Nunzia Ciardi: «Gli attacchi sul web fanno danni enormi. L'AI ha complicato tutto. Ecco come i cittadini possono difendersi» di Rinaldo Frignani

Vicedirettore dell'Agenzia per la cybersicurezza nazionale: sui social circolano tesi create dai bot per alimentare dibattiti su notizie false o distorte

(Fonte: https://palermo.corriere.it/ 3 settembre 2026)

«Per il cittadino la disinformazione può diventare una trappola nella quale è facile cadere: un dibattito architettato con **l'intelligenza artificiale** può catturare l'attenzione e coinvolgere persone già fidelizzate con gli algoritmi per intercettare i loro interessi, persone che non si rendono conto del rischio che la propria opinione ne possa uscire distorta». Nunzia Ciardi, vicedirettore dell'**Agenzia per la cybersicurezza nazionale** e già a capo della polizia postale, lancia l'allarme sulle nuove forme di infiltrazione e anche di guerra ibrida con le quali l'Italia si sta confrontando da anni, ma che sembrano negli ultimi mesi aver avuto nuovi e inquietanti impulsi.

Direttore, cosa ci troviamo di fronte?

«Quando si vive in contesti storici turbolenti come questi, la guerra ibrida diventa sempre di più un fenomeno con il quale dovremo fare i conti. Anche perché la cifra che la distingue nel dominio digitale oggi è la dissoluzione dei confini fra fenomeni differenti. Difficile insomma dare un'etichetta a determinati eventi: quando ci troviamo di fronte a un attacco a infrastrutture importanti come ospedali, oleodotti o acquedotti è molto complesso capire se si tratti di crimine ordinario a fini di lucro (come il ransomware con richiesta di riscatto), spionaggio, aggressione da parte di uno Stato ostile oppure criminalità tollerata o sponsorizzata da uno Stato non amico».

Sono tutte situazioni molto delicate.

«Sicuramente. Si tratta di un campo doppiamente insidioso, perché senza grandi sforzi bellici tradizionali si possono aggredire e colpire infrastrutture essenziali dei Paesi presi di mira con danni enormi a costi relativamente contenuti. Ma della **guerra ibrida fanno parte anche il creare difficoltà nel distinguere quello che sta accadendo** e fornire un'informazione distorta che può fare anch'essa gravi danni. In questo caso alla libera formazione del consenso. È un vero e proprio attacco alla circolazione delle idee e alla volontà delle persone inquinata proprio da messaggi e campagne di disinformazione».

Come si possono influenzare le opinioni altrui oggi?

«L'esempio più banale è quello dei social utilizzati per alimentare dibattiti su notizie inventate o distorte, tesi a a loro volta a creare discussioni che abilitano la disinformazione. A volte sono create da una serie di bot che distribuiscono messaggi e notizie non corretti, che servono anche a sollecitare sentimenti come indignazione, curiosità, paura su temi delicati. Finisce che il dibattito si auto-alimenta con utenti che partecipano, si potrebbe dire, intorno a una falda già inquinata a monte».

E come si possono contrastare questi attacchi?

«Non è semplice. Perché simili azioni sono difficilmente punibili in quanto si tratta di una materia scivolosa che rientra nella **libertà di espressione e di informazione**. Ed è anche difficile distinguere il vero dal falso, nonché circoscriverlo e individuare chi ha innescato l'attacco. Però posso dire per esperienza che una delle armi fondamentali per contrastare questo genere di situazioni è la preparazione delle persone, lo sviluppo di uno spirito critico. Non dobbiamo accettare acriticamente determinate notizie. Siamo invece purtroppo abituati a pensare che tutto quello che ci viene mostrato dalla Rete e sulla Rete sia indiscutibilmente vero. Invece la verità oggi è una realtà complessa».

Dominata dall'AI?

«Il massiccio avvento dell'Intelligenza artificiale in tutto questo ha complicato enormemente l'intero scenario. Se prima potevamo intercettare un allegato infetto in una mail con un minimo di attenzione, adesso è tutto molto più credibile, non ci sono più errori ortografici o di traduzione. Ma ricordo che credibile non vuol dire vero. Un dato: ci sono voluti 75 anni perché il telefono raggiungesse 100 milioni di utenti, 33 per l'auto, 16 per il cellulare, tre per Whatsapp, nove mesi per TikTok, ma appena due per ChatGPT. La velocità tecnologica non è mai stata così forte, è una valanga di informazioni alle quali il cittadino digitale viene sottoposto oggi. E l'AI è diventata l'arma ideale per la guerra ibrida perché in pochi secondi individua le vulnerabilità degli obiettivi».

Ma può essere usata anche per difendersi?

«Certo, ed è quello che accade. Perché non si stanca, è attiva 24 ore su 24 e intercetta anomalie del traffico di dati anche minime per lanciare l'allarme perché possono essere precursori di un attacco. Come Agenzia siamo in prima linea nell'uso dell'IA per prevenire incidenti. Negli Usa di recente ce ne sono stati alcuni con il blocco degli acquedotti. Ebbene, a ottobre in Italia fra le tante esercitazioni che facciamo ce ne sarà una proprio per prevenire attacchi cyber alle reti idriche, grandi e piccole per insegnare agli operatori come difendersi. Insomma, stiamo lavorando d'anticipo perché il momento lo richiede».