

La strumentalizzazione delle reti chiuse: piattaforme non convenzionali, disinformazione partecipativa e sfide dell'intelligence

Greta Furlan



International Institute for Global Analyses

Vision & Global Trends. International Institute for Global Analyses
Piazza dei Navigatori 22, 00147 – Rome (Italy)

The views and opinions expressed in this publication are those of the authors and do not represent the views of the Vision & Global Trends. International Institute for Global Analyses unless explicitly stated otherwise.

© 2026 Vision & Global Trends - International Institute for Global Analyses
© 2026 Greta Furlan

First Edition: October 2026
Analytical Dossier 19/2026 - ISSN 2704-6419

www.vision-gt.eu
info@vision-gt.eu

La strumentalizzazione delle reti chiuse: piattaforme non convenzionali, disinformazione partecipativa e sfide dell'intelligence

Greta Furlan



Vision & Global Trends – International Institute for Global Analyses

La strumentalizzazione delle reti chiuse: piattaforme non convenzionali, disinformazione partecipativa e sfide dell'intelligence

Greta Furlan

Il contributo analizza il ruolo delle piattaforme digitali non convenzionali e delle comunità online chiuse nelle dinamiche contemporanee della guerra cognitiva, con particolare attenzione ai processi di disinformazione partecipativa, radicalizzazione e manipolazione delle percezioni collettive. Attraverso l'esame delle caratteristiche strutturali e relazionali di ambienti quali Discord, Twitch e le comunità legate ai videogiochi, lo studio approfondisce i meccanismi attraverso i quali attori statali e non statali possono sfruttare i legami fiduciari, le appartenenze identitarie e le vulnerabilità sociali per orientare il dibattito pubblico e accentuare la polarizzazione. Particolare rilievo assume il passaggio dalla propaganda tradizionale a forme di influenza decentralizzata, nelle quali gli stessi utenti partecipano, spesso inconsapevolmente, alla produzione e alla diffusione di narrazioni manipolative. L'analisi evidenzia le difficoltà che tali fenomeni pongono alle attività di intelligence, soprattutto in relazione all'attribuzione delle operazioni di influenza, all'opacità delle reti comunicative e ai limiti del monitoraggio. Ne emerge la necessità di sviluppare strumenti di prevenzione e capacità di analisi che, nel rispetto delle libertà fondamentali, contribuiscano a rafforzare la resilienza cognitiva, la fiducia nelle istituzioni e la coesione sociale.

Parole chiave: Guerra cognitiva; Disinformazione partecipativa; Piattaforme digitali; Intelligence; Polarizzazione sociale.

1. Introduzione: La cognizione come nuovo fronte della conflittualità ibrida

La guerra cognitiva (*cognitive warfare*) si presenta essenzialmente come la competizione per la superiorità decisionale (*cognitive superiority*), sviluppandosi non come una rottura rispetto ai campi di battaglia tradizionali, ma come un livello in più che si aggiunge e li completa. Per comprendere questo scontro, bisogna guardare alla sua architettura divisa in tre livelli interconnessi: il livello infrastrutturale del cyber garantisce reti, architetture software e vettori di propagazione dei dati; il livello dell'informazione interviene sui flussi comunicativi per veicolare disinformazione e manipolare le narrazioni visive e testuali; infine, il livello dell'effetto, coincidente con la dimensione cognitiva vera e propria, costituisce il bersaglio ultimo, agendo direttamente sul substrato neuropsicologico ed emotivo per alterare la percezione della realtà.

Di conseguenza, l'obiettivo principale non è danneggiare i computer o diffondere notizie false, ma colpire le fasi di osservazione e orientamento del ciclo OODA (*Observe, Orient, Decide, Act*) elaborato da John Boyd¹, provocando ritardi, errori di valutazione e bloccando le decisioni sia dei vertici dello Stato sia dei cittadini.²

¹ Coram, R. (2002). *Boyd: The fighter pilot who changed the art of war*. Little, Brown and Company.

² NATO Science & Technology Organization. (2025). *Cognitive warfare (Chief Scientist Research Report)*. NATO.

Questo approccio lo possiamo ritrovare in alcune dottrine globali come per esempio quella dell'Esercito Popolare di Liberazione cinese che ha definito la strategia delle "Tre Guerre", la quale si basa sull'interazione tra guerra legale, guerra dell'opinione pubblica e guerra psicologica, finalizzata inoltre alla promozione di una narrazione favorevole.³

In questo quadro vediamo quindi che la manipolazione della percezione, che avviene anche tramite una promozione attiva della narrazione favorevole, non è solo un'attività di supporto ma un vero e proprio pilastro che definisce l'idea sunziana del vincere senza combattere.⁴

L'obiettivo fondamentale della guerra cognitiva risiede nella trasformazione della mente umana in un vero e proprio campo di battaglia operativa, mirando a rimodellare i processi psicologici e decisionali dei soggetti coinvolti. Questa manovra fa leva sulla costante iperstimolazione digitale, concepita per saturare le risorse della corteccia prefrontale dedicate al pensiero logico-critico (il cosiddetto "Sistema 2") e costringere la mente a ripiegare su risposte rapide, intuitive ed emotive ("Sistema 1").

In questo stato di sovraccarico è molto probabile che l'individuo sia portato ad attivare specifici bias cognitivi (di disponibilità, di conferma) che riducono la complessità della realtà.

In questo modo, il confronto sociale viene trasformato in una semplice logica da scontro: "noi contro di loro". Chi la pensa diversamente viene percepito subito come un nemico, mentre si accetta senza esitare qualsiasi cosa confermi le idee del proprio gruppo. A questo punto, la persona non è più soltanto una vittima della manipolazione: condividendo post, litigando online o diffondendo rabbia, comincia ad alimentare essa stessa la spaccatura, diventando senza rendersene conto un vero e proprio megafono della propaganda.⁵

Capiamo quindi che il bersaglio strategico della guerra cognitiva non si ferma più soltanto agli apparati militari o alle cancellerie governative, ma arriva ad investire l'intera società civile.

La minaccia fa perno sulle vulnerabilità strutturali delle democrazie aperte, prima fra tutte la progressiva frammentazione della fiducia pubblica nelle istituzioni, nella scienza e nei canali informativi tradizionali.⁶

È proprio dentro queste crepe e in questo clima di sfiducia diffusa che lo scontro ha cambiato casa, lasciando le piazze rumorose dei social tradizionali per infiltrarsi negli spazi che viviamo ogni giorno. Questo articolo nasce per raccontare come il mondo dei videogiochi e i server come Discord siano diventati il nuovo fronte invisibile: luoghi in cui governi ed estremisti sfruttano le spaccature del nostro tempo per orientare idee, reclutare consensi e radicalizzare le persone a fari spenti. L'obiettivo di questo lavoro è comprendere i meccanismi con cui questi spazi digitali vengono usati per condizionare il dibattito pubblico e spingere gli utenti verso forme di polarizzazione. Per fare questo, l'analisi si muove esaminando casi reali e strategie di comunicazione, concentrandosi in particolare sull'universo delle chat e delle community online.

2 L'ecosistema delle piattaforme non convenzionali: architettura, fiducia e vulnerabilità

Oggi i social network tradizionali come X, Facebook o Instagram sono diventati spazi troppo visibili e controllati: ogni post o interazione viene esaminata, moderata e segnalata molto rapidamente. È proprio per questo motivo che molti attori malevoli hanno deciso di spostare la loro attenzione verso l'ecosistema dei videogiochi e le piattaforme adiacenti, come *Discord*, *Twitch* o *Steam Community*.

³ Kania, E. B. (2016). The PLA's latest strategic thinking on the Three Warfares. China Brief, Jamestown Foundation.

⁴ Sun Tzu. (2011). L'arte della guerra (trad. di L. Matteucci). Feltrinelli.

⁵ Deppe, C., & Schaal, G. S. (2024). Cognitive warfare: A conceptual analysis of the NATO ACT cognitive warfare exploratory concept. *Frontiers in Big Data*, 7, Article 1452129.

⁶ NATO Science & Technology Organization. (2025). Cognitive warfare (Chief Scientist Research Report). NATO.

Dentro il videogioco vero e proprio, però, lo spazio di manovra per manipolare qualcuno è limitato: le chat scorrono troppo veloci durante le partite, ci sono filtri automatici sulle parole vietate e l'attenzione dei giocatori è tutta rivolta al gioco. Il videogioco funziona quindi soprattutto come luogo di primo contatto (*icebreaker*), da cui gli utenti vengono poi invitati a spostarsi su piattaforme esterne di supporto.

Queste ultime rappresentano l'infrastruttura di socializzazione che ogni videogiocatore usa quotidianamente per parlare e fare gruppo. Le loro caratteristiche principali sono la frammentazione in comunità private - non esiste una bacheca pubblica visibile a tutti, ma una rete frammentata di server chiusi- l'uso costante della chat vocale e l'accessibilità graduale: spesso c'è un canale pubblico di facciata e poi stanze nascoste o riservate a cui si accede solo su invito. L'aspetto centrale è che questi spazi sono difficili da monitorare dall'esterno: non possono essere controllati facilmente da ricercatori, polizie postali o algoritmi, poiché la moderazione quotidiana è affidata in larga parte ai proprietari del server, pur rimanendo attiva una supervisione centrale della piattaforma, che interviene dall'alto in caso di violazioni gravi.⁷

All'interno di questi ambienti si crea tra le persone un fortissimo senso di comunità, cosa che può essere sia un aspetto positivo sia forte vulnerabilità.

Le persone che comunicano tra di loro instaurano una forte fiducia tra pari e quindi l'interlocutore non viene percepito minimamente come una minaccia, anzi viene visto come un amico o un compagno di squadra.

In questo clima informale, le normali barriere critiche si abbassano e la ricerca di approvazione sociale da parte del gruppo (*in-group*) finisce spesso per prevalere sulle regole del mondo esterno.

Un importante esempio di ciò viene dato dal caso di Jack Teixeira, il quale, per guadagnare prestigio e impressionare la propria cerchia all'interno di Discord, ha pubblicato notizie e documenti riservati dell'intelligence statunitense. Pur non trattandosi di un'operazione d'influenza orchestrata dall'esterno, quanto piuttosto di una violazione della sicurezza da parte di un insider poi individuato dalle autorità, questo episodio dimostra chiaramente come il bisogno di riconoscimento sociale all'interno di queste bolle digitali possa spingere a superare qualsiasi vincolo di sicurezza o buon senso.⁸

In questo contesto, l'estremismo ha quasi del tutto abbandonato i manifesti ideologici tradizionali e i discorsi solenni, adottando invece i codici visivi e sarcastici tipici di internet e del gaming.

Molto spesso le narrazioni estreme vengono diffuse utilizzando il meccanismo del «si scherza soltanto» (*it's just a joke*), che funge da scudo difensivo e permette sia di eludere la moderazione, sia di evitare qualsiasi reazione etica o critica immediata. Nel momento in cui qualcuno solleva accuse di razzismo, misoginia o violenza, viene subito liquidato come una persona priva di senso dell'umorismo o non allineata al gruppo. È proprio per questo che chi si indigna davanti a certe frasi o meme viene progressivamente allontanato o isolato; chi invece ride o reagisce positivamente dimostra di essere ricettivo, finendo per ricevere messaggi privati (*DM*) o inviti in canali più riservati dove l'ideologia viene esplicitata in modo diretto.

Il vero pericolo risiede nel fatto che, continuando a ridere e a trattare con leggerezza episodi, simboli o narrazioni d'odio, la mente smette di percepire la reale gravità di questi temi. La violenza subisce un processo di de-drammatizzazione ed entra nella routine quotidiana, finendo per apparire accettabile e normale. Si consolida così una vera e propria identità di gruppo, in cui chi appartiene alla community si sente compreso e valorizzato, mentre chiunque si trovi all'esterno viene etichettato come nemico o assimilato alle istituzioni.

⁷ European Commission. (2023). Spotlight on games, gaming and gamification (RAN Spotlight). Directorate-General for Migration and Home Affairs

⁸ Guhl, J. (s.d.). Discord & extremism. Institute for Strategic Dialogue

A questo punto si innesca una vera e propria competizione interna: la condivisione di contenuti provocatori diventa una gara informale, in cui alzare costantemente il livello della provocazione viene premiato con l'approvazione dei pari, risate e un maggiore prestigio all'interno del server.⁹

3. Dalla strategia statale alle subculture digitali: la disinformazione partecipativa

All'interno di queste piattaforme decentralizzate non troviamo solo singoli individui o comunità nate spontaneamente: vi operano anche attori statali e le loro reti surrogate (*proxy*) nell'ambito della moderna guerra politica. Il loro obiettivo primario è ottenere vantaggi geopolitici mantenendosi costantemente al di sotto della soglia del conflitto convenzionale, sfruttando l'arena informativa per massimizzare l'impatto a costi estremamente ridotti. L'elemento più vantaggioso per gli apparati statali è garantito dal principio della non attribuibilità: attraverso l'impiego di account anonimi, profili fittizi o intermediari, viene mascherata l'origine ufficiale delle operazioni psicologiche condotte. I loro interventi non mirano tanto a convincere l'opinione pubblica della bontà o superiorità del proprio modello politico, quanto ad amplificare e approfondire le fratture e le vulnerabilità già presenti nella società bersaglio. Inserendosi nei dialoghi informali, questi attori spingono narrazioni che minano la credibilità dei governi, allontanano i cittadini dalla politica e logorano le relazioni internazionali, sfruttando le divisioni interne come leva di pressione geopolitica.¹⁰

Sul piano asimmetrico troviamo attori non statali, cellule estremiste e reti terroristiche che sfruttano queste piattaforme decentralizzate per scopi di reclutamento e indottrinamento. Diverse analisi dimostrano che non esiste una correlazione chiara tra l'utilizzo dei videogiochi e l'insorgenza di comportamenti violenti: il vero motivo per cui questi attori scelgono tali spazi è la possibilità di intercettare il proprio target demografico di riferimento all'interno di un ambiente privo di moderazione centrale.

Inoltre, questi gruppi radicali raramente sviluppano videogiochi da zero per fare propaganda, dati i costi elevati e la complessità tecnica che ciò comporterebbe; ricorrono invece alla pratica del *modding*, sfruttando piattaforme aperte come *Minecraft* o *Roblox* in cui chiunque può costruire ambientazioni personalizzate e invitare altri utenti ad accedervi. Ad esempio, cellule suprematiste hanno ricostruito su *Minecraft* e *The Sims* la moschea di Christchurch per far rivivere ai giocatori la strage terroristica del 2019 in prima persona, mentre all'interno di *Roblox* sono stati invece creati spazi virtuali che simulavano campi di concentramento o veri e propri "etno-stati", dove gli avatar potevano inscenare persecuzioni contro le minoranze. In questo modo fare propaganda risulta molto più accessibile: all'estremista basta creare la propria mappa modificata e far circolare il link di accesso tra i contatti con cui ha precedentemente instaurato un legame di fiducia.

Questa strumentalizzazione cambia a seconda dell'ideologia, anche se il posto in cui agiscono è lo stesso. Da una parte, l'estremismo di destra e i suprematisti sfruttano il clima che c'è già in certi gruppi: usano battute pesanti, meme e l'insofferenza verso il "politicamente corretto" per fare gruppo, facendo passare il razzismo e l'odio per una semplice difesa della propria comunità. Dall'altra parte, i gruppi jihadisti usano i videogiochi soprattutto come stile visivo: per attirare i ragazzi occidentali montano i video di attentati e combattimenti reali facendoli sembrare partite a

⁹ European Commission. (2023). Spotlight on games, gaming and gamification (RAN Spotlight). Directorate-General for Migration and Home Affairs

¹⁰ Robinson, L., Helmus, T. C., Cohen, R. S., Nader, A., Radin, A., Magnuson, M., & Migacheva, K. (2018). Modern political warfare: Current practices and possible responses (Research Report No. RR-1772-A). RAND Corporation

sparatutto come *Call of Duty*, con la visuale in prima persona e ritmi veloci. Così facendo, la violenza reale non fa più paura e viene percepita quasi come un gioco.¹¹

A questo punto, è necessario sottolineare come la disinformazione moderna funzioni proprio perché è di natura partecipativa. Per comprendere questo meccanismo, occorre distinguere tra disinformazione, intesa come la creazione e la diffusione deliberata e consapevole di contenuti falsi per manipolare il dibattito, e misinformation, che riguarda invece la condivisione involontaria di notizie inesatte da parte di utenti convinti della loro veridicità. All'interno di queste dinamiche non occorrono accordi formali o contatti diretti tra gli apparati statali e le comunità estremiste online: accade molto spesso che gli attori governativi si limitino a diffondere l'idea generale, alimentando il sospetto o esasperando le fratture sociali preesistenti, per poi ritirarsi senza bisogno di coordinare ogni singolo messaggio.

Il testimone passa così nelle mani degli utenti delle piattaforme decentralizzate. Attraverso una spinta dal basso (*bottom-up*), la base assorbe queste narrazioni, si sente investita di una sorta di missione e comincia a produrre contenuti in totale autonomia: vengono creati meme, condivisi screenshot decontestualizzati e montate clip di gioco provocatorie con l'intento di corroborare quella determinata tesi.

In questo modo, la propaganda strategica di uno Stato viene rilanciata e amplificata a costo zero da utenti reali, convinti di star semplicemente esprimendo il proprio pensiero o difendendo la propria visione del mondo. Per gli analisti e le agenzie di sicurezza diventa difficile distinguere dove si esaurisca la manovra informativa straniera e dove inizi il dissenso interno spontaneo. È proprio questo cortocircuito a rendere le operazioni di influenza cognitiva estremamente insidiose e difficili da neutralizzare, poiché non si presentano come un'aggressione esterna, ma si mimetizzano all'interno del fisiologico rumore di fondo del dibattito in rete; nonostante questa apparente invisibilità, tuttavia, è grazie all'applicazione di metodologie OSINT che gli investigatori riescono a rintracciare e disinnescare la genesi di queste campagne.¹²

4. La frammentazione sociale come obiettivo strategico: il paradosso della connettività

Le moderne operazioni di disinformazione ritrovano la loro efficacia non tanto in tecnologie particolarmente avanzate, quanto piuttosto nella vulnerabilità del contesto socioculturale in cui si inseriscono. Gli attori ostili, infatti, vanno a intercettare le debolezze e le fragilità della struttura, esasperandole fino a renderle ingestibili.

Di conseguenza, all'interno della società vengono a mancare i punti di riferimento più importanti: le istituzioni perdono credibilità e le persone iniziano a sentirsi sole, insicure ma soprattutto smarrite. Si crea quindi un'ampia sfiducia verso i governi e verso i media, i quali non sono più in grado di aiutare e orientare.

In questo contesto di profondo disorientamento e frammentazione sociale, la sfiducia di molti giovani smette di essere soltanto un problema strutturale e si trasforma in una possibilità perfetta per chi vuole influenzare il dibattito dall'esterno.

È inoltre importante sottolineare che le notizie false o manipolate non convincono le persone da un giorno all'altro: funzionano, infatti, solo se trovano un ambiente già polarizzato. Quando la divisione politica diventa troppo forte e non ci si fida più delle fonti ufficiali, il senso critico si abbassa: si finisce per credere a un contenuto non perché sia vero o verificato, ma semplicemente perché attacca la parte avversa e conferma le proprie antipatie.

¹¹ United Nations Office of Counter-Terrorism. (2022). Examining the intersection between gaming and violent extremism. United Nations.

¹² DiResta, R., Schafer, B., Starbird, K., & Barnes, R. (2021). Disinformation 2.0: Trends for 2021 and beyond (Hybrid CoE Working Paper No. 11). The European Centre of Excellence for Countering Hybrid Threats.

È proprio l'incrocio tra isolamento sociale e scontro continuo a rendere le comunità online facili da manipolare, trasformando i dubbi e la rabbia degli utenti nel carburante ideale per diffondere narrazioni tossiche.¹³

In questo scenario emerge con chiarezza come, all'interno delle dottrine di guerra informativa e ibrida (come per esempio quella delle "Tre Guerre"), l'obiettivo primario di simili manovre non sia la conversione ideologica del pubblico bersaglio: ad attori statali come la Cina o la Russia, non interessa davvero persuadere i cittadini della superiorità del proprio modello politico. Il traguardo coincide piuttosto con la polarizzazione in sé, trasformando qualsiasi questione, dalla politica estera alle scelte economiche, in uno scontro continuo, all'interno del quale non esiste mediazione e l'avversario politico viene percepito come una minaccia.

A sostenere questa dinamica interviene quello che possiamo definire il "paradosso della connettività": l'esplosione della rete e l'aumento dei contatti quotidiani non hanno favorito una maggiore coesione sociale, ma una frattura più profonda. Di fronte a una sovrabbondanza di stimoli e opinioni contrastanti, l'individuo tende spontaneamente ad aggregarsi a chi la pensa nello stesso modo, costruendo un'identità di gruppo che esclude l'esterno e tratta chi esprime un'opinione contraria come un nemico.

Tale meccanismo divide il corpo sociale in blocchi rigidi e reciprocamente ostili. L'effetto finale di una simile frattura è la paralisi: la democrazia si ritrova bloccata nei propri meccanismi decisionali, incapace di riconoscere con lucidità le minacce esterne e priva della coesione necessaria per elaborare una risposta strategica comune.¹⁴

All'interno di spazi circoscritti come server dedicati, canali tematici o community di gioco, questa dinamica assume una dimensione prettamente identitaria: il bisogno di appartenenza e di approvazione tra pari finisce per prevalere sulla ricerca dei fatti, portando a respingere a priori qualsiasi smentita o dato ufficiale proveniente dall'esterno, liquidato automaticamente come propaganda di parte.¹⁵

L'esposizione prolungata a narrazioni contrastanti, a provocazioni mirate e, soprattutto, a un continuo sovraccarico informativo produce un progressivo logoramento del senso critico. Gli individui arrivano a una vera e propria saturazione cognitiva, che alimenta un senso di stanchezza e di sfiducia generalizzata.

Questa condizione spinge la persona a credere che non esista alcuna verità condivisa, che ogni fonte sia manipolata ad arte e che qualsiasi informazione sia in realtà una presa in giro. Si forma così un contesto disilluso e nichilista, in cui gli utenti finiscono per essere il veicolo ideale per diffondere il caos in rete, spesso senza nemmeno rendersene conto. Ciò rende queste forme di influenza quasi invisibili: diventa infatti difficilissimo distinguere la rabbia spontanea delle persone dalle manovre organizzate dall'esterno.¹⁶

5. La crisi dell'attribuzione lineare: opacità, propaganda partecipativa e limiti dell'intelligence

¹³ Tucker, J. A., Guess, A., Barberá, P., Vaccari, C., Siegel, A., Sanovich, S., Stukal, D., & Nyhan, B. (2018). Social media, political polarization, and political disinformation: A review of the scientific literature. SSRN Electronic Journal

¹⁴ Thurner, S., Hofer, M., & Korbel, J. (2025). Why more social interactions lead to more polarization in societies. Proceedings of the National Academy of Sciences, 122(44), Article e2517530122.

¹⁵ Van Bavel, J. J., & Pereira, A. (2018). The partisan brain: How social identity shapes our divided mind. Current Directions in Psychological Science, 27(3), 213–224.

¹⁶ Claverie, B., & du Cluzel, F. (2022). "Cognitive Warfare": The advent of the concept of "cognitics" in the field of warfare. In B. Claverie, B. Prébot, N. Buchler, & F. du Cluzel (Eds.), Cognitive warfare: The future of cognitive dominance (STO-MP-HFM-334, pp. 2-1–2-7). NATO Collaboration Support Office.

Mentre nichilismo e polarizzazione trasformano gli utenti comuni nei vettori inconsapevoli della disinformazione, gli apparati di sicurezza e di intelligence si trovano ad affrontare la complessa sfida dell'attribuzione della minaccia. Riconoscere l'origine di un'operazione di influenza informativa non segue infatti le dinamiche lineari tipiche della sicurezza informatica tradizionale. Negli attacchi informatici convenzionali l'analista cerca tracce tecniche tangibili: l'obiettivo è individuare porzioni di codice compilato o un server di comando e controllo. In questo caso l'attribuzione poggia su elementi che, pur potendo essere in parte falsificati, mantengono un solido riscontro ingegneristico. Nelle operazioni di influenza, al contrario, l'azione non configura di per sé un reato informatico: trattandosi di manovre prettamente comunicative, la creazione di contenuti, meme o discussioni sfrutta le dinamiche ordinarie dei social media, violando i termini d'uso delle piattaforme e le normative sulla trasparenza, pur muovendosi in un'area grigia rispetto alle leggi penali tradizionali. L'aggressore non introduce un codice malevolo esterno, ma fa leva sulle fratture e sulle rivendicazioni preesistenti nel corpo sociale, rendendo difficile distinguere, a un primo sguardo, il singolo impulso ostile dal megafono spontaneo della folla, un confine che, come anticipato, l'indagine OSINT riesce tuttavia a tracciare mappando le reti di coordinamento. A tutto questo si aggiunge un evidente problema di trasparenza metodologica: le prove tecniche più rilevanti rimangono custodite nei registri proprietari delle grandi piattaforme, le quali condividono porzioni minime di dati solo con una ristretta cerchia di analisti selezionati, impedendo una verifica realmente indipendente da parte della comunità scientifica. Inoltre, mentre una parte della comunicazione statale sfrutta canali palesi e media ufficiali (operazioni aperte), la proiezione di influenza più subdola non agisce alla luce del sole: gli Stati tendono infatti a delegare la gestione operativa a intermediari privati, come agenzie di marketing, società di pubbliche relazioni o fabbriche di troll (operazioni coperte). In questo modo gli apparati mandanti si garantiscono una costante possibilità di smentita plausibile (*plausible deniability*), lasciando le istituzioni completamente disarmate e bloccate sul piano legale e politico.¹⁷

Ci troviamo oggi di fronte a una vera e propria “propaganda partecipativa”, in cui non è più solo un emittente statale a indirizzare messaggi a un pubblico passivo: sono gli utenti stessi delle piattaforme a collaborare alla diffusione del contenuto, rielaborandolo e amplificandolo all'interno delle proprie reti fiduciarie. È proprio questa dinamica a compromettere l'analisi e il monitoraggio di queste minacce: le comunicazioni tra pari godono di una credibilità interna elevatissima e circolano attraverso legami orizzontali impossibili da catalogare secondo i consueti schemi.

Il lavoro di indagine è reso ancora più difficile dal cambio di linguaggio. Il meme è diventato uno degli strumenti principali per trattare qualsiasi tema, anche il più serio, e l'ironia che racchiude crea un vero e proprio muro per l'analisi. Inoltre, chi diffonde queste narrazioni può sempre difendersi sostenendo che si tratti solo di uno scherzo o di una provocazione innocua.

Per chi si occupa di sicurezza e intelligence diventa così un'impresa capire dove finisca la rabbia genuina delle persone e dove inizi la manovra organizzata, lasciando gli analisti senza parametri chiari per misurare quanto sia reale e pericolosa la minaccia.¹⁸

A fronte della chiusura di queste piattaforme e del fatto che i governi devono mantenere determinate informazioni classificate, l'analisi su fonti aperte e la collaborazione tra pubblico e privato sono diventate uno strumento fondamentale. Lavorando su elementi visibili a tutti, come immagini

¹⁷ Pamment, J., & Smith, V. (2019). Attributing information influence operations: Identifying the actors behind platform manipulation. NATO Strategic Communications Centre of Excellence & European Centre of Excellence for Countering Hybrid Threats

¹⁸ Wanless, A., & Berk, M. (2017). Participatory propaganda: The engagement of audiences in the spread of persuasive communications. SecDev Foundation & Centre for Cyber Security and International Relations Studies (CCSIRS), University of Florence.

satellitari commerciali, tracce lasciate sui social o collegamenti tra siti web, ricercatori indipendenti e analisti di sicurezza riescono a ricostruire le campagne di influenza e a renderle note ai cittadini, senza il rischio di compromettere fonti o metodi riservati.

Usare queste informazioni per denunciare pubblicamente chi c'è dietro, però, apre un grosso dilemma noto nella letteratura strategica come *disclosure dilemma*, ovvero il delicato compromesso tra la necessità di esibire le prove e l'esigenza di proteggere i propri metodi investigativi. Se le istituzioni spiegano nei dettagli tecnici come hanno scoperto la manovra, mostrano all'avversario i propri metodi: il risultato è che chi attacca impara la lezione, cambia tattica e si sposta su canali ancora più difficili da controllare. Se invece le autorità accusano qualcuno senza mostrare prove schiaccianti, rischiano di non essere credute e di sembrare mosse da meri interessi politici, finendo per alimentare proprio quella sfiducia pubblica che volevano combattere.¹⁹

A tutto questo si aggiunge un limite strutturale delle democrazie liberali: lo Stato non può mettersi a spiare o a controllare a tappeto le conversazioni online dei propri cittadini senza violare la loro privacy e i loro diritti fondamentali. Questo vincolo mette le democrazie in netto svantaggio rispetto ai regimi autoritari, lasciando a chi attacca un grande spazio di manovra. Allo stesso tempo, però, dimostra che difendersi da queste minacce non significa trasformarsi in uno Stato di polizia digitale: la vera sfida sta nel proteggere la credibilità delle istituzioni e nel preservare la coesione della società senza rinunciare ai propri valori di libertà.²⁰

6. Conclusioni: ricostruire la fiducia per disarmare la guerra cognitiva

L'analisi di questi ambienti ci mostra chiaramente che la guerra cognitiva non si può vincere tramite la censura o il blocco informatico. Chiudere un server come Discord o smentire una notizia falsa nel momento in cui è già diventata virale serve a poco: negli spazi chiusi o decentralizzati, vietare qualcosa ottiene solo l'effetto indesiderato di spingerlo su piattaforme ancora più nascoste e difficili da monitorare, alimentando la rabbia verso l'esterno e finendo per rafforzare la complicità e la fiducia interna tra gli utenti. La vera risposta, quindi, non deve stare nel punire o nel rincorrere ogni singola ideologia, provocazione o meme. L'obiettivo degli avversari, infatti, non è tanto farci cambiare idea, quanto creare confusione, alimentare lo scontro continuo e bloccare la nostra capacità di scegliere con lucidità. La difesa deve perciò basarsi sulla prevenzione e sulla consapevolezza: insegnare soprattutto ai più giovani a riconoscere le trappole mentali della rete, a capire quando l'ironia e le battute nascondono messaggi d'odio e a non farsi usare come megafoni inconsapevoli della propaganda altrui.

Infine, il fatto che uno Stato democratico non possa spiare i propri cittadini o controllare ogni chat privata non è un segno di debolezza, ma il valore più grande da difendere. Rimanere vincolati a queste regole rende sicuramente il lavoro di difesa più difficile e lascia margini di manovra a chi attacca. Tuttavia, proteggere la nostra società dalla disinformazione non significa imitare i regimi autoritari togliendo la libertà, ma mantenere credibili le nostre istituzioni e ricostruire quel legame di fiducia tra le persone che è il vero bersaglio della guerra cognitiva.

¹⁹ Carnegie, A., & Carson, A. (2019, March 20). The disclosure dilemma: Nuclear intelligence and international organizations.

²⁰ Nilsson, N. (2025). Intelligence and strategic communication. NATO Strategic Communications Centre of Excellence

BIBLIOGRAFIA

Carnegie, A., & Carson, A. (2019, March 20). The disclosure dilemma: Nuclear intelligence and international organizations.

<https://onlinelibrary.wiley.com/doi/10.1111/ajps.12426>

Claverie, B., & du Cluzel, F. (2022). "Cognitive Warfare": The advent of the concept of "cognitics" in the field of warfare. In B. Claverie, B. Prébot, N. Buchler, & F. du Cluzel (Eds.), *Cognitive warfare: The future of cognitive dominance* (STO-MP-HFM-334, pp. 2-1-2-7). NATO Collaboration Support Office.

<https://hal.science/hal-03635889v1/document>

Coram, R. (2002). *Boyd: The fighter pilot who changed the art of war*. Little, Brown and Company.

<https://archive.org/details/boyd00robe/page/n3/mode/2up>

Deppe, C., & Schaal, G. S. (2024). Cognitive warfare: A conceptual analysis of the NATO ACT cognitive warfare exploratory concept. *Frontiers in Big Data*, 7, Article 1452129.

<https://pmc.ncbi.nlm.nih.gov/articles/PMC11565700/>

DiResta, R., Schafer, B., Starbird, K., & Barnes, R. (2021). *Disinformation 2.0: Trends for 2021 and beyond* (Hybrid CoE Working Paper No. 11). The European Centre of Excellence for Countering Hybrid Threats.

https://www.hybridcoe.fi/wp-content/uploads/2021/07/20210716_Hybrid_CoE_Working_Paper_11_Disinfo_2_0_WEB.pdf

European Commission. (2023). *Spotlight on games, gaming and gamification* (RAN Spotlight). Directorate-General for Migration and Home Affairs.

https://home-affairs.ec.europa.eu/document/download/e1c089f1-3c5d-4d15-af49-6fe07666fc3f_en?filename=spotlight_on_gamification_062023_en.pdf

Guhl, J. (s.d.). *Discord & extremism*. Institute for Strategic Dialogue.

<https://www.isdglobal.org/isd-explainer/discord-extremism/>

Kania, E. B. (2016). *The PLA's latest strategic thinking on the Three Warfares*. China Brief, Jamestown Foundation.

<https://jamestown.org/the-plas-latest-strategic-thinking-on-the-three-warfares/>

NATO Science & Technology Organization. (2025). *Cognitive warfare* (Chief Scientist Research Report). NATO.

<https://www.nato.int/content/dam/nato/webready/documents/sto/chief-scientist-report-cognitive-warfare.pdf>

Nilsson, N. (2025). *Intelligence and strategic communication*. NATO Strategic Communications Centre of Excellence.

<https://stratcomcoe.org/publications/download/Intelligence-and-StratCom-FINAL.pdf>

Pamment, J., & Smith, V. (2019). *Attributing information influence operations: Identifying the actors behind platform manipulation*. NATO Strategic Communications Centre of Excellence & European Centre of Excellence for Countering Hybrid Threats.

<https://share.google/3dI4CD6WFimJeyASi>

Robinson, L., Helmus, T. C., Cohen, R. S., Nader, A., Radin, A., Magnuson, M., & Migacheva, K. (2018). *Modern political warfare: Current practices and possible responses* (Research Report No. RR-1772-A). RAND Corporation.

https://www.rand.org/pubs/research_reports/RR1772.html

Sun Tzu. (2011). *L'arte della guerra* (trad. di L. Matteucci). Feltrinelli.

Thurner, S., Hofer, M., & Korbel, J. (2025). Why more social interactions lead to more polarization in societies. *Proceedings of the National Academy of Sciences*, 122(44), Article e2517530122.

<https://www.pnas.org/doi/10.1073/pnas.2517530122>

Tucker, J. A., Guess, A., Barberá, P., Vaccari, C., Siegel, A., Sanovich, S., Stukal, D., & Nyhan, B. (2018). Social media, political polarization, and political disinformation: A review of the scientific literature. *SSRN Electronic Journal*.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144139

United Nations Office of Counter-Terrorism. (2022). Examining the intersection between gaming and violent extremism. United Nations.

https://www.un.org/counterterrorism/sites/default/files/221005_research_launch_on_gaming_ve.pdf

Van Bavel, J. J., & Pereira, A. (2018). The partisan brain: How social identity shapes our divided mind. *Current Directions in Psychological Science*, 27(3), 213–224.

https://www.researchgate.net/publication/326139477_The_partisan_brain_An_identity-based_model_of_political_belief

Wanless, A., & Berk, M. (2017). Participatory propaganda: The engagement of audiences in the spread of persuasive communications. SecDev Foundation & Centre for Cyber Security and International Relations Studies (CCSIRS), University of Florence

<https://share.google/PgCKAb4gdeNQJ0z0Y>



Vision & Global Trends - International Institute for Global Analyses

www.vision-gt.eu

info@vision-gt.eu