviluppo che ha avuto inizio negli anni novanta del secolo scorso. Già nel 1992, infatti, il Comitato Nazionale per la Bioetica (CNB) aveva dedicato un parere al tema, mentre è del 1998 il primo Decreto Ministeriale, Linee Guida di riferimento per l'istituzione e il funzionamento dei Comitati etici. Nel 2013, dopo il decreto ministeriale 8 febbraio 2013, sono stati istituiti sul territorio italiano circa novanta CE.

Nel 2018 sono state realizzate ulteriori modifiche all'organizzazione della rete italiana, a partire dall'istituzione del Centro di coordinamento nazionale dei comitati etici territoriali per le sperimentazioni cliniche sui medicinali per uso umano e sui dispositivi medici, previsto dalla legge 11 gennaio 2018, n. 3 (legge Lorenzin).

Di fatto, come è stato evidenziato dal CNB in un parere del 2017, i CE svolgono, all'interno delle strutture di appartenenza, un'attività di consulenza etica che va oltre la valutazione dei protocolli della sperimentazione dei farmaci. Per far fronte a più specifiche esigenze, il CNB auspica lo sviluppo dei "Comitati per l'etica nella clinica", che non hanno ancora ricevuto un inquadramento legislativo e amministrativo all'interno dell'attuale processo di revisione organizzativa.

In riferimento ai molteplici aspetti del *Cognitive Warfare*, appare evidente la necessità di dedicarvi grande attenzione etica, ma anche di sviluppare una profonda consapevolezza della assoluta necessità di dover far crescere un settore, del tutto nuovo, dove i *competitors* possono già correre molto veloci. L'eventuale rinuncia a priori allo sviluppo di qualsiasi capacità volta ad accrescere l'operatività del combattente, potrebbe portare alla perdita di un vantaggio su un potenziale *competitor*, nel momento in cui questi decidesse di implementarla a sua volta per sé.

La necessità di istituire un Comitato Etico ad *hoc* per lo sviluppo, la ricerca, la valutazione e la validazione di ciò che attiene l'Innovazione e, in particolare, il *Cognitive Warfare* per il comparto Difesa in Italia appare cogente. La tecnologia avanza in modo inesorabile, così

come la conoscenza del cervello e del funzionamento dell'essere umano. Meno certe sono invece le conseguenze sull'essere umano relativamente agli sviluppi della tecnologia applicata, la cui conoscenza dipende esclusivamente dalla ricerca.

Sempre più importanti appaiono al riguardo le sinergie con le università, i laboratori di ricerca e l'industria. L'inserimento di ricercatori militari nei contesti scientifici nazionali e internazionali sono sempre più fondamentali. L'investimento nello specifico settore risulta indispensabile. L'individuazione di *stakeholders* e *partnership* è irrinunciabile, e per questa ragione la flessibilità cognitiva e manageriale appare una competenza indispensabile nella *leadership* militare.

Studiare e gestire le conseguenze dell'interazione sempre più inclusiva, talvolta intrusiva del rapporto uomo- macchina-tecnologia assume il carattere dell'urgenza. Basti pensare, già oggi, alle ripercussioni sulla psiche degli effetti dell'utilizzo dei droni, della robotica, della cibernetica applicata al campo di battaglia ove l'azione del combattente è mitigata dalla realtà virtuale o dalla distanza reale dal *target*. Le emozioni, le percezioni, il corpo, restano esclusi dall'azione, ma non i suoi contenuti distruttivi e i suoi effetti di retroazione (basti pensare ai bombardamenti a distanza tramite droni) per cui il cervello è poi chiamato ad integrare nell'esperienza di ciascuno le immagini ricevute, anche se lontane ed estranee, distanti ma reali (il disturbo da Stress Post Traumatico PTSD per combattimenti a distanza è un argomento già noto, con i suoi risvolti etici e psicologici).

IL COGNITIVE WARFARE NEL CONTESTO MULTIDOMINIO

La pervasività dei molteplici aspetti che concorrono alla competizione nella dimensione cognitiva e le possibili prospettive evolutive del fenomeno rappresentano un fattore di assoluta complessità le cui sfide e opportunità, se non adeguatamente affrontate, potrebbero avere significativi impatti sull'intera società a livello globale.

Appare quindi immediatamente evidente come il *Cognitive Warfare* e le sfide derivanti dalla portata del fenomeno esulino da competenze esclusive di un unico Dicastero o Paese e necessitino di un'azione corale e sinergica da supportare, sia a livello nazionale che internazionale, anche attraverso un processo di crescente coinvolgimento e responsabilizzazione dei numerosi *stakeholders*, anche privati.

Risulta quindi necessario sviluppare, a tutti i livelli (*whole of society*), una profonda consapevolezza della portata del fenomeno e delle sfide correlate per affrontare al meglio rischi e opportunità connesse allo sviluppo del *Cognitive Warfare*. Tale consapevolezza di una risposta *whole of government*, dovrà necessariamente essere sviluppata attraverso la ricerca del coinvolgimento attivo della Difesa, in coordinamento con il comparto *intelligence* nazionale, già nelle fasi di monitoraggio di possibili azioni ostili.

Tenuto conto del livello di interconnessione globale e del livello di sviluppo delle innovazioni tecnologiche, il *Cognitive Warfare* sarà sempre più utilizzato per la condotta di operazioni anche sotto la soglia di conflitto spostando il *focus* dello scontro dai tradizionali campi di battaglia alle menti. Un qualcosa di intangibile, ma che potrebbe diventare un'arma potentissima. L'associazione di una tipologia di *Warfare*⁵⁶ alla dimensione cognitiva è giustificato dall'incremento di azioni nell'*Information Environment*, poste a sistema con gli sviluppi tecnologici, quelli delle neuroscienze e di tutti quei nuovi strumenti che sfruttano l'ambiente informativo e lo spettro elettromagnetico per influenzare i processi cognitivi.

Già da qualche decennio, sulla base delle esperienze militari, la NATO annovera negli approcci dottrinali alla gestione delle crisi il *behaviour centric approach* volto a influenzare *l'audience*, ovvero attori, *stakeholder* e popolazione⁵⁷. In linea generale, mentre proseguono le attività di approfondimento in ambito NATO per definire meglio le caratteristiche del *Cognitive Warfare*, emerge la necessità di rilevare e comprendere le insidie e le sfide sottese, al fine di formulare ipotesi ed elaborare accurati *assessment* nella prospettiva di breve, medio e lungo termine.

⁵⁶ *Warfare: the activity of fighting a war or strongly competing, esp. with reference to the type of weapons used or to the way the fighting is done* (Cambridge Dictionary).

⁵⁷ Vds. NATO AJP-01 *Allied Joint Doctrine*, EDF V1 RD.

In tal senso, al fine di meglio comprendere il *Cognitive Warfare* e le sfide derivanti emerge la necessità di definire concettualmente come esso si inquadri pienamente **nell'ambito delle Operazioni Multidominio**, nella considerazione che utilizza azioni, mezzi e strumenti, attraverso le connessioni esistenti tra i cinque domini operativi, l'ambiente informativo e lo spettro elettromagnetico, per generare effetti sulla dimensione cognitiva e ottenere un vantaggio sull'avversario. L'attuale sfida militare comporta la necessità di conoscere la minaccia, di disporre di tecniche difensive efficaci, di opzioni di deterrenza e di modi per affrontare le conseguenze. Pertanto, il *Cognitive Warfare* non è qualcosa che viene utilizzato come alternativa alla guerra tradizionale, ma rappresenta un aspetto della competizione sopra e sotto soglia.

Al fine di gestire adeguatamente questa forma di competizione, la Difesa, di concerto con gli altri Strumenti del Potere nazionale e in maniera sinergica con gli altri Paesi dell'Alleanza, dovrebbe lavorare a vari livelli per definire e misurare le minacce, valutare le vulnerabilità delle sue componenti e incentivare le iniziative per mitigarle e sviluppare adeguate strategie di risposta.

Lo spazio cibernetico rappresenta un'opportunità, ma ha introdotto anche nuove minacce: l'accresciuta disponibilità e diffusione delle tecnologie di *broadcasting* implica la necessità sempre più stringente di pianificare le azioni militari considerandone il potenziale impatto sull'ambiente informativo, garantendo, al contempo, uno strumento per influenzare, modificare e minare le convinzioni della popolazione. Il cyberspazio e l'ampia copertura mediatica sono diventati un moltiplicatore di effetti per le tecniche della disinformazione. Inoltre, appare chiaro come l'evoluzione tecnologica abbia incrementato esponenzialmente l'efficacia stessa della comunicazione. La travolgente diffusione dei *digital media* e il prossimo impiego dei processori quantici facilitano le attività di profilazione della *target audience* e di diffusione dei prodotti audio-visivi all'uopo concepiti. Le operazioni cibernetiche si impongono inevitabilmente sia come strumento per la condotta delle operazioni nella dimensione cognitiva, sia come loro moltiplicatore d'efficacia.

Definito il quadro generale e tenuto conto della complessità del fenomeno, è possibile identificare alcune elementi di indirizzo generale per le singole macro-aree sviluppate:

a. Influenza

A livello nazionale risulterà necessario garantire unicità e continuità di indirizzo strategico al fine di mitigare, nel pieno rispetto della libertà di espressione e del dibattito pubblico, l'insorgere di fenomeni di estrema polarizzazione su temi divisivi che possono essere oggetto di strategie di disinformazione avversarie. In particolare, tenuto conto della possibile destabilizzazione dell'ecosistema informativo che può essere causata dall'azione di disinformazione, dovrà essere incentivato lo sviluppo, a livello nazionale, di specifici *tools* per l'identificazione di contenuti falsi/manipolati così come per

l'elaborazione del linguaggio naturale⁵⁸ in lingua italiana, che potrebbe essere usata da potenziali avversari per creare contenuti malevoli (*deepfake*). Al fine di comprendere l'insorgere e lo sviluppo di linee di influenza potrà, inoltre, essere necessario identificare e mappare *community, influencer, gruppi* (es. *gaming*) al fine di assicurare una migliore comprensione dei fenomeni.

b. Interferenza

La pervasività e le difficoltà di identificazione e contrasto degli strumenti di interferenza cognitiva necessitano di una sensibilizzazione istituzionale su opportunità e rischi correlati. In particolare, al fine di identificare e monitorare i possibili agenti e dispositivi di interferenza cognitiva, potrebbe risultare particolarmente utile istituire un osservatorio nazionale inter-agenzia⁵⁹, che dovrebbe rivestire il ruolo di coordinamento ed armonizzazione di iniziative e attività ministeriali.

c. Alterazione

La possibilità che attori privati e *competitors* possano sviluppare e sfruttare una superiorità nello sviluppo di interfacce sempre più avanzate e invasive apre scenari che possono avere significativi impatti anche in termini di Sicurezza nazionale.

Occorre, pertanto, comprendere come il differente quadro di riferimento ponga significative restrizioni alle possibilità di ricerca nazionali e valutare l'adozione dei necessari temperamenti che consentano di supportare lo sviluppo di conoscenza e competenza in un settore che potrà, in prospettiva, rappresentare un nuovo fattore di competizione geostrategica.

LINEE DI INDIRIZZO

Le potenziali implicazioni militari della competizione cognitiva necessitano di una crescente attenzione della Difesa al fenomeno attraverso una preliminare attività di **informazione, formazione ed educazione** di tutto il personale militare e, in particolare, della *Leadership* sin dai primi anni negli Istituti di formazione anche attraverso lo sviluppo di specifici *tools* che supportino l'acquisizione della consapevolezza (*pre-bunking*).

Inoltre, l'evoluzione tecnologica potrà consentire, attraverso la combinazione di differenti modalità di analisi (*eye tracking, heart rate*, macro espressioni e, in prospettiva, anche micro, *big data, Brain Computer Interface*, ecc.), lo sviluppo di *tools* sempre più efficaci per valutare e addestrare la capacità di resistere ad un'azione di influenza. Pertanto, dovrà essere

⁵⁸ *Natural language Processing* (NLP).

⁵⁹ Anche attraverso la ridefinizione delle attività e dei compiti del Comitato Nazionale per la Biosicurezza, le Biotecnologie e le Scienze della Vita (CNBBSV) operante presso la Presidenza del Consiglio dei Ministri dal 1992, ampliando la gamma delle sue competenze e la rappresentatività dei Ministeri e degli enti pubblici coinvolti nelle sue attività.

monitorato lo sviluppo del settore e valutata la possibilità, in prospettiva, di acquisire o sviluppare tali *tools*.

Al fine di indicare un processo che possa informare l'azione della Difesa nel contesto del *Cognitive Warfare* e partendo dalle preliminari attività di informazione, educazione e formazione sul fenomeno, è possibile definire un percorso secondo quattro linee di indirizzo:

a. Rilevanza della dimensione cognitiva

Nella sfera militare, la volontà di combattere, il morale, la coesione, la fiducia nella catena di comando e il processo decisionale a tutti i livelli sono fortemente a rischio in caso di attacchi cognitivi da parte dei nostri avversari. Il *Military Instrument of Power* (MIoP), infatti, può essere influenzato indirettamente comportando anche l'insorgere di sentimenti di sfiducia, divisione, radicalizzazione ecc. Il percorso di riconoscimento della rilevanza della dimensione cognitiva può, pertanto, essere descritto secondo i seguenti elementi principali:

- **Comprensione del ruolo della Difesa:** anche le sole azioni di influenza possono configurarsi come vere e proprie aggressioni attraverso il principio di equivalenza con l'azione cinetica, fino al punto da giustificare l'esercizio della legittima difesa e, a livello internazionale, l'eventuale richiesta di attivazione della clausola di difesa collettiva⁶⁰. Risulterà quindi necessario comprendere il ruolo della Difesa e garantirne il pieno coinvolgimento, in coordinamento con il comparto *intelligence* nazionale, già nelle fasi di monitoraggio di possibili azioni ostili;
- **Adattamento del quadro giuridico:** con il riconoscimento del ruolo della Difesa andrà assicurato, in linea con l'evoluzione a livello internazionale, il necessario adattamento del quadro giuridico-legale nazionale per abilitare l'azione dello Strumento Militare;
- **Definizione di indicatori condivisi:** tenuto conto della complessità e pervasività della minaccia, andranno definiti parametri e indicatori condivisi, a livello nazionale e internazionale, che possano consentire di monitorare l'evoluzione del fenomeno e supportare lo sviluppo di idonee strategie di risposta. Sussiste la necessità di comprendere, cioè, quando un atto di guerra cognitiva sia effettivamente in corso, atteso che questi possono manifestarsi, ad esempio, attraverso semplici *post* o *tweet*,

⁶⁰ NATO Art. 5: “Le parti convengono che un attacco armato contro una o più di esse in Europa o nell'America settentrionale sarà considerato come un attacco diretto contro tutte le parti, e di conseguenza convengono che se un tale attacco si producesse, ciascuna di esse, nell'esercizio del diritto di legittima difesa, individuale o collettiva, riconosciuto dall'art. 51 dello Statuto delle Nazioni Unite, assisterà la parte o le parti così attaccate intraprendendo immediatamente, individualmente e di concerto con le altre parti, l'azione che giudicherà necessaria, ivi compreso l'uso della forza armata, per ristabilire e mantenere la sicurezza nella regione dell'Atlantico settentrionale. Ogni attacco armato di questo genere e tutte le misure prese in conseguenza di esso saranno immediatamente portate a conoscenza del Consiglio di Sicurezza. Queste misure termineranno allorché il Consiglio di Sicurezza avrà preso le misure necessarie per ristabilire e mantenere la pace e la sicurezza internazionali”.

finalizzati a una “narrativa” credibile per manipolare grandi masse di popolazione (disinformazione e misinformazione);

- **Sviluppo di strategie di risposta:** sulla base dei parametri condivisi andranno sviluppate specifiche strategie di risposta che possano consentire la tempestiva adozione di specifiche opzioni predefinite di risposta ed *escalation* e/o *de-escalation* (*escalation management options*).

b. Comprensione della minaccia

La complessità degli aspetti che concorrono alla competizione nella dimensione cognitiva, se non adeguatamente analizzate e affrontate, potrebbero avere significativi riflessi anche in termini di Sicurezza nazionale. In tal senso, occorrerà porre particolare attenzione alla comprensione della minaccia attraverso i seguenti elementi principali:

- **Condivisione delle informazioni:** al fine di monitorare le possibili sorgenti di rischio, una maggiore sensibilizzazione del comparto *intelligence* e la piena condivisione delle informazioni con la Difesa potranno consentire di assicurare una attenta valutazione dei progetti e programmi di ricerca avviati dai *competitors* e il monitoraggio di flussi internazionali (farmaci e dispositivi), anche attraverso la collaborazione con *stakeholders* privati;
- **Definizione dei parametri di interesse:** identificare i possibili agenti e dispositivi di interferenza cognitiva, così come i parametri sulla base dei quali valutare programmi e progetti di ricerca dei *competitors* e la valutazione delle strategie di influenza perpetrate, risultano determinanti per disporre di un quadro di situazione aggiornato che consenta di comprendere la reale portata della minaccia;
- **Monitoraggio dei flussi internazionali:** al fine di assicurare una piena comprensione del fenomeno andrà effettuato un attento monitoraggio dei flussi internazionali di agenti, componenti e programmi. In particolare, per sopperire anche all’attuale impossibilità di contrastare la diffusione e l’impiego di farmaci “*off label*”, andrà effettuato un attento monitoraggio dei flussi di farmaci e dispositivi di possibile interferenza cognitiva;
- **Monitoraggio delle aree di interesse strategico:** la possibilità di trovarsi ad operare in contesti in cui sono presenti attori che potrebbero trovarsi in condizioni “alterate” dovute all’utilizzo di agenti farmacologici⁶¹ o altri strumenti di interferenza cognitiva, richiede un’attenta valutazione preliminare nella considerazione della difficoltà di contrastare tali soggetti. La Difesa dovrà, pertanto, condurre un attento monitoraggio dei flussi verso le aree di interesse strategico. Inoltre, al fine di effettuare un’attenta

⁶¹ I cosiddetti *Performance Enhancement Drugs* (PED).

attività di prevenzione e contrasto, dovrà valutare la possibilità di disporre di specifiche figure professionali (farmacologi, tossicologi, ecc.), anche attraverso la costituzione di un bacino di professionalità da cui poter attingere per esigenze specifiche.

c. Ricerca e sviluppo tecnologico

Particolarmente rilevante, per comprendere e affrontare le future sfide, appare il ruolo della ricerca, anche a supporto dello sviluppo tecnologico e risulta necessario presidiare i contesti di interesse anche attraverso l'istituzione di specifiche posizioni da ricercatore in contesti sinergici (Accademia, Ricerca, Industria e Difesa). In tal senso, possono essere individuati i seguenti elementi principali:

- **Supporto alla ricerca nazionale:** il nostro Paese dispone di assolute eccellenze che, tuttavia, come in molte delle democrazie occidentali, spesso si trovano ad operare in un quadro etico-giuridico di riferimento particolarmente stringente rispetto ai *competitors* internazionali. Pertanto, andrà assicurato il necessario supporto nazionale al settore della ricerca nella considerazione che tale situazione rappresenta un elemento di asimmetria strategica a favore degli avversari, anche in ambito militare.
- **Partecipazione a programmi internazionali:** data l'attenzione dedicata in ambito internazionale al tema del *Cognitive Warfare* e l'evoluzione tecnologica nel settore della modulazione di energia al cervello, anche per il possibile sviluppo di sistemi a energia diretta, con possibili risvolti in termini di capacità militari, risulta necessario assicurare la partecipazione della Difesa ai tavoli internazionali, promuovendo la partecipazione dei Centri di ricerca nazionali allo scopo di garantire il mantenimento e la condivisione delle conoscenze scientifiche, tecniche e tecnologiche nello specifico segmento e un coerente e armonico sviluppo nazionale;
- **Costituzione di un Comitato Etico per l'Innovazione della Difesa:** le implicazioni correlate allo sviluppo di interfacce neurali impiegate in contesti militari implica una profonda riflessione sulla necessità militare di disporre di strumenti di ausilio in contesti sempre più complessi, contesi e congestionati in cui si riducono i tempi decisionali per orchestrare risposte efficaci e che potrebbero comportare l'insorgere di una superiorità cognitiva da parte degli attori che, prima di altri, potranno ricorrere a tali strumenti. Pertanto, a garanzia del pieno rispetto dei valori democratici e dell'indirizzo politico nazionale, e tenendo in debita considerazione la crescente necessità militare correlata ai rischi della competizione cognitiva, risulta ineludibile la costituzione di un Comitato Etico per l'Innovazione della Difesa che possa esprimere un parere informato e competente su innovativi progetti di ricerca militare inerenti il *Cognitive Warfare*, da sviluppare attraverso contesti sinergici con Accademia, Ricerca e Industria;

- **Sviluppo di progetti di ricerca militare:** in considerazione della valenza strategica conseguente all'applicazione in campo militare di interfacce neurali, risulterà necessario, preferibilmente sulla base degli indirizzi dell'auspicato Comitato Etico per l'Innovazione della Difesa, avviare specifici progetti di ricerca volti a valutare l'idoneità di impiego attraverso lo sviluppo di specifici scenari (*scenario-design*) e, al contempo, sviluppare le necessarie capacità di contrastare/neutralizzare l'impiego di tali strumenti da parte di un possibile avversario. Inoltre, al fine di garantire la possibilità di sviluppare eventuali sistemi a energia diretta, anche offensivi, e le necessarie misure di *detection* e contrasto, risulterà necessario valutare la possibilità di avviare anche specifici progetti di ricerca militare nel settore.

d. Integrazione effetti cinetici - non cinetici

Se da un lato, l'attuale contesto internazionale conferma la centralità delle capacità convenzionali, dall'altro l'evoluzione del *Cognitive Warfare* enfatizza la rilevanza delle capacità non cinetiche anche quali abilitanti della manovra classica. Risulta, quindi, necessario che la Difesa sviluppi sempre più una propria capacità di integrazione e sincronizzazione degli effetti cinetici e non cinetici e valuti, qualora necessario, anche lo sviluppo e il dimensionamento della componente non cinetica. In tale linea di indirizzo d'intervento possono essere declinati i seguenti elementi principali:

- **Potenziamento della capacità di comunicazione:** la varietà e complessità degli attuali scenari operativi hanno determinato l'esigenza di affiancare alle operazioni militari classiche forme di intervento di tipo "non letale". In tale ambito, ha assunto un ruolo preponderante la "strategia comunicativa" (narrativa) verso la popolazione locale e i suoi *leader*, finalizzata all'esercizio del massimo sforzo da dedicare alla costruzione del consenso attraverso il dialogo, quale fattore di successo nelle missioni. Una delle risorse più efficaci per un Comandante per il conseguimento dei propri obiettivi di missione in Teatro Operativo può essere rappresentata dalla capacità di sviluppare delle *performance* efficaci nel campo comunicativo attraverso tutti gli strumenti a sua disposizione. In tale quadro, risulta fondamentale una gestione consapevole dei rapporti con i *leaders-key communicators* i quali, negli scenari attuali, devono essere considerati tra i *main actors*, a beneficio del conseguimento degli obiettivi della missione.

La Difesa dovrà quindi informare la propria azione comunicativa verso la promozione di un sentimento favorevole utile a sostenere, in particolare nelle aree di interesse strategico, un approccio preventivo che possa limitare, almeno inizialmente, la portata di strategie di influenza avversarie. Inoltre, al fine di monitorare l'ambiente informativo, dovranno essere acquisiti e sperimentati specifici *tools* di *marketing* che consentano di svolgere funzioni di ingaggio, ascolto, monitoraggio e *network analysis*

in grado di coinvolgere individui, gruppi e *communities* e di misurare l'efficacia della *performance* comunicativa. Per massimizzare l'efficacia dell'azione comunicativa dovranno essere sviluppate nuove modalità di creazione di contenuti che, attraverso l'azione di indirizzo della Comunicazione Strategica, possano consentire di coinvolgere l'*audience* attraverso aspetti identitari, culturali ed emotivi a livello operativo e tattico, anche attraverso lo sviluppo e l'impiego di strumenti per l'elaborazione del linguaggio naturale;

- **Addestramento all'integrazione degli effetti:** la crescente rilevanza della competizione nella dimensione cognitiva richiederà una sempre maggiore consapevolezza della portata degli effetti non cinetici in tutte le fasi di una campagna militare. Occorre pertanto sviluppare una sempre maggiore capacità di integrazione degli effetti cinetici e non cinetici attraverso un processo di progressivo e costante addestramento e aggiornamento del personale, anche in funzione delle capacità/strumenti che si renderanno via via disponibili e l'implementazione e l'impiego di strumenti di simulazione dell'evoluzione dell'ecosistema informativo. Inoltre, in funzione dell'evoluzione del *Cognitive Warfare*, potrà risultare necessario aggiornare l'attuale processo di pianificazione e condotta delle operazioni per assicurare la rilevanza della dimensione cognitiva, sviluppando anche specifici indicatori di monitoraggio della *performance*;
- **Sviluppo del vantaggio informativo:** nell'ambito della Funzione Operativa *Intelligence* (per sua natura interforze, inter-agenzia e intergovernativa), occorrerà acquisire una superiorità nella raccolta informativa, che si espanderà di pari passo con l'avanzare del mondo digitale, soprattutto in considerazione dell'incalzante evoluzione dell'*Internet of Things* (IoT), che troverà sempre maggiore applicazione in ambito militare (*Internet of Military Things* - IoMT), anche in funzione del crescente numero di piattaforme e sistemi connessi nello spazio di battaglia digitalizzato ed esteso. Parallelamente, per garantire la possibilità di esercitare efficacemente il Comando e Controllo nelle Operazioni Multidominio sarà fondamentale ricercare e mantenere il vantaggio informativo, ossia una condizione in cui le forze militari mantengono l'iniziativa in termini di uso, diniego e manipolazione delle informazioni, al fine di ottenere la comprensione della situazione (*situational understanding*), ottimizzare il processo decisionale e influenzare il comportamento degli attori in campo. L'uso, il diniego e la manipolazione delle informazioni può essere ritenuto intrinsecamente un aspetto Multidominio: assicurarsi il vantaggio informativo – attraverso azioni *cross-domain* che vedono impiegate tutte le capacità a disposizione di una forza militare – contribuisce a creare quelle finestre di opportunità per ottenere un vantaggio operativo sull'avversario. Al riguardo, considerata l'importanza dei dati e la natura temporanea delle informazioni in relazione agli effetti che si possono conseguire nella dimensione

cognitiva, il vantaggio operativo, che si può ottenere da un'informazione, degrada rapidamente nel tempo;

- **Implementazione di nuove soluzioni tecnologiche:** nell'ambito della competizione nella dimensione cognitiva, anche la ricerca e lo sviluppo tecnologico assumono sempre maggiore valenza di competizione strategica. Pertanto, al fine di garantire la necessaria competitività rispetto ai potenziali avversari, risulterà necessario promuovere la celere implementazione di nuove soluzioni tecnologiche attraverso un processo di innovazione della Difesa che colga le opportunità già dalla ricerca di base, consenta una rapida sperimentazione e validazione delle nuove soluzioni e assicuri una veloce introduzione in servizio di nuovi strumenti e capacità per garantire una sempre maggiore capacità di integrazione tra effetti cinetici e non cinetici.



RILEVANZA DIMENSIONE COGNITIVA



COMPRESIONE DELLA MINACCIA

RICERCA E SVILUPPO TECNOLOGICO

INTEGRAZIONE EFFETTI CINETICI





Monitoraggio
aree interesse
strategico



Monitoraggio
Flussi
internazionali



Sviluppo progetti
di ricerca
militare



Costituzione
Comitato Etico
Innovazione



Partecipazione
programmi
internazionali

ETICI-NON CINETICI



Implementazione
nuove soluzioni
tecnologiche



Sviluppo
vantaggio
informativo



Addestramento
integrazione
effetti

LE OPERAZIONI INFORMATIVE RUSSE

Il controllo e l'influenza della sfera informativa sono emersi nella discussione strategica russa a partire dalla seconda metà degli anni '90. In questi anni, il controllo dei flussi di informazione viene soprattutto concepito come una tematica inerente alla protezione (o interferenza) nei sistemi *Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance* (C4ISR). La trasmissione delle informazioni fra i comandi, le unità sul campo e, in parte, le autorità politiche vengono in questi anni concepiti come un tema che finalmente evolve dalla classica salvaguardia dello spettro elettromagnetico e assume una dimensione tattica e operativa a sé stante. La gestione dei flussi di informazione diventa in questi anni una problematica più vicina all'ottimizzazione del OODA⁶² *Loop* dei Comandanti e delle forze sul campo, aprendo la strada all'integrazione dell'elemento cognitivo nelle operazioni. Vecchie pratiche come la *maskirovka*⁶³ e l'interferenza in operazioni combinate vengono riproposte e concettualizzate nel tentativo di fornire alle Forze Armate russe lo strumento per rafforzare e accompagnare azioni convenzionali. L'obiettivo primario di quelli che verranno poi definiti "colpi informativi" (*infomazionnyi udar*) è quello di disorganizzare e confondere le truppe avversarie nei momenti precedenti e contemporanei a un'operazione cinetica, combinando ad esempio disinformazione mirata con attacchi d'artiglieria per applicare pressione su unità nel corso di un'operazione informativa⁶⁴.

Il nuovo ruolo della sfera cognitiva nella teoria operativa russa si è affermata soprattutto a partire dalle riforme militari nella seconda metà degli anni 2000, quando le Forze Armate russe iniziano a ragionare a un passaggio verso quella che viene definita "*Non-contact Warfare*". L'enfasi viene posta sull'utilizzo di missili ad alta precisione e portata, l'utilizzo massiccio di guerra elettronica e, in generale, la degradazione dei sistemi di sistemi avversari come preconditione necessaria a uno scontro convenzionale⁶⁵. L'obiettivo, in sostanza, è favorire successive operazioni militari massimizzando la disorganizzazione dell'avversario e creare una situazione di incertezza permanente⁶⁶.

⁶² *Observe, Orient, Decide, Act.*

⁶³ La *maskirovka*, letteralmente mascheramento-camuffamento, è l'insieme di azioni di depistaggio visivo, disinformazione e psicologia applicata, per far credere agli avversari qualcosa che non è vero. Elaborata negli anni Venti, rivisitata all'indomani dell'Operazione Barbarossa del 1941, essa arriva fino ai giorni nostri. La *maskirovka* è dunque l'evoluzione di una pratica che risale agli albori dell'era sovietica affinata negli anni della Guerra Fredda.

⁶⁴ Vorobyev I.N. Information-strike operation. *Voennaya Mysl*, No. 6. 2007

⁶⁵ "Russian Military Thought on the Changing Character of War: Harnessing Technology in the Information Age," *Jamestown*, <https://jamestown.org/program/russian-military-thought-on-the-changing-character-of-war-harnessing-technology-in-the-information-age/>.

⁶⁶ Kofman, M., Fink, A., Gorenburg, D., Chesnut, M., Edmonds, J., & Waller, J. (2021). *Russian Military Strategy: Core Tenets and Operational Concepts*. CNA.

È proprio qui che il termine “sfera cognitiva” viene per la prima volta utilizzato per indicare il travolgimento delle capacità cognitive dei Comandanti e l’interferenza nei flussi informativi necessari alla gestione della “*network-centric warfare*” (*setezentricheskaya voyna*)⁶⁷.

Quest’approccio sistemico vedrà poi la maturazione in Ucraina a partire dal 2014, e poi di nuovo nel 2022. L’amplificazione delle azioni cinetiche e l’azione preventiva per la preparazione di operazioni militari è stata individuata da molti ricercatori ucraini come uno dei principali ingredienti delle campagne russe in questi anni. Analisti ucraini, soprattutto, vedono le operazioni russe come misure volte a creare “*significant difficulties in identifying the sources of aggression, its scale and goals, methods and forms, instruments*” e compromettere la coesione fra Forze Armate e autorità politiche⁶⁸. Nella pratica, le misure sono quasi sempre gestite dalle unità di guerra elettronica⁶⁹ e comprendono: il disturbo di segnali GPS e radio satellitari; l’utilizzo di specifici *payload* di *jamming* sui droni Orlan 10 per colpire la telefonia mobile o rilevare e disturbare i radar di controbatteria; la trasmissione mirata di messaggi intimidatori sui telefoni personali dei soldati nemici o l’invio mirato di SMS contenenti virus che consentono l’intercettazione del telefono. A ciò si aggiungono azioni *cyber* come il sabotaggio delle interfacce digitali di ministeri e enti governativi e la diffusione di *deepfake* di *Leader* e Comandanti⁷⁰ per seminare confusione su ciò che sta effettivamente succedendo.

Allo stesso tempo, le operazioni di influenza sono state progressivamente percepite come uno strumento strategico-politico oltre che puramente militare. In questo ambito è evidente che l’esperienza del crollo sovietico e delle “rivoluzioni colorate⁷¹” abbia definito la percezione dell’ambito informativo come quello nel quale è possibile raggiungere obiettivi politici con azioni al di sotto della soglia di un conflitto cinetico.

Una tendenza diffusa consiste nell’individuare l’origine di tale approccio nell’articolo di Valery Gerasimov del 2013⁷², nel quale il Capo di Stato Maggiore russo sosteneva che i conflitti moderni implicano un rapporto di 4 a 1 nell’uso di misure rispettivamente non-

⁶⁷ Skokov S.I., Grushka L.V. Influence of Network-centrism concept on evolution and functioning of management system of the Armed Forces of the Russian Federation. *Voennaya mysl'* no. 12, 2014.

⁶⁸ Michelle Grisé et al., *Russian and Ukrainian Perspectives on the Concept of Information Confrontation: Translations, 2002–2020* (RAND Corporation, August 18, 2022), https://www.rand.org/pubs/research_reports/RRA198-7.html.

⁶⁹ Le *Cyber Electro Magnetic Activities* (CEMA) consistono nella sincronizzazione, coordinamento e integrazione di attività cibernetiche ed elettromagnetiche che assicurano un vantaggio operativo inibendo e/o degradando l’utilizzo dello spettro elettromagnetico e del cyberspazio da parte dell’avversario. Risultano un abilitante fondamentale: della ricerca informativa, fornendo la necessaria *situational awareness* per accelerare i propri processi decisionali e ostacolare quelli avversari; del C2, attraverso la difesa dei propri sistemi e l’attacco di quelli avversari; della manovra informativa, veicolando i prodotti della comunicazione operativa tesi sia a guadagnare il consenso sia a indebolire la volontà di combattere l’avversario.

⁷⁰ Laurent Borzillo, “Le combat cyberélectronique russe en Ukraine,” *Le Rubicon*, 8 juillet 2022, <https://lerubicon.org/publication/le-combat-cyberelectronique-russe-en-ukraine/>.

⁷¹ Movimenti di protesta avvenuti a seguito della trasformazione dei paesi socialisti europei successivamente al 1989. Tali proteste hanno adottato un colore (es. arancio Ucraina, rosa Georgia, ecc.) come simbolo per identificare i loro sostenitori e il carattere del movimento.

⁷² Valery Gerasimov, “*The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations*” in *Voyenno-Promyshlenny Kurier* (VPK) (Military-Industrial Courier), 27 February 2013.

militari e militari da parte degli attori coinvolti. Tuttavia, lungi dall'illustrare un approccio unicamente russo al modo di fare la guerra e con una chiara priorità agli elementi cognitivi, economici e informativi, Gerasimov parlava soprattutto della percezione russa delle dottrine occidentali: *"In his view, the West pioneered indirect approaches to warfare, leveraging political subversion, propaganda, and social media, along with economic measures such as sanctions. From his perspective, humanitarian interventions, the use of Western special forces, funding for democracy movements, and the deployment of mercenaries and proxies were all features of a U.S. doctrine of indirect warfare"*⁷³.

Questo malinteso è fondamentale per capire la maniera con cui i russi approcciano la sfera cognitiva nell'ambito strategico, soprattutto perché si basa su un'analisi sostanzialmente errata dei movimenti popolari nati dopo il 1991 e le dinamiche che hanno portato al crollo dell'Unione Sovietica⁷⁴. Non potendo concepire questi eventi se non come il risultato di influenze esterne e azioni politiche pilotate dall'Occidente, gli strateghi russi hanno individuato nella manipolazione a lungo termine della coscienza pubblica una vera e propria tecnologia psicologico-informativa. Aleksandr Bartosh, dell'Accademia per le Scienze militari, parla ad esempio della gestione occulta di *"motivazioni diverse e non sempre consapevoli e, in generale, del comportamento di un'ampia gamma di partecipanti agli affari pubblici"*. Grazie al controllo occulto di vari canali (ad esempio internet, televisione, letteratura, programmi educativi, ONG e sette religiose), l'entità colpita *"perde gradualmente la sensibilità" all'influenza distruttiva e accetta volontariamente un nuovo modello cognitivo"*⁷⁵. Questa lettura sembra in sostanza guidata più dalla necessità di giustificare una politica di censura e repressione dello spazio informativo domestico, sfociata in ultima analisi in misure come la legge sugli "agenti stranieri"⁷⁶, piuttosto che una concettualizzazione analiticamente solida della strumentalizzazione dello spazio informativo. Ciò non ha ovviamente impedito alle autorità russe di provare a sfruttare queste conclusioni in operazioni d'influenza all'estero. In Europa, i risultati da esse ottenute sono stati per lo più modesti⁷⁷ e legati soprattutto a contingenze politiche locali. In Italia, ad esempio, i tentativi di disinformazione e propaganda hanno avuto effetti marginali rispetto a quelli di un ecosistema informativo e politico già di per sé polarizzato, limitando le azioni russe all'amplificazione di posizioni già presenti⁷⁸.

⁷³ Michael Kofman, "Russian Hybrid Warfare and Other Dark Arts," *War on the Rocks*, March 11, 2016, <https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/>.

⁷⁴ Nikitina, Yulia. "The "Color Revolutions" and "Arab Spring" in Russian Official Discourse." *Connections* 14.1 (2014): 87-104.

⁷⁵ Alexander Bartosh, "Linguistic Security of the Country," *Independent Military Review*, last modified February 14, 2014, accessed October 4, 2022, http://nvo.ng.ru/concepts/2014-02-14/1_model.html.

⁷⁶ <https://www.rferl.org/a/putin-signs-off-harsher-foreign-agent-law/31943645.html>

⁷⁷ "Russia Fails in German Disinformation Campaign," *CEPA*, last modified November 15, 2021, 2022, <https://cepa.mystagingwebsite.com/article/russia-fails-in-german-disinformation-campaign/>.

⁷⁸ Michelangelo Freyrie, "Propaganda, il 'quarto potere' diffuso di Putin in Italia," *Affari Internazionali - Politica ed economia estera*, 10 maggio 2022., <https://www.affarinternazionali.it/propaganda-il-quarto-potere-diffuso-di-putin-in-italia/> e Michelangelo Freyrie, "Manuale di interferenza | Come la Russia organizza le sue operazioni politiche all'estero," *Linkiesta.it*, 30 luglio, 2022, <https://www.linkiesta.it/2022/07/russia-lega-politica/>.

È evidente che questa realtà è ben lontana dall'illusione russa di poter vincere una guerra senza neanche sparare un colpo o di poter provocare instabilità durature simili a quelle che hanno portato al collasso dei regimi arabi e post-sovietici. La pesante campagna di disinformazione ai danni del legittimo governo ucraino⁷⁹, ad esempio, o il tentativo di privare Kiev del supporto occidentale,⁸⁰ hanno avuto per ora effetti sostanzialmente nulli. Quello che è un elemento di debolezza nel contesto europeo si è tuttavia rivelato un punto di forza nel contesto africano. La capacità di inserirsi in conflitti e narrazioni preesistenti, come l'ostilità nei confronti dei Paesi europei (e la Francia in particolare), ha permesso alla Russia di guadagnare una buona reputazione sul continente. In tal senso, le massicce campagne di disinformazione e propaganda *on-line* hanno grandemente favorito le manifestazioni dell'*hard power* russo, che si tratti del contributo militare tramite i mercenari della compagnia ChVK Wagner oppure contratti di sfruttamento minerario. La chiave per comprendere il successo di queste campagne rimane in ogni caso il supporto da parte dei regimi e governi locali, che trovano nel supporto russo una "opzione esterna" politicamente più appetibile delle alleanze con gli Stati occidentali.⁸¹ L'intesa con la giunta del Mali, in tal senso, è esemplare.⁸²

Alla luce di ciò, risulta difficile pensare che questo tipo di avvicinamento politico, seppur facilitato da propaganda mirata, possa realmente essere giudicata quale ricorso a una cassetta degli attrezzi "cognitiva". Essa non sembra infatti basarsi primariamente su un radicale intervento sul OODA *Loop* dei governanti o di un'alterazione della percezione africana della realtà – almeno né più né meno di quanto non lo faccia qualsiasi tipo di azione politico-diplomatica. Non sono attualmente pubblicamente note iniziative analoghe al progetto "*Brain*" nel contesto russo, anche se non può esserne esclusa l'esistenza.

⁷⁹ Justin Ling, "Russia Launches Social Media Offensive Alongside Missiles," *Foreign Policy*, 24 February 2022, accessed October 4, 2022, <https://foreignpolicy.com/2022/02/24/russia-ukraine-attack-social-media-telegram/>.

⁸⁰ "'Grotesque' Russian Disinfo Campaign Mimics Western News Websites to Sow Dissent," *POLITICO*, last modified September 27, 2022, <https://www.politico.eu/article/russia-influence-ukraine-fake-news/>.

⁸¹ "Russia Has Made Worrying Inroads into Africa," *Financial Times*, September 4, 2022.

⁸² Neil Munshi, "How France Lost Mali: Failure to Quell Jihadi Threat Opens Door to Russia," *Financial Times*, December 22, 2021.

LA GUERRA COGNITIVA CINESE

Sin dalla fine della Guerra Fredda, l'Esercito Popolare di Liberazione (EPL) ha affrontato un processo di modernizzazione che si poneva l'obiettivo di affrontare il superamento della "mobilitazione totale" e preparare le forze armate a conflitti locali, brevi, net-centrici e con un'organizzazione interforze. Questo cambio epocale è stato stimolato da uno scenario strategico che è lentamente ma progressivamente diventato ostile a Pechino, con un'accelerazione dall'inizio della pandemia causata dal virus SARS-CoV2.

In particolare, non sono passati inosservati la vittoria della coalizione occidentale nella Guerra del Golfo (2 agosto 1990 - 28 febbraio 1991) che fu rapida, decisiva e guidata dalla tecnologia che ha portato alla Rivoluzione negli Affari Militari (RAM); la terza crisi dello stretto di Taiwan (1995/1996) che vide coinvolti gli Stati Uniti; il bombardamento statunitense dell'ambasciata cinese a Belgrado (7 maggio 1999). Tali preoccupazioni sono ulteriormente accresciute di conseguenza al "Pivot To Asia" dell'amministrazione Obama, alla continuazione di tale politica da parte dell'amministrazione Trump, oltre alla guerra commerciale e le pressioni su Hong Kong e Xinjiang, al tentativo dell'amministrazione Biden di allineare o riallineare i partner dell'Indo-Pacifico a Washington, attraverso piattaforme diplomatico-militari quali il *Quadrilateral security Dialogue* (Quad), l'*Indo-Pacific Economic Framework* (IPEF) e AUKUS (patto di sicurezza trilaterale tra Australia, Regno Unito e Stati Uniti). Viste da Pechino, queste azioni hanno portato a un senso di "accerchiamento" nell'Indo-Pacifico e rivelano una "mentalità da Guerra Fredda"⁸³.

Il marxismo, insieme al pensiero di Sun Tzu, ricoprono un ruolo centrale nel pensiero strategico cinese. Il concetto di "materialismo dialettico" sottolinea l'importanza delle condizioni del mondo reale e le contraddizioni all'interno delle relazioni. Nella strategia cinese questo concetto implica una dialettica fra oggettivo-soggettivo: in pratica, gli strateghi cinesi sviluppano "stratagemmi" basati su una valutazione delle condizioni materiali che devono affrontare in un dato momento.⁸⁴ La tensione tra condizioni oggettive e pensiero soggettivo viene utilizzata per produrre in modo creativo vantaggi strategici (*Shi*) per manipolare un problema o un avversario. Questo potrebbe, ad esempio, includere lo studio di *hobby*, punti deboli e difetti di Comandanti avversari, ma anche perseguire "solo una certa vittoria", evitando "battaglie decisive sfavorevoli". In altre parole, gli strateghi cinesi si concentrano sul "potenziale di una situazione"⁸⁵, mentre gli occidentali sono abituati a prendere decisioni basate su prescrizioni come le *courses of action*.

⁸³ State Council Information Office of the People's Republic of China (2019) White Paper: China and the World in the New Era. July 10. hr.china-embassy.gov.cn/eng/gdxw/201910/t20191007_2561455.htm

⁸⁴ Thomas, T.L. (2020) *CHINA - Military Strategy: Basic Concepts and Examples of its Use*.

⁸⁵ Orinx, K. and de Swielande, T.S. (2022) 'China and Cognitive Warfare: Why Is the West Losing?'. Bernard Claverie; Baptiste Prébot; Norbou Beuchler; François du Cluzel. 'Cognitive Warfare: The Future of Cognitive Dominance'. NATO Collaboration Support Office. fffhal-03635930f, p. 8.

Nonostante Sun Tzu e Marx abbiano vissuto in epoche molto distanti e diverse fra loro, questo approccio è in sinergia con alcuni concetti del pensiero di Sun Tzu, quali “conosci il tuo nemico” e “vincere senza combattere”. Tuttavia, è opportuno ricordare che dalla Prima Guerra dell’Oppio (1839-1842) la Cina si è relazionata con un sistema internazionale costruito dall’Occidente; pertanto la cultura strategica cinese, pur rimanendo generalmente ancorata a valori dalla tradizione millenaria, ha nel tempo subito “contaminazioni”, recependo alcuni tratti di quella occidentale.

L’importanza di concetti quali la guerra cognitiva assume ancora più interesse se contestualizzate nel sistema politico cinese. Alla base della grande strategia della Cina c’è la relazione simbiotica fra Partito Comunista Cinese (PCC) e industrie in settori strategici che rimangono sotto il controllo statale diretto o indiretto. Tale relazione rappresenta il cuore della potenza cinese. Infatti, in un libro bianco del governo di Pechino veniva fatto notare che “il sistema politico della Cina stabilito dalla Costituzione” rientra fra i cosiddetti “interessi principali” non negoziabili.⁸⁶ Tale sistema rappresenta la colonna portante dello storico successo della Cina, ma anche la principale causa dello scontro odierno con gli USA⁸⁷.

La sinergia strategica che tale sistema costituzionale agevola mette la Cina in una posizione privilegiata per poter investire con maggiore efficienza sul futuro dell’economia mondiale e della guerra, ovvero le tecnologie a doppio uso. A tal fine, la Cina vuole spingersi oltre e affinare questo sistema di cooperazione con la dottrina della “fusione civile-militare”, definita dagli USA come “eliminazione delle barriere fra ricerca civile e settori commerciali da una parte, e industria della difesa dall’altra”⁸⁸. Di fatto, si punta alla creazione di un sistema nazionale politico-militare-scientifico che possa fare rete su questioni di importanza strategica. Come sottolineato da Xi Jinping all’interno della Commissione Centrale per lo Sviluppo Militare e Civile Integrato (CCIMCD), la parola d’ordine rimane “unificare”, che già era una costante nel sistema politico-industriale cinese, e diventa oggi “più serio e supportato da maggiore risorse”⁸⁹. L’obiettivo di tale impegno di coordinazione è quello di rendere la Cina *leader* mondiale nel settore dell’Intelligenza Artificiale (IA). Infatti, Pechino ritiene che l’IA determinerà la prossima rivoluzione negli Affari Militari e che il Paese che prima di ogni altro saprà applicare la IA alla prossima generazione dell’arte bellica otterrà la supremazia militare⁹⁰.

Tale contesto sociale e istituzionale, parallelamente a un ambiente internazionale sempre più sfavorevole a Pechino, ha favorito l’integrazione di un sempre più alto grado di tecnologia in campo militare. Questa necessità è stata interpretata fin dalla fine della Guerra

⁸⁶ http://english.www.gov.cn/archive/white_paper/2014/09/09/content_281474986284646.htm

⁸⁷ Leoni, Z. (2021) *American Grand Strategy from Obama to Trump: Imperialism After Bush and China’s Hegemonic Challenge* (Cham: Palgrave), chapter 3

⁸⁸ US Department of State, 2020. Military-Civil Fusion and the People’s Republic of China. May. [Shttps://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Page.pdf](https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Page.pdf), p. 1.

⁸⁹ L. Laskai, 2018. Civil-Military Fusion and the PLA’s pursuit of dominance in emerging technologies. *The Jamestown Foundation – China Brief*. April 9. <https://jamestown.org/program/civil-military-fusion-and-the-plas-pursuit-of-dominance-in-emerging-technologies/>

⁹⁰ Laskai, op. cit., n. 30.

fredda dalle massime cariche della Repubblica Popolare Cinese. Dal 1993 il presidente Jiang Zemin sosteneva che la Cina non avrebbe più combattuto solamente “guerre locali in condizioni moderne” – come nell’era di Deng Xiaoping – ma che avrebbe dovuto prepararsi a combattere “guerre locali in condizioni altamente tecnologiche e moderne”.⁹¹ Da quel momento in avanti, l’enfasi dei presidenti cinesi sul fattore tecnologico in guerra si è fatta sempre più marcata, fino ad evolvere nel concetto di “guerre locali informatizzate” promosso da Xi Jinping nel 2015, a voler sottolineare che il carattere del conflitto è evoluto a un confronto tra “sistemi di sistemi basati sull’informazione”. Come nei decenni precedenti, con il cambiare dell’ambiente strategico e il miglioramento della tecnologia militare cinese, la dottrina militare si è evoluta. Gli strateghi cinesi stanno già pensando ad un superamento dell’informatizzazione del conflitto, e all’emergere del concetto di “intelligentizzazione” ovvero la guerra caratterizzata da un ruolo centrale dell’Intelligenza Artificiale. Rispetto alla guerra informatizzata, questo nuovo concetto richiede una maggiore velocità nell’elaborazione delle informazioni e delle decisioni, oltre all’uso di sciame di droni e la guerra cognitiva.⁹²

Quando si parla di IA e del dominio cognitivo, il dibattito nella comunità scientifico-militare cinese guarda con maggiore interesse all’ “intelligenza ibrida” (混合智能) ovvero alla ricerca di sinergie fra cervello umano e algoritmo.⁹³ Secondo il Ten. Generale Liu Guozhi, direttore della Commissione per la Scienza e Tecnologia all’interno Commissione Militare Centrale, l’intelligenza ibrida diventerà “la forma di intelligenza più elevata” e si svilupperà come un’interfaccia computer-cervello finalizzato al “potenziamento delle prestazioni umane”. L’interfaccia è considerata necessaria dalla Cina perché si prevede che “il ritmo e la complessità delle operazioni aumenteranno, forse drammaticamente” e il cervello umano viene visto da alcuni come “un nuovo spazio di combattimento”. Di fatto, mentre in molti si chiedono se le macchine possano sostituire le persone con l’umanizzazione dei robot, è verosimile ipotizzare che si assista a una tendenza di robotizzazione degli umani, con l’obiettivo di creare un super-soldato che diventi un tassello all’interno della rete di guerra. Sebbene la creazione di un super-soldato sia al centro del dibattito cinese, gli sviluppi della guerra cognitiva da un punto di vista di Pechino guardano tutti all’evoluzione dell’IA che apre ampie possibilità nel dominio cognitivo. C’è chi considera la guerra cognitiva come un’estensione del concetto di disinformazione⁹⁴, ma anche chi parla di “interferenza diretta” e “controllo inconscio del cervello”, causando anche “danni mentali, confusione e allucinazioni nel nemico”, con l’obiettivo di costringerlo a “deporre le armi” prima di combattere e ad arrendersi.

⁹¹ Burke, E.J. et al. (2020) People's Liberation Army Operational Concepts. RAND. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA300/RRA394-1/RAND_RRA394-1.pdf, p. 3

⁹² Takagi, K. (2022) *The future of China's cognitive warfare: lessons from the war in Ukraine*. War on the Rocks. July 22. <https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine/>

⁹³ Kania EB. Minds at war: *China's pursuit of military advantage through cognitive science and biotechnology*. Prism. 2020;8(3), p. 83

⁹⁴ Hung, TC, and Hung, TW (2020) *How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars*. Journal of Global Security Studies, 7(4), 1-18

RECIPROCIÀ E NORME SOCIALI

Come evidenziato già da alcuni famosi esperimenti di Solomon Asch risalenti agli anni 50, le persone tendono ad essere fortemente influenzate dalle opinioni altrui, anche quando queste ultime portano a conclusioni palesemente errate. Questi meccanismi sono sostenuti dalle cosiddette norme sociali, che regolano il comportamento umano in tutte le società e organizzazioni umane. Attraverso le norme sociali, definiamo quali siano i comportamenti accettabili e quelli deprecabili e le informazioni che dovremmo (o non dovremmo) condividere. In altre parole, le norme sociali sostengono gli individui nella selezione dei comportamenti da mettere in atto nella loro vita quotidiana. Tra queste norme sociali, gioca un ruolo fondamentale un meccanismo peculiare, quello della reciprocità dell'influenza sociale. Nel 2021, Joshua Zonca, Alessandra Sciutti e Anna Folso, ricercatori della linea di ricerca *Contact* dell'Istituto Italiano di Tecnologia (IIT), attraverso una serie di esperimenti con partecipanti umani hanno scoperto che più alta è la considerazione di cui godiamo all'interno di un gruppo, maggiore sarà la nostra tendenza a fidarci delle opinioni degli altri e mostrarci accondiscendenti verso essi. Se invece le nostre idee sono poco valorizzate all'interno di un gruppo, tenderemo a dissentire dalle opinioni altrui. In altre parole, lo scambio di informazioni tra esseri umani segue delle norme sociali, che ci spingono a mostrarci più concordi verso le idee degli altri per mantenere saldi i nostri rapporti sociali e, quindi, ricevere maggiore considerazione in futuro. Se da un lato questo fenomeno potrebbe portarci ad essere più ricettivi rispetto alle idee altrui, dall'altro potrebbe portarci a dare eccessivo peso a notizie false o opinioni di fonti poco attendibili. Questa scoperta evidenzia la facilità con cui il contesto sociale può influenzare i nostri processi decisionali e la nostra percezioni degli altri. Gli stessi ricercatori hanno anche scoperto che questo fenomeno emerge già all'età di 10 anni, mentre bambini più piccoli non hanno ancora sviluppato le competenze "sociali" che sostengono la capacità di aderire a norme sociali complesse.

Nello specifico, i risultati di un esperimento che prevedeva l'interazione di bambini dai 6 ai 10 anni con un adulto hanno mostrato che i bambini più piccoli, fino a 8 anni, tendono ad essere poco compiacenti e si fidano più di se stessi che dell'adulto, indipendentemente dal loro comportamento. Dai 10 anni, invece, emerge un atteggiamento analogo a quello degli adulti: i bambini danno più rilevanza alle opinioni degli adulti se gli adulti danno loro credito. Zonca, Sciutti e colleghi si sono spinti oltre e hanno testato se la reciprocità dell'influenza sociale può emergere addirittura mentre interagiamo con un *robot* sociale umanoide, ovvero un *robot* con fattezze e comportamenti ispirati all'umano.

La risposta a questo quesito è che l'interazione con questi *robot* genera meccanismi di reciprocità, sebbene questi meccanismi siano meno forti e pervasivi di quelli osservati nell'interazione sociale tra esseri umani. In particolare, i risultati di questi studi hanno mostrato che le persone tendono a fidarsi maggiormente di un robot quando quest'ultimo si è mostrato disposto a fidarsi del suo compagno d'interazione umano.

Questi risultati si aggiungono ad una serie di studi internazionali in cui si evidenzia come la fiducia che riponiamo in un *robot* non dipende esclusivamente da quanto quest'ultimo si mostra competente in un certo compito: anche con i *robot*, siamo influenzati dalla natura "sociale" dei contesti d'interazione con altre persone o agenti artificiali. In altre parole, anche l'interazione con *robot* può seguire alcuni tipi di norme sociali, sebbene queste possano essere diverse da quelli abitualmente osservate nelle interazioni tra esseri umani.

Per riassumere, numerosi studi hanno evidenziato come i contesti sociali amplifichino alcuni problemi legati alla trasmissione e valutazione delle informazioni a cui abbiamo accesso nella nostra vita quotidiana. Se capire e valutare al meglio queste informazioni complesse è di per sé un compito estremamente difficile, il fatto che la maggior parte delle informazioni venga condivisa in contesti sociali rende ancora più complessa una gestione ottimale della conoscenza condivisa. Numerosi processi psicologici e sociali ci spingono a considerare le informazioni in modo non oggettivo e razionale e, di conseguenza, a generare e condividere con gli altri informazioni erranee e distorte. Ciò pone serie preoccupazioni sulle dinamiche contemporanee che sottendono il consolidamento della conoscenza collettiva e l'adesione ad atti di responsabilità collettiva, dalla vaccinazione di massa al distanziamento sociale durante una pandemia globale.

METODOLOGIA DI LAVORO E BIBLIOGRAFIA

Abbracciando il paradigma dell'*Open Innovation* attraverso il coinvolgimento del *network* INNOV@DIFESA costituito da esperti militari ed esperti civili provenienti dal mondo accademico, industriale e della ricerca, sotto la guida dell'Ufficio Generale Innovazione Difesa il tema della crescente competizione cognitiva (*Cognitive Warfare*) è stato analizzato da un punto di vista multidisciplinare, cercando di identificarne le possibili traiettorie di sviluppo e le linee di indirizzo per la Difesa.

Di seguito l'elenco degli esperti che hanno fornito continuo ed estensivo supporto allo sviluppo del Concetto, ai quali lo Stato Maggiore della Difesa esprime il proprio riconoscimento, e le citazioni bibliografiche.

ESPERTI

Area Industria

- Ing. Paolo PROIETTI, *Leonardo S.p.A. – NATO STB e STO Panel Member – AIAD GdL RiTec Chairman*
- Dott. Andrea STRIPPOLI LANTERNINI, *MDBA Italia – Infosec & Cybersecurity Compliance – Consultant*
- Ing. Roberto DE FINIS, *Sistemi & Automazione S.p.A.- Direttore Operativo (C.O.O.)*

Area Accademia

- Prof. Andrea GAGGIOLI, *Università Cattolica del sacro Cuore– Professore ordinario di Psicologia e Direttore del Centro Studi e Ricerche di Psicologia della Comunicazione.*
- Prof. Zeno LEONI, *docente di Sicurezza internazionale presso il King College London e la Defence Academy of the UK*
- Dott.ssa Roberta MONNI, *Ministero dell'Interno, Direzione Centrale della Difesa Civile – Dirigente responsabile per le relazioni comunitarie e internazionali;*

Area Ricerca

- Dott. Michelangelo FREYRIE, *Istituto Affari Internazionali (IAI) – Ricercatore nei programmi Difesa e Sicurezza*
- Dott. Andrea PAGNIN, *Istituto Italiano di Tecnologia - Head of Innovation & Development Office*
- Dott. Alessandra SCIUTTI, *Istituto Italiano di Tecnologia - Tenure Track Researcher, head of the CONTACT (COgNiTive Architecture for Collaborative Technologies) Unit*
- Dott. Massimo AMOROSI, *esperto in studi strategici, specializzato in minacce biologiche*

BIBLIOGRAFIA

Pubblicazioni Nazionali

- Presidenza del Consiglio dei Ministri, Strategia di Cybersicurezza 2022-2026 (2022)
- Presidenza del Consiglio dei Ministri, Piano di Implementazione - Strategia di Cybersicurezza 2022-2026 (2022)
- Ministero della DIFESA, Strategia di Sicurezza e Difesa per il Mediterraneo (2022)
- STATO MAGGIORE DIFESA, Il Concetto Strategico del Capo di Stato Maggiore della Difesa (2022)
- STATO MAGGIORE DIFESA, Concetto Scenari Futuri (2021)
- STATO MAGGIORE DIFESA, Approccio della Difesa alle Operazioni Multidominio (2022)
- STATO MAGGIORE DIFESA, L'impatto delle *Emerging & Disruptive Technologies* (EDTs) sulla Difesa (2022)

Pubblicazioni NATO

- NATO *Strategic Concept* (2022)
- NATO *Warfighting Capstone Concept* (NWCC), (2020)
- NATO *Allied Joint Publication* (AJP-01-F), “*Allied Joint Doctrine*” (*study draft*)
- NATO *Allied Joint Publication* (AJP-10-A1), “*Allied Joint Doctrine for strategic Communications*” (*harmonization draft*)
- NATO *Allied Joint Publication* (AJP-3.10-B1), “*Allied Joint Doctrine for Information Operations*” (*study draft*)
- NATO Science & Technology Organization, *Science & Technology Trends 2020-2040. Exploring the S&T Edge* (2020)

Pubblicazioni Estere

- NATO INNOVATION HUB, “*Cognitive Warfare*” (2020)
- NATO INNOVATION HUB, “*Cognitive Warfare: an attack on truth and thought*” (2020)
- NATO INNOVATION HUB, *Cognitive Workshop: Innovative Solutions to Improve Cognition* (2021)
- NATO INNOVATION HUB, *Emerging Neuroscience and Technology (NeuroS/T): Current and Near-Term Risks and Threats to NATO Biosecurity* (2021)
- NATO INNOVATION HUB, *Intelligence Amplification* (2020)
- European Union, *Strategic Compass* (2021)
- US Joint Staff, *Joint Concept for Human Aspects of Military Operations* (2016)
- US Joint Staff, *Joint Concept for Operating in the Information Environment* (2018)
- UK MoD, *Joint Concept Note 2/18 “Information Advantage”* (2018)
- UK MoD, *Human Augmentation – The Dawn of a New Paradigm* (2021)

- ESP Centro Conjunto de Desarrollo de Conceptos (ESP) “*The Cognitive Domain – Exploratory Concept*” (2020)
- Meeting of the High Contracting Parties to the Convention on Prohibitions or restrictions on the Use of Certain Conventional weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (2019)
- National Defense University Press, *Minds at War. China’s Pursuit of Military Advantage through Cognitive Science and Biotechnology* (2020)
- Scandinavian Journal of Military Studies, 4(1), *Cyborgs, Neuroweapons, and Network Command*, <https://doi.org/10.31374/sjms.86> (2021)
- US Strategic Multilayer Assessment, *Operational Cyberpsychology: Adapting a Special Operations Model for Cyber Operations*, (2021)
- Australian Government DoD, *A Method for Ethical AI in Defence* (2020)

Saggi

- Gaggioli A., Ferscha A., Riva G., Dunne S., Viaud-Delmon I., *Human Computer Confluence. Transforming Human Experience Through Symbiotic Technologies*, De Gruyter Open Ltd (2016) <https://doi.org/10.1515/9783110471137> ;
- Dando M., *Neuroscience and the future of chemical-biological weapons*, Palgrave Macmillan (2015)
- Dando M., *Neuroscience and the Problem of Dual Use. Neuroethics in the New Brain Research Projects*, Springer (2020)
- Evans N.G., *The ethics of Neuroscience and National Security*, Routledge (2021)
- Hartley D.S. III, Jobson K.O., *Cognitive Superiority. Information to Power*, Springer (2021)
- Moreno J., Schulkin J., *The Brain in Context: A Pragmatic Guide to Neuroscience*, Columbia University Press (2019);
- Andrea Gaggioli A., Riva G., *Realtà virtuali: Gli aspetti psicologici delle tecnologie simulate e il loro impatto sull'esperienza umana*, Giunti Psychometrics (2019);
- Fogg, B. J., Cuellar, G. & Danielson, D., *Motivating, influencing, and persuading users: an introduction to captology*. In A. Sears & J. A. Jacko (Eds.), *Human-computer interaction. Fundamentals*. London: CRC Press. Taylor & Francis Group (2009);
- Rossi S., *Il cervello elettrico. Le sfide della neuromodulazione*, Raffaello Cortina Editore (2020);
- Lin. P, Mehlman M.J., Abney K., *Enhanced Warfighters: Risk, Ethics, and Policy*, The Greenwall Foundation (2013)
- Galliot J., Lota M., *Super Soldiers: The Ethical, Legal and Social Implications*, Ashgate Publishing Company (2015).

Publicazioni scientifiche/accademiche

- Friston, K., & Kiebel, S., *Predictive coding under the free-energy principle*. Philosophical transactions of the Royal Society of London. Series B, Biological sciences, 364(1521), <https://doi.org/10.1098/rstb.2008.0300> (2009)
- Héloïse Goodley, *Pharmacological performance enhancement and the military. Exploring an ethical and legal framework for “supersoldiers*, Chatham House (2020)
- Jonathan Moreno, Michael L. Gross, Jack Becker, Blake Hereth, Neil D. Shortland III and Nicholas G. Evans, *The ethics of AI-assisted warfighter enhancement research and experimentation: Historical perspectives and ethical challenges*, Front. Big Data (2022)
- National Academies of Sciences, *An Assessment of Illness in U.S. Government Employees and Their Families at Overseas Embassies*, <https://nap.nationalacademies.org/catalog/25889/an-assessment-of-illness-in-us-government-employees-and-their-families-at-overseas-embassies> (2020)
- Gutzwiller, R., Ferguson-Walter, K., Fugate, S., & Rogers, A., “*Oh, Look, A Butterfly!*” *A Framework For Distracting Attackers To Improve Cyber Defense*. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 62(1). <https://doi.org/10.1177/1541931218621063>(2018)
- Riva, G., Baños, R. M., Botella, C., Mantovani, F., & Gaggioli, A. *Transforming Experience: The Potential of Augmented Reality and Virtual Reality for Enhancing Personal and Clinical Change*. Frontiers in psychiatry, 7, 164. <https://doi.org/10.3389/fpsy.2016.00164> (2016)
- Shao S., Wu J., Zhou Q., *Developments and challenges in human performance enhancement technology*, Medicine in Novel Technology and Devices, www.journals.elsevier.com/medicine-in-novel-technology-and-devices/ (2021)
- Asch, S. E. *Effects of group pressure upon the modification and distortion of judgment in Groups, leadership and men*, Carnegie Press (1951).
- Claidière, N., & Whiten, A., *Integrating the study of conformity and culture in humans and nonhuman animals*. Psychological bulletin, 138(1) (2012)
- Connolly, J., Mocz, V., Salomons, N., Valdez, J., Tsoi, N., Scassellati, B., and Vázquez, M., *Prompting prosocial human interventions in response to robot mistreatment*. In Proceedings of ACM/IEEE International Conference on Human-Robot Interaction. (2020)
- Eisenberger, N. I., Lieberman, M. D., & Williams, K. D., *Does rejection hurt? An fMRI study of social exclusion*. Science, 302(5643) (2003)
- Fehr, E., & Schurtenberger, I., *Normative foundations of human cooperation*. Nature Human Behaviour, 2(7) (2018)
- Hertz, U., Palminteri, S., Brunetti, S., Olesen, C., Frith, C. D., & Bahrami, B., *Neural computations underpinning the strategic management of influence in advice giving*. Nature Communications, 8(1) (2017)
- Kahn Jr, P. H., Kanda, T., Ishiguro, H., Gill, B. T., Shen, S., Gary, H. E., and Ruckert, J. H., *Will people keep the secret of a humanoid robot? Psychological*

- intimacy in HRI*. In Proceedings of ACM/IEEE International Conference on Human-Robot Interaction (2015).
- Mahmoodi, A., Bahrami, B., & Mehring, C., Reciprocity of social influence. *Nature communications*, 9(1) (2018)
 - Pryor, C., Perfors, A., & Howe, P. D., *Even arbitrary norms influence moral decision-making*. *Nature Human Behaviour*, 3(1) (2019)
 - Strohkorb Sebo, S., Traeger, M., Jung, M., and Scassellati, B., *The ripple effects of vulnerability: The effects of a robot's vulnerable behavior on trust in human-robot teams*. In Proceedings of ACM/IEEE International Conference on Human-Robot Interaction (2018)
 - Van der Hoorn, D. P., Neerincx, A., & de Graaf, M. M., *"I think you are doing a bad job!" The Effect of Blame Attribution by a Robot in Human-Robot Collaboration*. In Proceedings of the 2021 ACM/IEEE International Conference on Human-Robot Interaction, (2021, March)
 - Zonca, J., Folsø, A., & Sciutti, A., *Dynamic modulation of social influence by indirect reciprocity*. *Scientific Reports*, 11(1) (2021)
 - Zonca, J., Folsø, A., & Sciutti, A., *I'm not a little kid anymore! Reciprocal social influence in child–adult interaction*. *Royal Society Open Science*, 8(8), 202124 (2021)
 - Zonca, J., Folsø, A., & Sciutti, A., *The role of reciprocity in human-robot social influence*. *iScience*, 24(12), 103424 (2021)
 - Zonca, J., & Sciutti, A., *Does human-robot trust need reciprocity? Proceedings of the 2021 workshop "Robot Behavior Adaptation to Human Social Norms"*, in Conjunction with the 30th IEEE International Conference on Robot and Human Interactive Communication (Ro-Man) (2021)
 - Scattolin et al., *Reduced Ownership over a virtual body modulates dishonesty*. *iScience* 25,104320 (2022)
 - National Academies, *Human-AI Teaming: State-of-the-Art and Research Needs* (2022)
 - Douglas T., *If Nudges Treat their Targets as Rational Agents, Nonconsensual Neurointerventions Can Too*, *Ethical Theory and Moral Practice* <https://doi.org/10.1007/s10677-022-10285-w> (2022)
 - Denning T., Matsuoka Y, Khono T., *Neurosecurity: security and privacy for neural devices*, *Neurosurg Focus* (2009)
 - Davidovic J., Crowell F.S., *Operationalizing the Ethics of Soldier Enhancement*, *Journal of Military Ethic* <https://doi.org/10.1080/15027570.2021.2018176> (2021)
 - Moreno J., Gross M.L., Becker J., Hereth B., Shortland N.D., Evans N.G., *The ethics of AI-assisted warfighter enhancement research and experimentation: Historical perspective and ethical challenges*, *Frontiers in Big Data* (2022)
 - Helbing D., Ienca M., *Why Converging Technologies Need International Regulation*, *Research Gate* (2022)
 - RAND Corporation, *Brain Computer Interfaces – U.S. Military Applications and Implications – An Initial Assessment* (2020)





UGID
Ufficio Generale Innovazione Difesa
UGID
INNOV@DIFESA

