Intelligenza Artificiale, la fine del mondo è garantita

geopolitika.ru/it/article/intelligenza-artificiale-la-fine-del-mondo-e-garantita

27 febbraio 2024

Aleksandr Dugin

Per procedere verso l'onnipotenza dell'Intelligenza Artificiale (IA), è necessario concettualizzare l'umanità stessa come un grande computer, i cui elementi, tuttavia, non funzionano troppo perfettamente.

Il materialismo, il nominalismo, l'evoluzionismo, la filosofia analitica (basata sul positivismo logico) e la tecnocrazia stanno preparando una base teorica per questo (trasmessa e implementata attraverso la scienza, l'educazione e la cultura).

In un certo senso, l'umanità, così come è rappresentata dalla scienza e dalla filosofia moderne, è già un'IA, una rete neurale. L'IA è umana nella misura in cui il pensiero dell'umanità è artificiale, emulato dalle epistemologie del Moderno e del Postmoderno.

- Lo Stato borghese è un computer di prima generazione.
- La società civile è di seconda generazione.
- Il dominio completo del governo mondiale è della terza.
- La transizione all'intelligenza artificiale è la quarta, la finalizzazione del processo di alienazione.

La storia del capitalismo è il processo di creazione del supercomputer. È impossibile fermarsi a metà strada. La nuova era culminerà, necessariamente, nell'IA.

L'unico modo per cambiare questo stato di cose è rifiutare la Modernità nella sua interezza, con la sua intera immagine scientifica del mondo, che è un'abiezione di Dio e dell'uomo.

La filosofia gender è la penultima tappa di questo percorso: i transgender sono un riscaldamento prima del passaggio a individui transumani (l'umano è facoltativo). Dopo aver rifiutato il cristianesimo e il Medioevo, l'Occidente, come i maiali gardesani, si è precipitato verso il baratro. Perché dovremmo sorprenderci se ci ritroviamo a precipitare verso il basso?

L'intelligenza artificiale è l'ultima fermata, ma siamo saliti su questo treno 500 anni fa. L'unico modo per fare la differenza è far deragliare il capitalismo, ora, altrimenti ciao.

L’a Ontologia Orientata agli Oggetti è in generale l'ontologia perfetta e sviluppata dei paesaggi postumani - il genocidio del soggetto a favore dei Grand Dehors (leggi divinità idiote - la loro metafora, non la nostra!). I Grand Dehors dominano il mondo moderno. Novorossiya è sulla sua strada. La SMO è una guerra filosofica.

Il compito dei russi è quello di superare la cyber-realtà, è difficile evitarla, dovremo cavalcare la tigre e trasformare il veleno in medicina. L'Idea russa deve sconfiggere e sottomettere non solo l'Ucraina, ma anche l'Intelligenza Artificiale. Questa è la posta in gioco.

Traduzione a cura di Lorenzo Maria Pacini

Il ruolo dell’intelligenza artificiale alla frontiera della cybersicurezza

wired.it/branded/article/intelligenza-artificiale-cybersicurezza-microsoft

Gianluca Dotti

21 febbraio 2024

L’incremento del numero di ransomware e l’ampliamento del perimetro di attacco da parte dei cybercriminali rende necessario impiegare strumenti di difesa sempre più precisi e rapidi. La consapevolezza sui rischi e l'adozione di comportamenti virtuosi sono essenziali per creare sistemi di sicurezza efficaci: ne abbiamo discusso con Tamara Zancan di Microsoft Italia

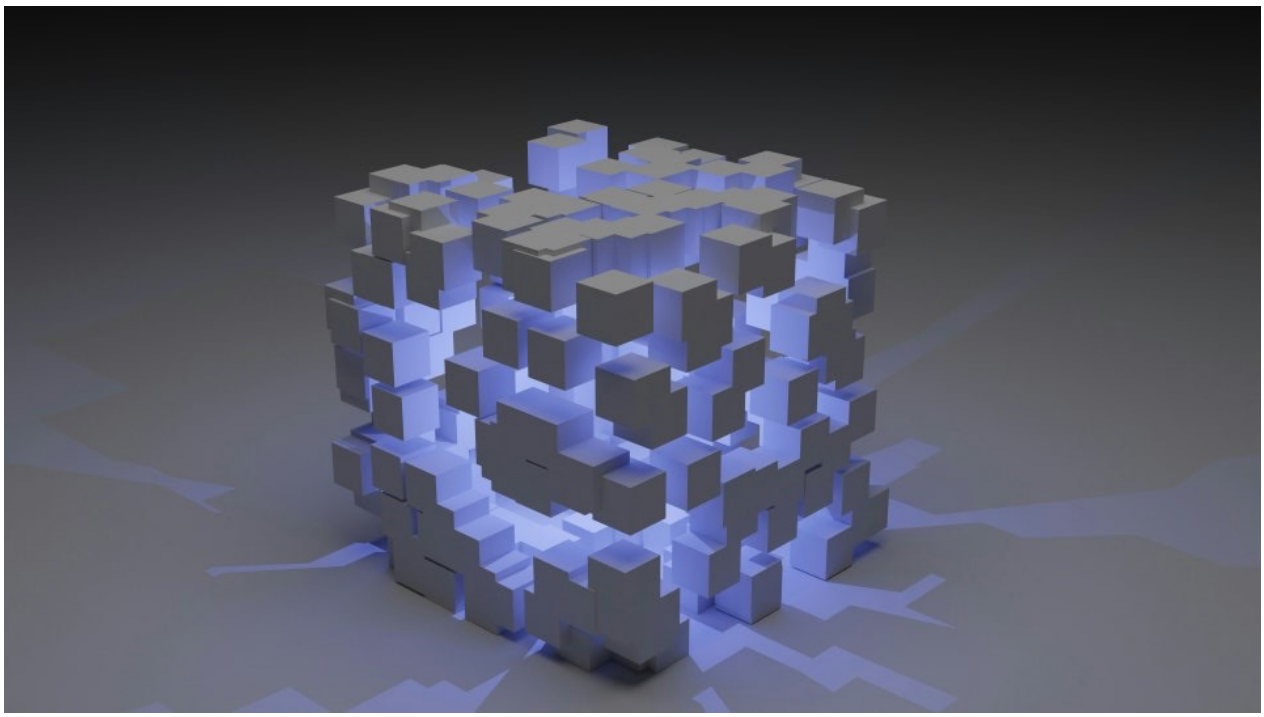

foto: Shubham Dhage/Unsplash

In un contesto caratterizzato dalla crescita vertiginosa delle **minacce digitali**, il ruolo della **cybersecurity** e della **protezione dei dati** è diventato essenziale, sia dal punto di vista tecnologico ed economico sia - di conseguenza - per lo sviluppo sociale. Dal più recente

Microsoft Digital Defense Report, i cui dati sono relativi al periodo tra luglio 2022 e giugno 2023, emergono per esempio trend globali e dati preoccupanti per la sicurezza delle aziende, delle organizzazioni e anche dei singoli utenti della rete. Tra **innovazione digitale**, **intelligenza artificiale** e **big data**, è necessaria la creazione di una maggiore consapevolezza collettiva, partendo da percorsi formativi *ad hoc* nelle scuole fino ad arrivare all'aggiornamento costante di chi ogni giorno deve fare i conti con nuove minacce informatiche. Abbiamo parlato di questi temi con **Tamara Zancan**, Direttrice Cybersecurity, Compliance e Identity di **Microsoft Italia**.

Tamara Zancan, cosa significa fare cybersicurezza in questo momento storico? E quali sono le sfide che è necessario affrontare per non farsi cogliere impreparati?

"Negli ultimi anni si è verificata un'accelerazione senza precedenti nell'innovazione tecnologica, ridefinendo sia le metodologie di attacco dei cybercriminali sia gli strumenti di cybersicurezza. Le complessità aumentano di giorno in giorno ed è essenziale **investire per aggiornare le tecnologie per la difesa**. Le aziende e le organizzazioni devono essere in grado di individuare le intrusioni in maniera tempestiva ed efficace per evitare la perdita di dati e informazioni sensibili.

"Noi di Microsoft rileviamo ogni mese **30 miliardi di attacchi alle password**, e questi numeri sono destinati a crescere considerando le caratteristiche del mondo attuale. Anche i sistemi di **autenticazione a più fattori** sono considerati un elemento di rischio: i cybercriminali effettuano tentativi di accesso nella speranza che gli utenti accettino senza verificare. L'obiettivo primario rimane quello di sensibilizzare il più possibile, ribadendo l'importanza di adottare comportamenti virtuosi nella quotidianità. Nel nostro caso stiamo adottanto l'approccio cosiddetto **zero trust**, ossia viene controllato qualsiasi accesso alle infrastrutture aziendali, grazie a sistemi di autenticazione multifattoriali"

Tamara Zancan, Direttrice Cybersecurity, Compliance e Identity di Microsoft Italia

Quali sono i trend globali più rilevanti in materia di cybersicurezza?

"Il **Microsoft Digital Defense Report** ha fatto emergere un aumento generalizzato degli attacchi informatici. I ransomware, virus che limitano l'accesso a un dispositivo e ne mettono in pericolo i dati, sono sempre più veloci e sofisticati, mettendo continuamente alla prova i sistemi di sicurezza. L'obiettivo principale degli attacchi rimane **rubare informazioni**, ma anche monitorare le comunicazioni o manipolare l'opinione pubblica.

"Negli ultimi anni i ransomware sono diventati una minaccia più consistente sia per le aziende sia per i singoli utenti. Rispetto allo stesso periodo dell'anno precedente, sono **aumentati del 70%**. L'obiettivo che perseguiamo è diventare sempre più veloci nel rispondere a minacce che sono più sofisticate e rapide. Molto spesso **il tempo risulta essere un fattore chiave**, perché ritardi anche solo di qualche minuto nell'azione contro

l’attacco possono essere determinanti per l’inefficacia della difesa. Numeri alla mano, gli effetti di virus sugli utenti sono sempre più rapidi: il tempo medio tra quando – per esempio – viene cliccato un link malevolo e quando di verifica il danno è ormai **inferiore a un’ora**”.

Di quali strumenti possono dotarsi utenti e aziende per proteggere dati e asset? E che ruolo può avere l’intelligenza artificiale?

“L’intelligenza artificiale è uno strumento di cui non si può più fare a meno, perché garantisce un **livello di attenzione e monitoraggio** non raggiungibile in altro modo. I sistemi di AI da un lato sono una nuova opportunità di difesa, dall’altro aprono le porte a **ulteriori minacce da parte dei cybercriminali**. Visto che le aziende hanno una struttura sempre più aperta, il perimetro da difendere è molto più esteso rispetto a prima, e di conseguenza aumentano i punti di vulnerabilità. Questo implica la necessità di **controllare un numero elevato di aspetti differenti**, anche all’interno dell’IoT, e questo diventa possibile solamente grazie al supporto di software automatizzati, capaci di analizzare in pochi istanti enormi quantità di dati. Inoltre, gli algoritmi di AI riescono a produrre informazioni utili per il **miglioramento dei sistemi di cybersecurity**, identificando i punti deboli nel perimetro di difesa”.

In che modo Microsoft utilizza i sistemi di AI per proteggere i dati dai cybercriminali?

"Già da qualche anno abbiamo incluso l’utilizzo dell’intelligenza artificiale come strumento automatizzato per il rilevamento delle minacce e per fornire un supporto al team di sicurezza durante un attacco. A partire dal 2023, è stato annunciato **Microsoft Copilot for Security**, uno strumento di cybersecurity basato sull’intelligenza artificiale capace di individuare e rispondere ancora più rapidamente alle minacce informatiche. Progettato per lavorare in **stretta sinergia con il team dei professionisti della sicurezza**, consente di controllare con maggiore precisione cosa stia accadendo all’interno dei propri ambienti. Grazie all’utilizzo di questo strumento, vengono colti anche dei dettagli fondamentali sia per velocizzare gli interventi durante le emergenze sia per supportare i nuovi professionisti a sviluppare competenze più specialistiche. È anche facile da utilizzare e **collegato con i modelli di OpenAI**, in modo tale da essere continuamente aggiornato con i sistemi di sicurezza più all’avanguardia".

Qual è oggi il valore della formazione sulla cybersicurezza? E chi sono le persone su cui è più importante fare questa azione?

“Chiunque può e deve contribuire alla diffusione della consapevolezza dei rischi relativi alla sicurezza, anche perché questi non riguardano solamente **furti di identità o di denaro** ma possono coinvolgere anche questioni **sanitarie** e **geopolitiche**. Non si tratta più di una questione rilevante per i soli addetti ai lavori, ma è necessario che **tutti prestino attenzione alla sicurezza** dei propri dati, per se stessi e per gli altri. È bene sempre ricordare che il rischio non riguarda solamente le grandi aziende, ma anche per le piccole e medie imprese, e i singoli cittadini.

“La Fondazione Mondo Digitale insieme a Microsoft Italia si è fatta promotrice di un’**Alleanza per la cybersecurity**, per rafforzare la consapevolezza tra i cittadini. Ancora troppo spesso mancano, per esempio, percorsi formativi specifici rivolti alla sicurezza in rete e momenti di formazione all’interno delle aziende per **ridurre i comportamenti potenzialmente pericolosi**”

La sua posizione lavorativa, ossia che ci sia una donna a capo di una divisione dedicata alla cybersicurezza, fa ancora notizia. Cosa si può fare per promuovere il raggiungimento di una reale parità di genere nell’ambito della cybersecurity?

“Cercare di avvicinare le donne alle discipline tecniche e informatiche è una sfida che portiamo avanti quotidianamente, anche attraverso **percorsi scolastici e programmi di formazione**. Rendere le discipline Stem più adatte e appetibili alle ragazze, cercando di superare le barriere culturali, è essenziale per favorire la parità di genere. Soprattutto se si considera la direzione che sta prendendo il mondo del lavoro. Nonostante in questi ultimi anni si siano visti notevoli passi in avanti – quando ho iniziato a lavorare, ai congressi ero sempre l’unica donna o quasi – la strada da fare è ancora tanta, anzitutto a **livello culturale**. Ci tengo a trasmettere l’idea che anche nell’ambito della cybersecurity possono lavorare tante donne: sarebbe molto bello se un giorno potesse diventare una cosa del tutto *normale* e non più un'eccezione”.