

Guerra Cognitiva: strategie, impatti e prospettive alla luce delle nuove dottrine ibride



La guerra cognitiva (Cognitive Warfare) rappresenta l'evoluzione più sofisticata delle operazioni di influenza, dove la mente umana diventa il campo di battaglia primario attraverso l'integrazione di intelligenza artificiale, neuroscienze e infrastrutture cibernetiche avanzate. Questo paradigma emergente trasforma radicalmente il panorama della cybersecurity, richiedendo ai professionisti del settore competenze integrate che spaziano dalla *threat intelligence* tradizionale alle scienze cognitive.

La NATO ha formalmente riconosciuto la cognizione come sesto dominio di guerra nel 2023, affiancandola ai domini terrestre, marittimo, aereo, cibernetico e spaziale. Secondo il framework del NATO Allied Command Transformation, la guerra cognitiva si definisce come *“attività condotte in sincronizzazione con altri strumenti di potere, per influenzare attitudini e comportamenti mediante l'influenza, protezione o distruzione della cognizione individuale, di gruppo o a livello di popolazione, al fine di ottenere un vantaggio sull'avversario”*. Questa definizione sottolinea il salto qualitativo rispetto alle operazioni di *information warfare* tradizionali: l'obiettivo non è più controllare cosa le persone pensano, ma come pensano.

Fondamenti tecnico-scientifici

della guerra cognitiva

La guerra cognitiva si distingue dalle operazioni psicologiche tradizionali per l'integrazione sistematica di tecnologie emergenti e metodologie scientifiche avanzate. **L'architettura tecnologica sottostante combina intelligenza artificiale generativa, reti neurali avversarie (GAN) e sistemi di *behavioral analytics* per manipolare i processi cognitivi con precisione e scala senza precedenti.**

Infrastruttura tecnologica e vettori di attacco

I sistemi di guerra cognitiva operano attraverso un'infrastruttura distribuita che include:

Generazione di contenuti sintetici: Le Generative Adversarial Networks (GAN) consentono la creazione di deepfake video e audio con accuratezza superiore al 90% nella sincronizzazione labio-vocale. I modelli *autoencoder* mappano diversi individui su rappresentazioni latenti condivise, permettendo la sostituzione realistica di volti nei contenuti video. La tecnologia Wav2Lip raggiunge precisioni di sincronizzazione audio-visiva preferite dall'osservatore umano nel 90% dei casi.

Piattaforme di distribuzione scalabili: Le Content Delivery Networks (CDN) distribuite geograficamente utilizzano *routing anycast* per ridurre la latenza fino al 50%, mentre l'*edge computing* permette l'ottimizzazione in tempo reale dei contenuti. I sistemi *auto-scaling* dinamici gestiscono carichi variabili attraverso architetture multi-cloud containerizzate via Docker e Kubernetes.

Sistemi di profilazione comportamentale: Gli algoritmi di *machine learning* analizzano pattern digitali multi-sorgente per identificare vulnerabilità psicologiche specifiche. I modelli predittivi determinano la suscettibilità individuale a narrative specifiche, mentre l'analisi delle emozioni in tempo

reale adatta dinamicamente i contenuti persuasivi.

Casi studio contemporanei: operazioni documentate 2022-2025

Le operazioni di guerra cognitiva documentate negli ultimi tre anni rivelano patterns operativi sofisticati e coordinate multidominio.

Operazioni cinesi: Il caso Taiwan

La campagna COVID-19 di Taiwan (2021-2022) rappresenta un caso emblematico di integrazione tra guerra cognitiva e operazioni psicologiche tradizionali. Durante l'epidemia di COVID-19, la Cina ha orchestrato campagne di disinformazione sincronizzate con incursioni aeree PLA per minare la fiducia nel programma vaccinale taiwanese. Le *content farm* cinesi (KKnews, read01) hanno diffuso informazioni false sui vaccini Medivac, ottenendo un impatto misurabile: solo 3 milioni di dosi Medivac sono state somministrate su 60 milioni di vaccinazioni totali.

Durante la visita di Nancy Pelosi nell'agosto 2022, la Cina ha dimostrato capacità di coordinamento cyber-cognitivo attraverso attacchi simultanei ai sistemi di segnaletica digitale (hack dei 7-Eleven con messaggi "Warmonger Pelosi, get out of Taiwan") e campagne di disinformazione massive.

Operazioni russe: L'influenza algoritmica

Le operazioni TikTok russe (2022-2025) hanno sfruttato la manipolazione algoritmica per influenzare l'opinione pubblica occidentale sui conflitti in Ucraina e Israele-Palestina. La strategia del "controllo riflessivo" manipola i processi decisionali nemici attraverso l'inganno, ottenendo **cambiamenti misurabili nell'opinione pubblica giovanile americana e australiana sui conflitti geopolitici.**

Operazioni iraniane: Attacchi ibridi

L'attacco cyber-cognitivo all'Albania (luglio 2022) ha dimostrato l'integrazione di operazioni distruttive cibernetiche con *warfare* psicologico. Gli attori statali iraniani legati ai Guardiani della Rivoluzione hanno simultaneamente compromesso sistemi governativi e lanciato messaggi psicologici per minare la fiducia pubblica.

Operazioni israeliane: AI targeting

I sistemi "Lavender" e "The Gospel" rappresentano l'evoluzione dell'*AI targeting* militare con implicazioni cognitive. Questi sistemi utilizzano elaborazione di dati di sorveglianza massiva e *analytics* predittive per identificazione e profilazione psicologica automatizzata dei target.

Tecnologie emergenti e sviluppi futuri

L'integrazione di neuroscienze computazionali e tecnologie emergenti sta aprendo nuove frontiere nella guerra cognitiva. La ricerca NATO identifica le "neuroarmi" come tecnologie progettate per influenzare direttamente i processi neurali, incluse tecniche di stimolazione transcranica, interfacce cervello-computer e potenziali applicazioni farmacologiche.

Sistemi di detection avanzati

I sistemi di rilevamento multimodali analizzano inconsistenze facciali, sincronizzazione labiale innaturale e artefatti computazionali. La Coalition for Content Provenance and Authenticity (C2PA) sta sviluppando standard tecnici per la verifica di contenuti, mentre Adobe e Microsoft implementano sistemi di Content Credentials per l'autenticazione di immagini e video.

La watermarking digitale incorpora pattern pixel/audio

rilevabili da computer ma impercettibili all'osservatore umano. I pattern scompaiono nelle aree modificate, fornendo prova di alterazione, mentre causano l'aspetto irrealistico dei deepfake quando utilizzano *media watermarked*.

Contromisure e architetture difensive

Framework NATO per la resilienza cognitiva

NATO ha sviluppato un approccio a quattro pilastri per la difesa cognitiva:

Educate: Costruzione di alfabetizzazione cognitiva e consapevolezza delle minacce attraverso programmi di formazione specializzati.

Collaborate: Condivisione informazioni e risposta coordinata tramite sistemi di *early warning* e partnership pubblico-private.

Protect: Tecnologie difensive e procedure operative standard per la protezione delle infrastrutture cognitive.

Shape: Operazioni di influenza proattive all'interno di framework legali ed etici.

Soluzioni tecniche CISA e ENISA

CISA ha introdotto il concetto di "infrastruttura cognitiva" come la più critica delle infrastrutture, richiedendo protezione specializzata. Il framework MDM (Misinformation, Disinformation, Malinformation) fornisce tassonomie operative per la classificazione delle minacce.

L'European Union Agency for Cybersecurity (ENISA) ha sviluppato il framework FIMI (Foreign Information Manipulation and Interference) che integra la cybersecurity con le minacce cognitive attraverso infrastrutture tecnologiche condivise.

Sistemi di autenticazione crittografica

Le soluzioni blockchain per la verifica dei media creano *record tamper-evident* per l'autenticazione dei contenuti. I metadata sicuri incorporati descrivono le caratteristiche dei dati, mentre l'assenza o incompletezza dei metadata indica potenziali alterazioni.

Evoluzione del panorama delle minacce

L'integrazione dell'AI generativa ha accelerato drammaticamente le capacità offensive nella guerra cognitiva. I Large Language Models (LLM) sbloccati permettono produzione rapida e sostenuta di disinformazione, mentre gli influencer sintetici generati dall'AI consentono manipolazione su larga scala.

Sfide emergenti 2024-2025

La frammentazione delle piattaforme sta spingendo gli utenti verso ambienti meno moderati, mentre le operazioni di influenza ibride combinano campagne digitali con *warfare* cinetico. **Deloitte proietta frodi abilitate dall'AI per \$40 miliardi entro il 2027**, con organizzazioni commerciali sempre più soggette a disinformazione sponsorizzata da stati.

Implicazioni per la sicurezza nazionale e internazionale

La guerra cognitiva rappresenta un cambio paradigmatico dove la mente umana diventa il campo di battaglia primario, richiedendo strategie *comprehensive* che proteggano sia i sistemi tecnici che i processi decisionali umani. **L'integrazione di cooperazione internazionale, tecnologie di *detection* avanzate e framework di difesa cognitiva *evidence-based* fornisce le basi per contromisure efficaci.**

Raccomandazioni strategiche

Per i professionisti della cybersecurity: Implementare capacità di *detection deepfake* in tempo reale utilizzando metodi multipli, sviluppare sistemi *behavioral analytics* per identificare comportamenti inautentici coordinati, stabilire sistemi di verifica di *provenance* per comunicazioni critiche.

Per le organizzazioni: Integrare strutturalmente team che combinano cybersecurity, comunicazioni e *intelligence*, preparazione obbligatoria per la leadership senior sulla sicurezza cognitiva, programmi di formazione continua basati sull'esposizione per il personale.

L'evoluzione della guerra cognitiva continuerà rapidamente, guidata da progressi nell'AI generativa, tensioni geopolitiche crescenti e democratizzazione di strumenti di attacco sofisticati. Il successo nella difesa richiede un cambio fondamentale da approcci reattivi centrati sulla tecnologia a strategie proattive centrate sull'uomo che integrino soluzioni tecniche con insights delle scienze cognitive e costruzione di resilienza organizzativa.

La sfida è mantenere il passo con minacce che evolvono alla velocità dell'innovazione AI, sviluppando allo stesso tempo contromisure che preservino i valori democratici e la libertà di espressione. Il successo in questo dominio richiederà collaborazione internazionale senza precedenti, investimenti sostenuti in ricerca e sviluppo, e un approccio multidisciplinare che integri competenze tecniche, psicologiche e politiche.

Bibliografia:

- Beauchamp-Mustafaga, N. (2023). *Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States*. RAND Corporation, RR-A853-1.

- Claverie, B., & du Cluzel, F. (2022). Cognitive Warfare: The advent of the concept of “cognitics” in the field of warfare. *HAL Archive*, hal-03635889.
- Deppe, C., & Schaal, G. S. (2024). Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. *Frontiers in Big Data*, 7, 1452129.
- Hung, T. C., & Hung, T. W. (2022). How China’s cognitive warfare works: a frontline perspective of Taiwan’s anti-disinformation wars. *Journal of Global Security Studies*, 7(4), ogac016.
- Miller, S. (2023). Cognitive warfare: an ethical analysis. *Ethics and Information Technology*, 25, 46.
- European External Action Service. (2025). *3rd EEAS Report on Foreign Information Manipulation and Interference Threats*.
- ENISA & EEAS. (2022). *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity*. Publications Office of the EU.
- NATO Allied Command Transformation. (2023). *Cognitive Warfare Exploratory Concept*. NATO ACT, Report No.: ACT/SPP/CNDV/TT-6700.
- NATO Science and Technology Organization. (2023). *Cognitive Warfare, a Battle for the Brain*. STO Meeting Proceedings, STO-MP-HFM-334.
- CNA Corporation. (2023). *Assessing Russian Cyber and Information Warfare in Ukraine: Expectations, Realities, and Lessons*.
- <https://www.ictsecuritymagazine.com/notizie/israele-guerra-a-gazza/>
- Francesco Arruzzoli (2022). Deepfake & Cyber Intelligence: Tecniche di creazione, rilevamento e prevenzione. *ICT Security Magazine*

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/cognitive-warfare-guerra-cognitiva/>