

Corsa all'intelligenza artificiale e cybersicurezza. Intervista a Carola Frediani

di Francesco Nasi

20-05-2025

Le tecnologie digitali sono ormai parte integrante dei conflitti moderni: attacchi cyber, propaganda e automazione dei sistemi d'arma. Guardando all'intelligenza artificiale, è ancora più evidente come le grandi potenze si muovano in un cyberspazio privo di regole condivise, mentre le Big Tech condizionano sempre di più le politiche globali. In questa intervista, Carola Frediani - tecnologa per la sicurezza informatica, giornalista esperta di cybersicurezza e cofondatrice del progetto di informazione su temi cyber e digitali "Guerre di Rete" - analizza come l'intelligenza artificiale generativa apra nuove frontiere ma esponga anche a gravi rischi legati alla privacy, ai bias e alle manipolazioni.

Negli ultimi due anni nuovi sistemi di intelligenza artificiale generativa hanno conquistato l'attenzione del dibattito pubblico e suscitato molte riflessioni sul loro impatto a livello sociale. Questi sistemi rientrano nell'ambito di attenzione della cybersecurity? Se sì, quali nuove possibilità e minacce portano con sé?

Carola Frediani: Se da un lato le tecnologie di intelligenza artificiale hanno portato a molte novità, dall'altro sono esposte a un numero crescente di minacce e vulnerabilità per la sicurezza. Alcune sono specifiche dei modelli e dei sistemi di intelligenza artificiale, altre sono legate più in generale all'infrastruttura software. Ad esempio, per citarne solo alcune, la mancanza di misure per salvaguardare i dati sensibili durante lo sviluppo, la fase di test e l'implementazione dei modelli, può portare a violazioni della privacy. Oppure c'è il rischio dell'introduzione (deliberata o meno) di pregiudizi (bias) nei modelli di apprendimento automatico o nei dataset utilizzati per addestrarli, con conseguenti risultati distorti. O ancora la possibilità di inviare istruzioni malevole in un modello di intelligenza artificiale (prompt injection), facendolo deviare dal comportamento previsto. Consiglio la lettura dell'ultimo report OWASP (Open Worldwide Application Security Project) al riguardo.

Gli attuali scenari di conflitto armato - pensiamo all'Ucraina e a Gaza, ma anche al Sudan - non si limitano alla violenza fisica, ma presentano forme ibride di cyber warfare, dove il digitale e le nuove tecnologie fungono sia terreno di scontro che da arma da combattimento. Quali sono le caratteristiche principali di queste forme di conflitto?

Carola Frediani: Ci sono diverse cose che colpiscono nelle ultime guerre che abbiamo visto: la crescente rilevanza di attacchi cyber che precedono e accompagnano la guerra, con due obiettivi principali: disarticolare infrastrutture critiche, a partire da quelle di comunicazione; e la propaganda sui social. Poi la mobilitazione di gruppi di cyber-volontari o di gruppi di hacktivisti (o presunti tali); l'uso di droni e la loro progressiva automazione; l'uso di sistemi di intelligenza artificiale per individuare e accelerare l'individuazione di obiettivi da colpire, col rischio concreto di diminuire la supervisione e la responsabilità umana.

Oltre agli scenari di conflitto armato vero e proprio, di cui spesso anche il grande pubblico può prendere contezza attraverso i media mainstream, perdurano le operazioni di cyber warfare tra

Stati. Pensiamo all'attacco portato avanti dal gruppo Salt Typhoon, vicino al governo cinese, nei confronti di milioni di cittadini americani, un attacco che sarebbe addirittura arrivato a violare il sistema di intercettazioni usato dall'FBI. Come si stanno muovendo le grandi potenze su questo fronte?

Carola Frediani: Questi attacchi ci sono sempre stati. Il caso Salt Typhoon mostra che se un governo o un'azienda raccolgono dati sensibili, o indeboliscono dei sistemi introducendo delle vulnerabilità, ci saranno anche altri soggetti pronti ad approfittarne. Per questo non bisogna raccogliere più dati di quelli strettamente necessari, e dove necessario, bisogna implementare i più alti standard di sicurezza. In generale, sul fronte cyber le grandi potenze (penso a Stati Uniti, Cina, Russia, Israele, Gran Bretagna) non sembrano interessate finora a raggiungere accordi per regolare l'uso di questi strumenti. Che tra le altre cose offrono l'opportunità della plausible deniability, cioè di mascherare e negare la paternità di un attacco. Poi, se si ha tempo e si hanno risorse, si riesce ad arrivare a una attribuzione ma ci si muove comunque in uno spazio grigio e ambiguo per definizione.

L'ascesa dell'intelligenza artificiale ha portato alla ribalta nuove aziende tecnologiche, come Open AI (Chat GPT), Anthropic (Claude) e NVIDIA (la quale ha però una traiettoria di sviluppo diversa dalle altre). Quali sono i punti di forza e i limiti di queste aziende? Che ruolo giocano nello sviluppo dell'intelligenza artificiale? Sono giganti destinati a durare?

Carola Frediani: Siamo nel mezzo di una corsa all'intelligenza artificiale che è commerciale, industriale, nazionale, strategica. In questa corsa c'è tanto hype. Ci sono contraddizioni anche terminologiche e ideologiche che trovano spiegazione solo nella logica "move fast, break things" e fai una exit con un sacco di soldi. Questo dopo aver saccheggiato dati, opere, contenuti per i processi di addestramento. Inoltre, rischiamo di dimenticarci che prima della GenAI eravamo già immersi in altre forme di intelligenza artificiale, come quella predittiva, che sono forse meno visibili ma probabilmente più importanti perché hanno un impatto su decisioni che ci riguardano. Per fortuna l'AI Act europeo, la legge sull'intelligenza artificiale, questo lo aveva ben presente, anzi era nata nella sua elaborazione ben prima di questa recente esplosione di chatbot e generatori di immagini. Quindi quanto dureranno queste aziende è difficile da prevedere perché le variabili in gioco sono tante, e anche di natura geopolitica.

La seconda presidenza di Donald Trump negli Stati Uniti si annuncia come ancora più dirompente della prima. Che cosa ci dobbiamo aspettare in termini di politiche digitali? E in questo quadro, che ruolo potrà giocare un imprenditore come Elon Musk, che, come sappiamo, ha avuto una posizione determinante nella campagna elettorale repubblicana?

Carola Frediani: Lo stiamo vedendo già dai primi giorni di presidenza Trump: apertura al mondo delle criptovalute; eliminazione dei limiti e delle richieste di trasparenza per le aziende attive nell'intelligenza artificiale; richiesta all'Unione Europea di non applicare le sue leggi con le aziende americane. Ed è solo l'inizio. Di Elon Musk ci sarebbe molto da dire, ma possiamo limitarci a dire che sicuramente sta influenzando altri imprenditori tech, a partire da Mark Zuckerberg.

Come dimostrato in maniera esplicita dal caso Musk (ma anche dal repentino cambio delle policy sulla moderazione dei contenuti su Meta preannunciato da Zuckerberg), il connubio tra imprese private e potere pubblico è decisivo, indipendentemente dall'area geografica di appartenenza. Come si configura questo rapporto tra Big Tech e istituzioni nei vari contesti regionali? Quali sono le differenze tra grandi attori come Cina, Unione Europea e Stati Uniti?

Carola Frediani: Questo connubio non è un fenomeno del tutto nuovo. Ma con i giganti tech e dell'intelligenza artificiale rischia di riconfigurare gli equilibri fra poteri privati e statali. Quello che stiamo vedendo negli Stati Uniti è senza precedenti. L'uomo più ricco del mondo, che controlla

tecnologie essenziali per la Difesa (come i satelliti), che si compra una piattaforma per influenzare media e politica e la usa in modo privatistico, che va al governo ma in forma obliqua per cui mantiene tutti i suoi conflitti di interesse, anzi li accresce e che ora punta a rientrare nella partita dell'intelligenza artificiale da protagonista. Dov'è lo Stato? Ma, soprattutto, cos'è diventato?

Concentrandoci invece sull'Unione Europea, si è parlato molto negli ultimi anni dell'impianto regolatorio composto da Artificial Intelligence Act, Digital Markets Act e Digital Services Act. Qual è l'obiettivo di queste normative? Riusciranno a costruire un modello "europeo" di sviluppo tecnologico?

Carola Frediani: Queste leggi europee hanno vari obiettivi ma sicuramente al centro c'è l'idea che le aziende tech e digitali non siano immuni a una regolamentazione che tuteli i diritti dei cittadini, così come altre aziende e settori industriali nel tempo hanno dovuto sottostare a una serie di regole sulla salute, l'ambiente, l'inquinamento, la tracciabilità della filiera, i diritti del lavoro, la tassazione e via dicendo. Per di più queste aziende lavorano in un ambito che va a toccare temi delicati, che incidono ad esempio sull'ecosistema informativo, e quindi possono avere vari impatti sui meccanismi delle democrazie. Non parliamo poi dell'impatto di sistemi che introducono decisioni automatizzate sulla base di modelli di intelligenza artificiale: giustamente l'AI Act europeo ha messo una serie di paletti per impedire che questi sistemi agiscano in totale opacità con effetti rilevanti sulla vita delle persone.

Infine, quale ruolo può ritagliarsi l'Italia in questa partita? Qual è la situazione del nostro Paese sul fronte del digitale, e più in particolare su due ambiti come la cybersicurezza e la corsa all'intelligenza artificiale?

Carola Frediani: L'Italia non spicca in modo particolare in Europa su questi temi. C'è sicuramente tanto lavoro da fare, soprattutto sul fronte della cybersicurezza della Pubblica Amministrazione. Ma pensare di muoversi su alcuni temi solo come singolo Stato mi pare riduttivo, soprattutto quando si parla di sviluppo industriale. L'Unione Europea e i maggiori Stati europei devono trovare il modo di creare politiche industriali congiunte, perché le sfide a livello globale sono troppo difficili da gestire. Come singolo Stato possiamo fare del piccolo cabotaggio e avere l'impressione di cavarcela sul breve termine, ma a lungo termine serve una visione più ampia.