



Difesa Cognitiva Nazionale: Come Proteggere l'Italia dalle Operazioni d'Influenza Informative

Pubblicato il 21/08/2026

Nel panorama attuale della sicurezza globale, la difesa di un Paese non riguarda solo i **confini territoriali** o la **protezione dei dati informatici**. Esiste un vero e proprio “fronte informativo” dove vengono condotte le cosiddette **operazioni d'influenza cognitive**. L'obiettivo di queste campagne — coordinate in modo sistematico dalla **Federazione Russa** — non è semplicemente diffondere notizie false, ma **dividere l'opinione pubblica, minare la fiducia nelle istituzioni** e **indebolire l'alleanza dell'Italia** con i propri partner europei ed euro-atlantici.

Per garantire una vera **resilienza democratica**, l'Italia necessita di una strategia nazionale organizzata su quattro pilastri principali: **coordinamento istituzionale, tecnologia di rilevamento, prevenzione culturale** e **formazione dei cittadini**.

Una “Regia” Istituzionale Unificata

Per contrastare gli attacchi nel dominio informativo non servono azioni isolate, ma un **coordinamento centrale dello Stato**:

- **Centro di Risposta Rapida sulle Minacce Informative:** Creazione di una struttura coordinata dalla **Presidenza del Consiglio** e dall'**Intelligence (DIS)** in grado di monitorare ed etichettare tempestivamente le **ingerenze straniere** sul dibattito pubblico.
- **Collaborazione Internazionale:** Piena integrazione con il **Servizio Europeo per l'Azione Esterna (SEAE)** dell'UE e con i **centri d'eccellenza della NATO** dedicati al contrasto delle minacce ibride.

Monitoraggio e Blocco delle Reti Automatiche

La propaganda moderna usa **strumenti di automazione, profili falsi (bot) e Intelligenza Artificiale Generativa** per creare contenuti e cloni visivi estremamente credibili:

- **Sistemi di Allerta Precoce tramite AI:** Adozione di algoritmi per tracciare la nascita artificiale di campagne virali, identificando la creazione di **siti cloni dei giornali italiani** che diffondono notizie inventate (tecnica **Doppelgänger**).
- **Trasparenza delle Piattaforme Digitali:** Applicazione rigida del **Digital Services Act (DSA)** europeo, imponendo la **rimozione tempestiva di profili falsi** e campagne manipolative coordinate.

La Prevenzione Informale: Fare “Prebunking”

Confutare una notizia falsa dopo che si è già diffusa ha un'efficacia limitata. La strategia migliore è la **prevenzione**:

- **Spiegare le Tecniche Prima che Vengano Usate (Prebunking):** Informare la popolazione su **come funzionano le leve psicologiche** della propaganda (uso dell'indignazione, finti esperti, immagini alterate) prima che la campagna arrivi online.
- **Comunicazione Istituzionale Chiara e Tempettiva:** Colmare i vuoti d'informazione durante momenti delicati (elezioni o crisi internazionali) con **dati certi e trasparenti**, evitando che vengano occupati dalla propaganda avversaria.

Educazione Digitale e Coinvolgimento dei Cittadini

Il cittadino non deve essere solo un soggetto passivo, ma il **primo baluardo di difesa**:

- **Alfabetizzazione ai Media:** Introduzione nelle **scuole** e nella **Pubblica Amministrazione** di moduli dedicati all'**analisi critica delle fonti** e alla verifica dei contenuti visivi e di testo generati da AI.
- **Supporto al Giornalismo d'Inchiesta:** Promozione di **standard elevati di verifica delle fonti** e supporto a ricercatori e analisti impegnati nel tracciamento delle ingerenze estere.

Fonti Ufficiali e Riferimenti Documentali

1. **Unione Europea - European External Action Service (EEAS):***Reports on Foreign Information Manipulation and Interference (FIMI) Threats* (Rapporti ufficiali UE sul tracciamento delle manipolazioni informative estere).
2. **Commissione Europea:***EU Code of Practice on Disinformation e Digital Services Act (DSA)* (Normative e codici di condotta per la trasparenza informatica e il contrasto alla disinformazione).
3. **EUvsDisinfo:** Progetto dell'Unione Europea dedicato alla rilevazione e alla catalogazione delle **campagne di disinformazione della Federazione Russa**.
4. **NATO Strategic Communications Centre of Excellence (CoE):** Studi strategici dedicati alla **guerra psicologica**, alle **operazioni d'influenza** e alla **difesa cognitiva**.
5. **Sistema di Informazione per la Sicurezza della Repubblica (DIS / Governo Italiano):***Relazione Annuale sulla Politica dell'Informazione per la Sicurezza* (Analisi delle minacce ibride e della disinformazione verso l'Italia).