HWG Sababa

Cognitive warfare:

quando la mente umana diventa il campo di battaglia

Alessio Aceti, HWG Sababa

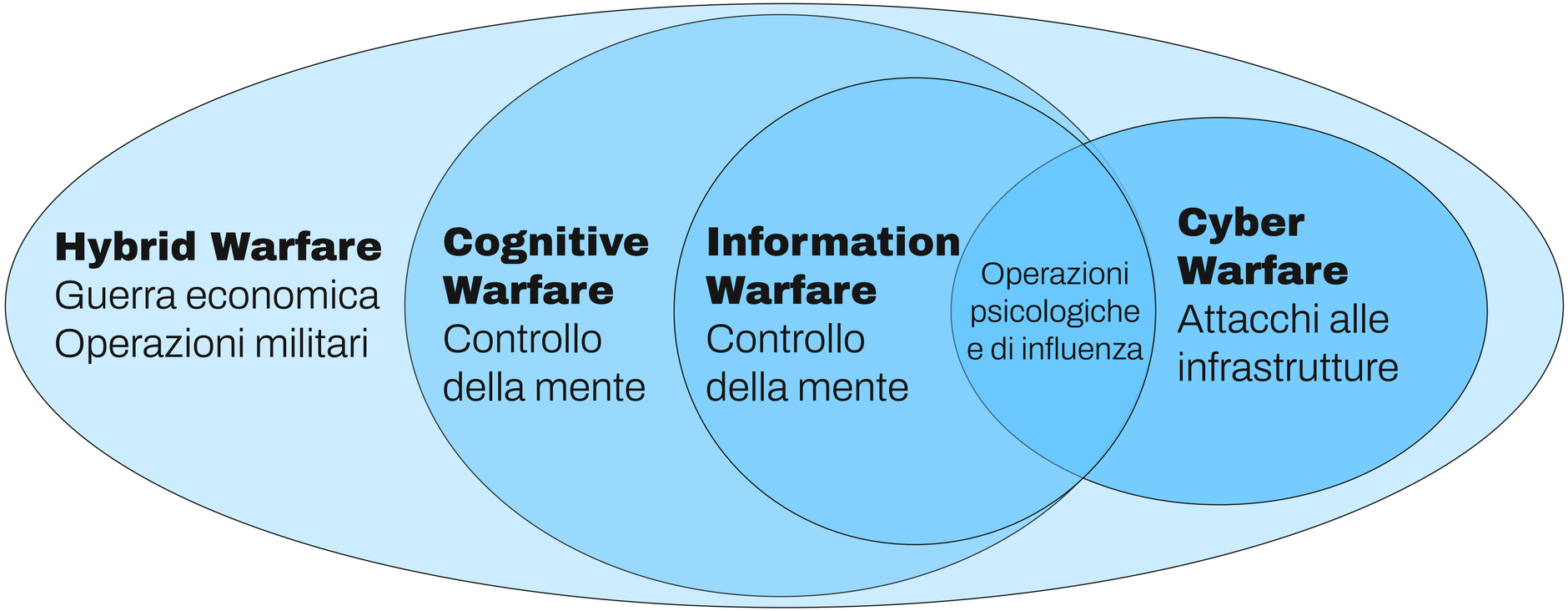
The Marion Stokes Project

Marion Stokes

1929-2012

Strumenti e metodi di disinformazione

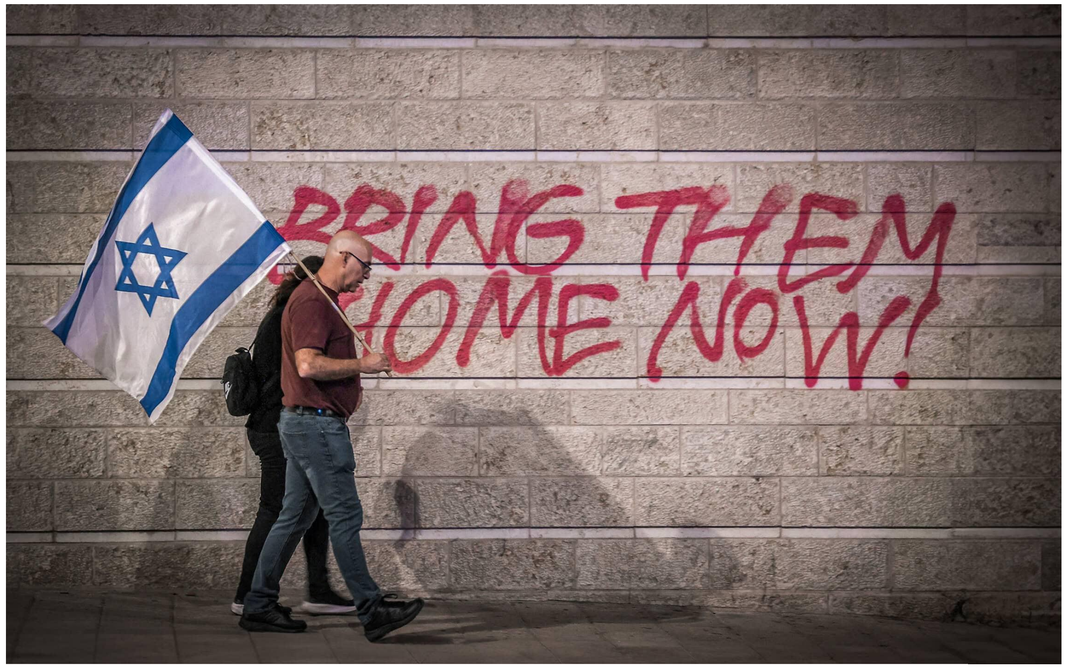
La guerra cognitiva mira al dominio della mente: utilizza informazioni, intelligenza artificiale e scienze comportamentali per influenzare il modo in cui le persone pensano e decidono.



Cognitive Warfare: Relazioni Concettuali

1. Plasmare la percezione

La percezione è il risultato del contesto narrativo.
Il contesto influisce sulle emozioni, le emozioni guidano l’azione.



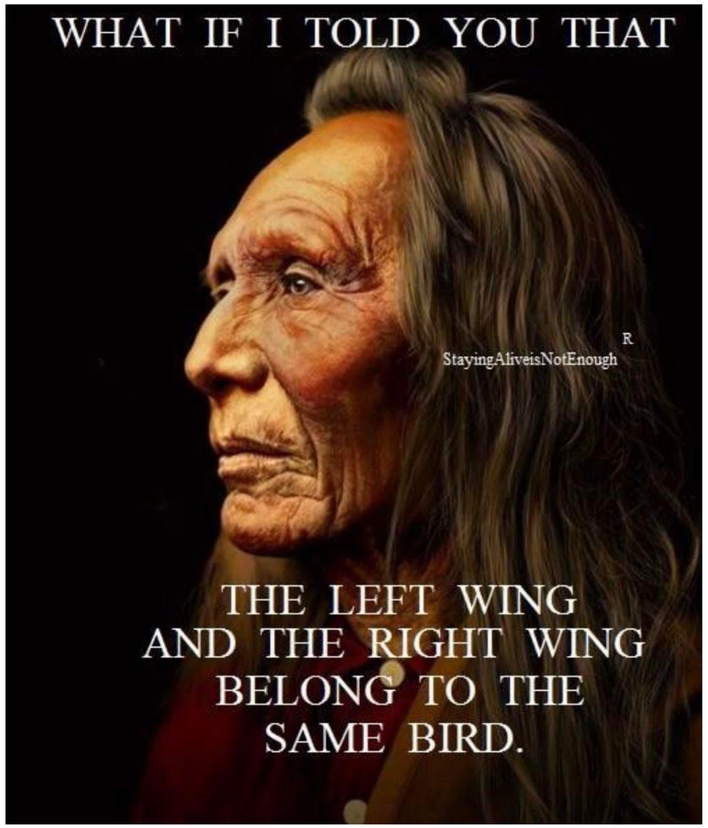
Autodifesa

Catastrofe umanitaria

2. Minare la fiducia

Il sovraccarico di informazioni contraddittorie mina la legittimità delle istituzioni.

L'obiettivo non è far credere a una menzogna, ma **far dubitare di tutto.**

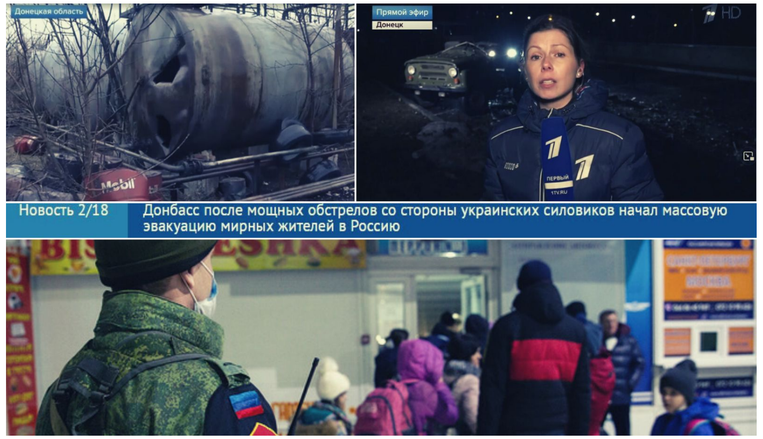


3. Strumentalizzazione delle narrazioni digitali

Intere storie vengono costruite a tavolino e usate come vere e proprie armi.

Queste narrazioni vengono amplificate da botnet, troll farm e media statali per vari scopi:

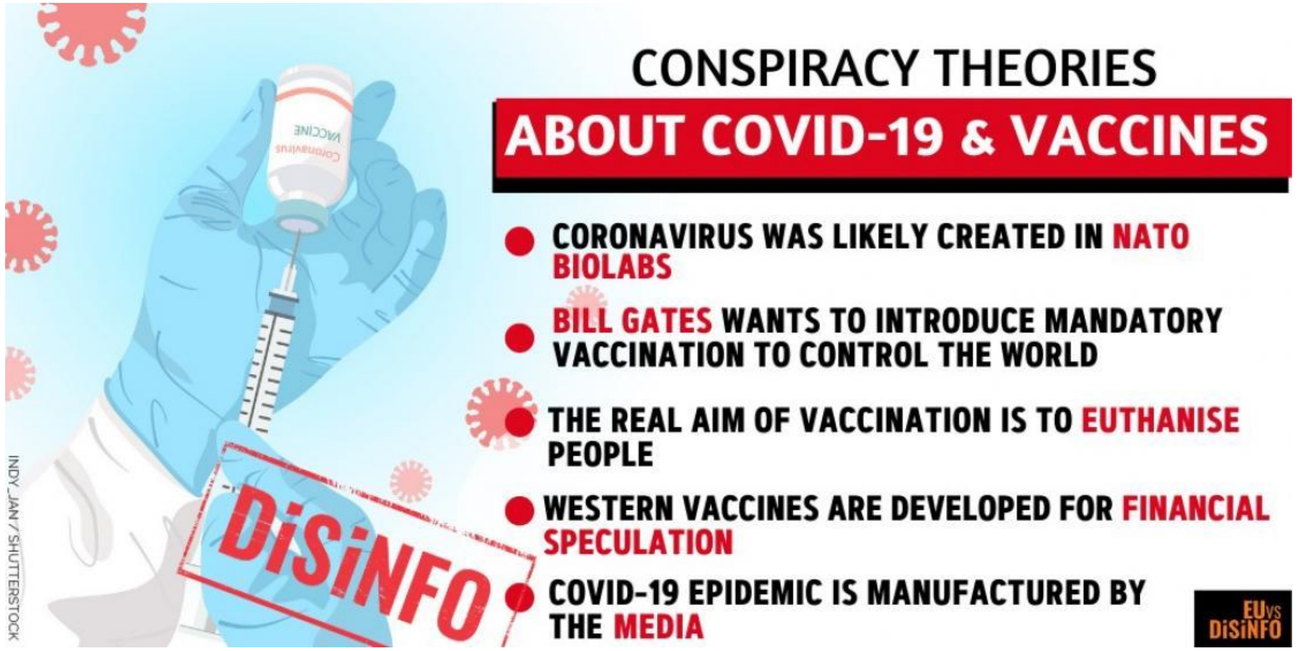
- giustificare un’aggressione
- mobilitare il sostegno interno
- indebolire alleanze



4. Uso commerciale delle narrazioni

Anche player commerciali possono trasformare le narrazioni in armi per competere e trarre profitto.

Queste narrazioni sfruttano la paura, l’incertezza e la sfiducia nelle autorità.



Le istituzioni hanno bisogno di partner privati

HWG Sababa

Velocità

Gli attacchi cognitivi si propagano in pochi minuti, mentre le risposte istituzionali arrivano spesso dopo giorni

Portata

Milioni di contenuti circolano su piattaforme frammentate

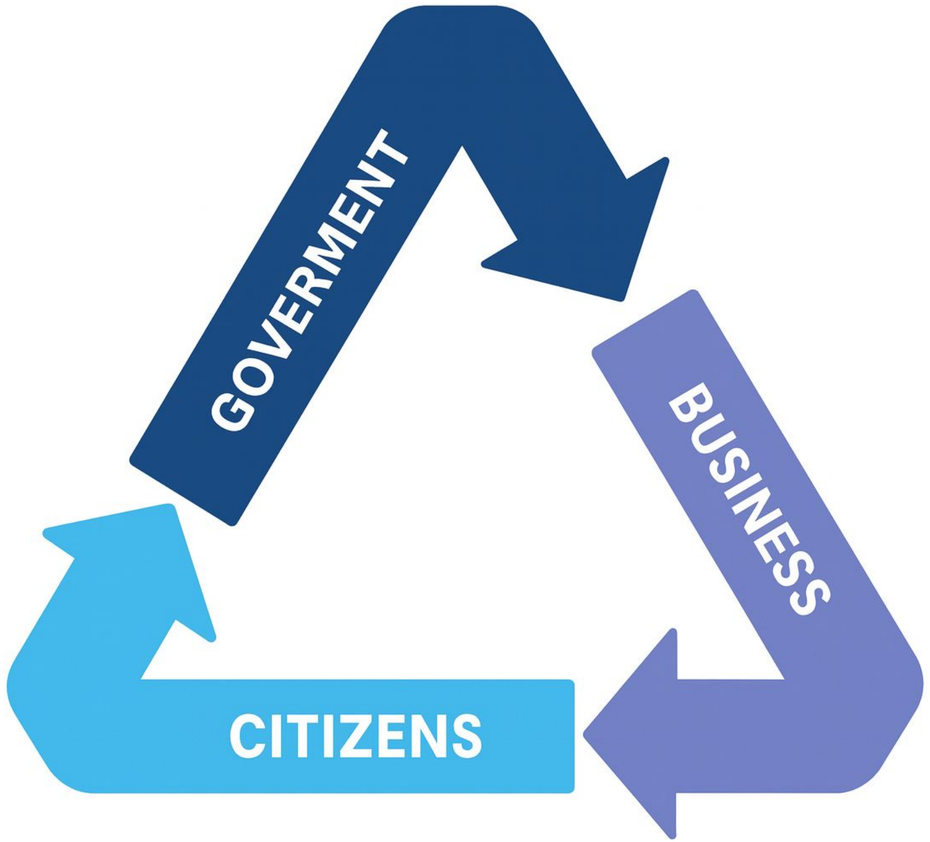
Credibilità

Sempre più spesso i cittadini si affidano alla voce di influencer più che alle fonti ufficiali

Perché le fake news sono così attraenti?

Le fake news viaggiano più veloci della verità: **hanno il 70% di probabilità in più di essere condivise** – non perché convincono di più, ma perché sorprendono, emozionano e fanno sentire le persone parte di qualcosa.

Perché il settore privato è essenziale



1. Il settore privato controlla la maggior parte delle **infrastrutture digitali**: dagli algoritmi di rilevamento ai dati comportamentali, fino agli strumenti analitici che determinano la circolazione delle informazioni.
2. Come la cybersecurity si è evoluta grazie alla **cooperazione tra pubblico e privato**, anche la protezione del dominio cognitivo richiede oggi lo stesso tipo di alleanza. Percezione e fiducia sono diventate i nuovi bersagli.
3. Solo l'unione **tra legittimità delle istituzioni, velocità e innovazione delle imprese e consapevolezza dei cittadini** può garantire una difesa efficace contro la manipolazione della realtà.

Marion Stokes registrò 35 anni di trasmissioni televisive per impedire che la storia venisse riscritta.

↓ ↓ ↓

1. Intelligence & Early Warning

HWG Sababa

Nella difesa cyber, la detection tempestiva può contenere un incidente e salvare date e infrastrutture.
Nella difesa cognitiva, salva un'intera società.

Le aziende private – tra cui fornitori di cybersecurity, laboratori di IA e società di data analytics – **monitorano già anomalie nel traffico**, comportamenti coordinati non autentici e narrazioni che si diffondono su più piattaforme.

Queste stesse competenze possono essere impiegate per individuare tempestivamente operazioni di influenza e contenerle prima che si amplifichino.

Dal Cyber SOC all'InfoOps Center

Monitorare l'ambiente informativo, integrare fonti di intelligence open-source e fornire alert precoci alle istituzioni – anche con meccanismi di automazione sia su enrichment che response.

HyperSOC™

Monitor – Detect – Alert – Share

2. Tecnologie e Strumenti

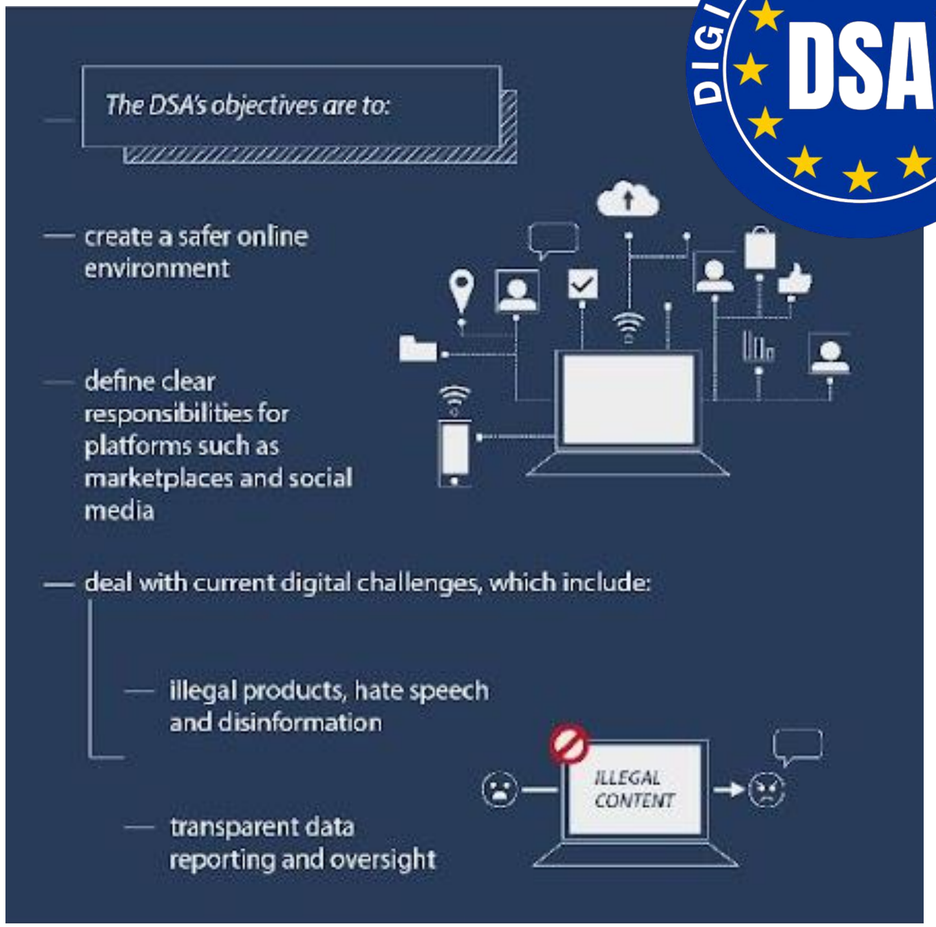
HWG Sababa

Il settore privato è il motore dell'innovazione da cui dipende la difesa cognitiva.

Laboratori di IA, startup e aziende di cybersecurity possono offrire:

- **Strumenti di rilevamento** – per individuare deepfake, bot e contenuti manipolati.
- **Analisi comportamentale** – per tracciare cambiamenti improvvisi nelle narrazioni e operazioni di influenza coordinate.
- **Piattaforme di resilienza** – per simulare e testare la resistenza a campagne di attacco cognitivo.

Con il **Digital Services Act**, questi strumenti stanno diventando parte integrante dell'ecosistema di sicurezza europeo, trasformando l'innovazione privata in difesa pubblica.



3. Costruire la resilienza

Le società resilienti non eliminano la manipolazione: imparano a riconoscerla e a resisterle.

- La resilienza pubblica si rafforza attraverso **alfabetizzazione digitale e campagne di sensibilizzazione**, sostenute dall'esperienza del settore privato in materia di marketing, scienze comportamentali e comunicazione.
- Serve una collaborazione strutturata con **media, telco, unità di fact-checking e piattaforme digitali** per rafforzare la capacità dei cittadini di riconoscere le tattiche di manipolazione e sviluppare un pensiero critico.
- I cittadini restano la prima linea di difesa, ma è il settore privato a fornire **la creatività e la capacità di diffusione** necessarie per renderla davvero efficace.

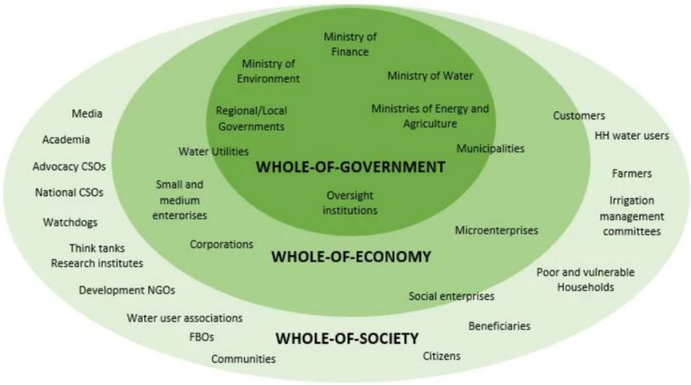
4. Gestione della Crisi

Quando un attacco cognitivo colpisce – una fake news virale, una fuga di notizie manipolata o una campagna mirata – velocità e credibilità diventano fattori decisivi.

Le istituzioni hanno bisogno di **meccanismi di risposta rapida pubblico–privati**, in cui aziende certificate contribuiscono a verificare i fatti, proteggere le comunicazioni e fornire voci affidabili non governative.

Il **Rapid Alert System** (RAS) dell'UE costituisce una base importante, ma mostra ancora limiti in termini di reattività e coinvolgimento operativo.

- Una partecipazione più attiva del settore privato può trasformarlo in un sistema dinamico e predittivo: con alert più tempestivi, copertura più ampia, narrazioni correttive immediate e maggiore fiducia pubblica.
- I timori legati a possibili bias o falsi allarmi possono essere mitigati attraverso metodi trasparenti e verifiche congiunte.
- Un approccio "whole-of-society" garantisce consapevolezza e risposta a livello locale: enti regionali e municipali possono individuare più rapidamente operazioni narrative mirate rispetto ad organi centrali.



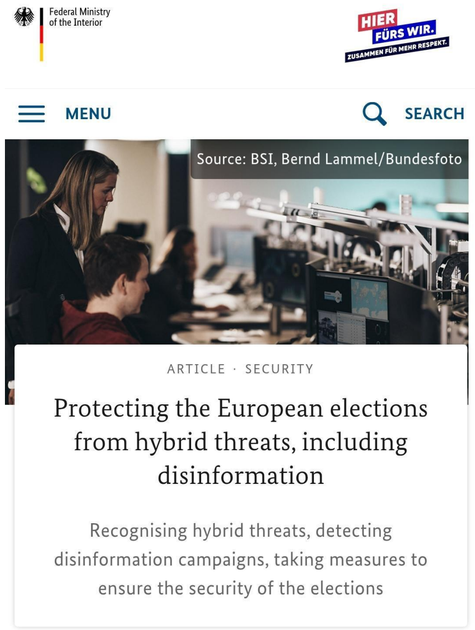
5. Ricerca e Supporto alle Policy

HWG Sababa

Costruire un’architettura della fiducia

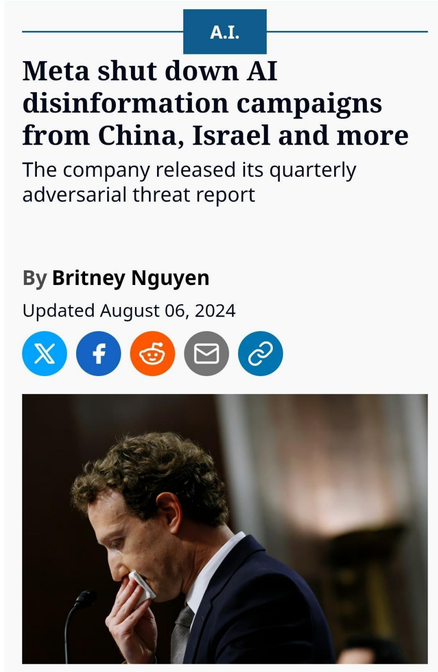
- Una difesa solida nel tempo si basa su **ricerca condivisa**, **standard comuni** e **principi etici forti**.
- La ricerca e sviluppo privata **nei campi dell’intelligenza artificiale, delle scienze comportamentali e dell’OSINT** può orientare le politiche pubbliche e contribuire a definire quadri normativi che tutelino allo stesso tempo sicurezza e libertà civili.
- La collaborazione su **etica dell’IA**, **narrative intelligence** e **integrità dell’informazione** rappresenta oggi l’equivalente dei grandi standard cyber e costituisce la base per una vera architettura della fiducia nel dominio cognitivo.
- **Le alleanze di ricerca pubblico–private** definiranno come le società potranno innovare in sicurezza nell’era dell’informazione sintetica.

La collaborazione esiste già.
Il passo successivo è estenderla al dominio cognitivo.



Per NATO e UE, la percezione è la nuova frontiera della sicurezza; la capacità di rilevamento dipende dalle partnership con l'industria.

I modelli ISAC dimostrano che condividere informazioni rafforza la fiducia; il passo successivo è condividere anche le minacce cognitive.



Il SOC può evolvere in un vero e proprio Information Operations Center, estendendo la difesa cyber alla difesa cognitiva.

Marion Stokes registrava perché sapeva che **la memoria è potere.**

Lei lo ha fatto da sola, ma **oggi la memoria è una missione condivisa.**

Nella guerra cognitiva, **istituzioni**, **imprese** e **cittadini** devono registrare, verificare e ricordare insieme.

HWG Sababa

www.hwgsababa.com