

Cybersicurezza, disinformazione e libertà individuale nell'era dell' IA

Raffaele Federici



- Il 30 gennaio 2024 i CEO dei principali social network sono stati ascoltati dai membri della commissione giustizia del Senato degli Stati Uniti intenti a promuovere un progetto di legge volto a responsabilizzare le società private per i materiali pubblicati nelle piattaforme di loro proprietà.
- Gli algoritmi hanno un potere stupefacente per individuare le nostre vulnerabilità, non solo i nostri gusti e preferenze.



Perché questo passaggio?

- L'IA negli ultimi anni è al centro dei processi produttivi delle piattaforme digitali.
 - Viene utilizzata per analizzare i dati dell'utente per fornire contenuti personalizzati con il rischio di creare una "bolla di filtro" che limita la loro esposizione a opinioni diverse.
 - Viene usata per monitorare le attività dei concorrenti sui social media, come l'interazione con i clienti e la pubblicità, ma anche per modellare il comportamento degli utenti stessi attraverso tecniche di persuasione, ossia inducendoli a interagire con la piattaforma in modo specifico, ad esempio utilizzando le notifiche push o giochi interattivi: il confine tra finzionale e reale, tra artificiale e umano, si assottiglia se non addirittura ibrida.

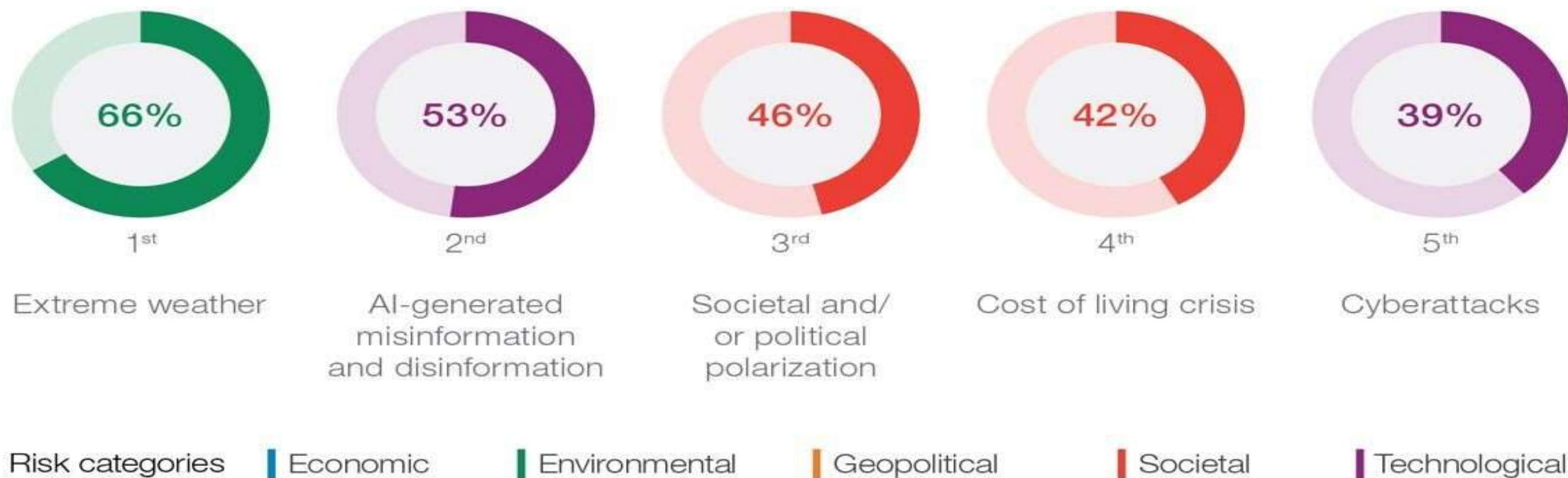
L'Intelligenza Artificiale

- È un argomento ubiquo.
- Ognuno di noi ne ha una idea e ne immagina le sue innumerevoli applicazioni.
- Pochi sanno realmente come funzioni.
- Nessuno può dire con certezza cosa porterà.

- In una società sempre più interconnessa, la sicurezza informatica rappresenta una delle principali sfide.
- Il cyberspazio è il nuovo ambiente di comunicazione emergente dall'interconnessione mondiale dei computer dove insistono macchine dotate di intelligenza artificiale.
- Il cyberspazio, ossia l'ambiente digitale in cui si svolgono le attività online, è diventato una nuova frontiera di conflitto tra le nazioni e i gruppi di attori non statali;
- La protezione delle infrastrutture critiche è diventata una priorità assoluta per i governi, le organizzazioni pubbliche e private e gli individui.

Current risk landscape

"Please select up to five risks that you believe are most likely to present a material crisis on a global scale in 2024."



Source: World Economic Forum Global Risks Perception Survey 2023-2024.

- La rivoluzione tecnologica contemporanea sta producendo mutamenti radicali nell'architettura del tessuto sociale, apportando cambiamenti nelle relazioni con sé e con l'altro, con la percezione dello spazio, con la rilevanza del lavoro, della politica, dell'economia, ma in particolar modo con il mondo delle informazioni e delle modalità attraverso le quali interagire con la conoscenza: tutte le istituzioni sono state chiamate a modificare i propri assetti dalla digitalizzazione dei dati, dall'uso dei digital device, dalla diffusione dell'intelligenza artificiale con il fine di migliorare le proprie prestazioni e possibilità di offerta rispetto alle crescenti richieste della società

- L'essere umano ha da sempre un timore reverenziale verso quello che immagina e costruisce.
- Come se fossimo costantemente in attesa che le nostre stesse opere ci distruggano.
- Pensiamo al Golem: una figura antropomorfa fatta di argilla che il rabbino di Praga, Jehuda Löw ben Bezalel, nel XVI secolo, plasmò e risvegliò allo scopo di proteggere il quartiere ebraico della città. Ma i golem diventarono sempre più grandi, al punto che il rabbino non fu più in grado di servirsene per difendere la sua comunità dagli attacchi antisemiti e così decise di disfarsi dei più grandi. Fino a quando perse il controllo di un gigante che iniziò a distruggere tutto ciò che incontrava: un epilogo tutt'altro che felice.



Juho Steiner-Pong 1915

Isaac Asimov

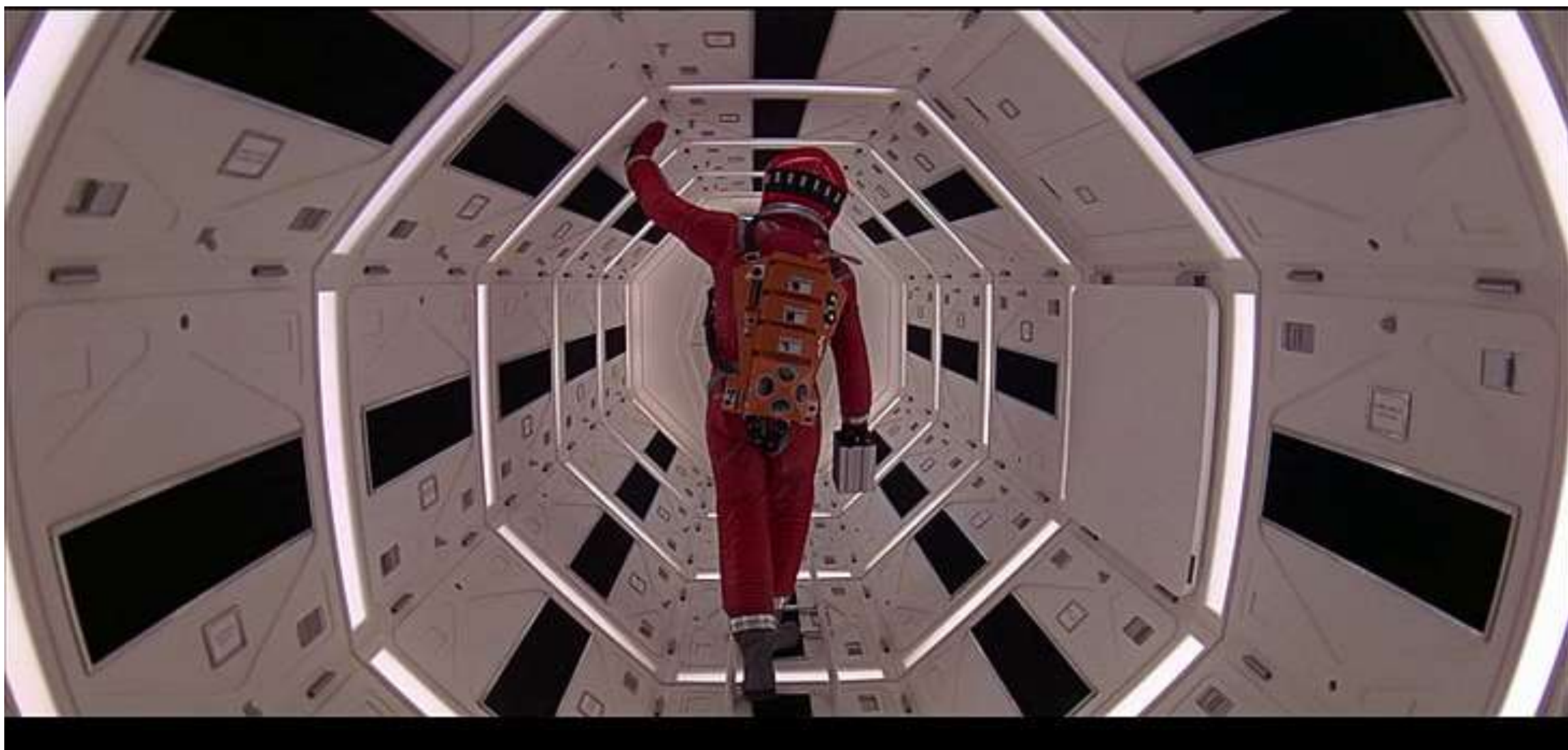
- “Anche da giovane non riuscivo a condividere l’opinione che, se la conoscenza è pericolosa, la soluzione ideale risiede nell’ignoranza. Mi è sempre parso, invece, che la risposta autentica a questo problema stia nella saggezza. Non è saggio rifiutarsi di affrontare il pericolo, anche se bisogna farlo con la dovuta cautela. Dopotutto, è questo il senso della sfida posta all’uomo fin da quando un gruppo di primati si evolse nella nostra specie. Qualsiasi innovazione tecnologica può essere pericolosa: il fuoco lo è stato fin dal principio, e il linguaggio ancor di più; si può dire che entrambi siano ancora pericolosi al giorno d’oggi, ma nessun uomo potrebbe dirsi tale senza il fuoco e senza la parola”

LE TRE LEGGI DELLA ROBOTICA

1. Un robot non può recar danno a un essere umano né può permettere che, a causa del proprio mancato intervento, un essere umano riceva danno.
2. Un robot deve obbedire agli ordini impartiti dagli esseri umani, purché tali ordini non contravvengano alla Prima Legge.
3. Un robot deve proteggere la propria esistenza, purché questa autodifesa non contrasti con la Prima e con la Seconda Legge.

MANUALE DI ROBOTICA
56^a Edizione - 2058 d.C.













- Dopo il lancio di ChatGPT da parte di OpenAI, l'intelligenza artificiale generativa è diventata uno dei temi di attenzione più caldi per le sue potenziali ricadute economiche, securitarie e geopolitiche.
- Recentemente la startup xAI di Elon Musk ha svelato il suo chatbot Grok, integrato con la piattaforma X.
- A sua volta, in Cina Ant Group di Alibaba ha ricevuto il via libera dal governo per distribuire prodotti basati sul suo modello di IA generativa nel settore finanziario.
 - È l'inizio di una nuova rivoluzione tech?

- L'Intelligenza Artificiale ha almeno tre punti di forza:
 - (1) la crescita esponenziale delle prestazioni computazionali (potenza di calcolo);
 - (2) la concomitante disponibilità di enormi set di dati e progressi nello sviluppo di algoritmi di apprendimento profondo (deep learning);
 - (3) la rapida espansione (e raccolta) degli investimenti.

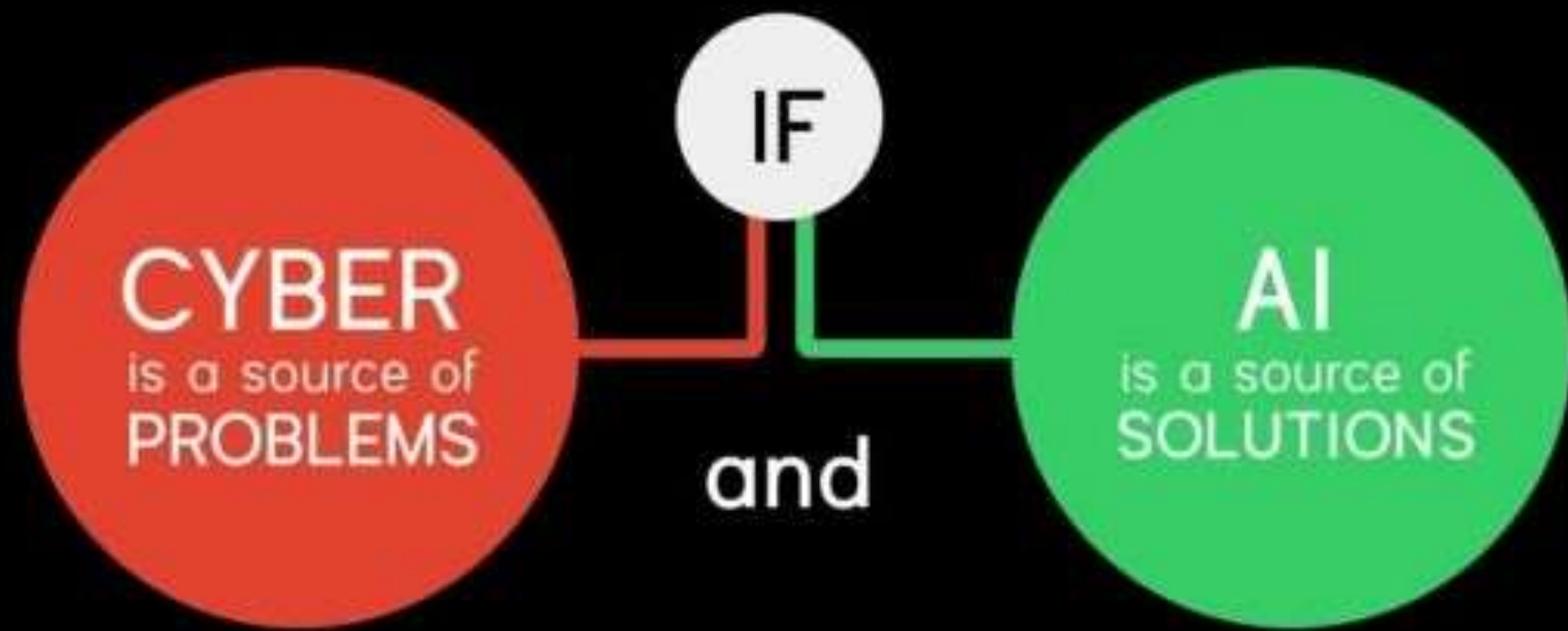
Nel tempo in cui il panorama tecnologico è in costante evoluzione e definisce la nostra esistenza, l'integrazione tra intelligenza artificiale (AI) e cybersicurezza sta diventando sempre più rilevante nell'ambito dell'innovazione.

- Questi due settori, un tempo erano separati, si stanno ora incontrando e intersecando in modi che promettono di ridefinire le basi stesse della sicurezza digitale.



- La convergenza tra Intelligenza Artificiale e cybersicurezza è essenziale in un mondo in continua evoluzione.
- L'adozione di strumenti e tecniche basate sull'IA nella cybersicurezza non è più solo un'opzione, ma una necessità per contrastare l'aumento della sofisticazione degli attacchi informatici.
 - Ma ci sono anche nuovi rischi.

- Dalle decisioni algoritmiche alle raccomandazioni sugli acquisti, dai robot alla sorveglianza sociale, dalla cybersicurezza all'autonomia operativa dei veicoli e delle armi, l'impatto dell'intelligenza artificiale e della robotica sulla vita delle persone è sempre più ramificato e pervasivo.
- Difficile restituire un quadro d'insieme delle questioni etiche sollevate dall'incontro tra IA e individui nella società contemporanea: la protezione dell'autonomia a fronte della raccolta minuziosa di dati personali, le forme di benessere collettivo da promuovere attraverso l'automazione, la trasparenza e l'equità delle decisioni prese con il supporto di un algoritmo, il ruolo dei sistemi intelligenti nella crisi ambientale.
- L'automazione non è segno incontrovertibile di sventura, ma nemmeno indizio sicuro di progresso.
- Cosa sarà delle persone, delle società e della vita sul nostro pianeta dipende in modo cruciale da come sapremo affrontare le sfide etiche dell'età dell'intelligenza artificiale.



What happens if we bring the two together?











Dati e sicurezza

- La quantità di informazioni attualmente in circolazione e, soprattutto, il crescente valore commerciale delle stesse ha condotto ad una società dell'informazione, caratterizzata dal crescente valore della conoscenza (tanto che, scriveva Lyotard, «la questione del sapere nell'era dell'informatica è più che mai la questione del governo»).
- Oggi, il sapere ha la forma del dato.
 - E (anche) il potere.

La libertà e i dati

- In un mondo in cui ognuno può condividere la propria esperienza online, attraversando ogni barriera spaziale, per entrare in una rete di interconnessione globale, che diventa fonte di informazione, luogo di incontro (matchmaker), custode delle memorie, modalità di lavoro, lasciamo ogni giorno dietro di noi una serie di tracce, sulle nostre attività, spostamenti, preferenze, sul nostro stesso modo di essere.
 - I dati non svaniscono.
- Se moltiplichiamo le piccole tracce per milioni di utenti, ci rendiamo conto dell'enorme mole di dati che può essere raccolta. L'informazione digitale è radicata in tutti gli aspetti della società e la produzione di dati sembra crescere in maniera inarrestabile.

- La raccolta di dati esprime il suo pieno potenziale se collegata all'uso dell'intelligenza artificiale e, a sua volta, ne alimenta la diffusione.
- “Big data” e “intelligenza artificiale” sono due concetti chiave che contrassegnano l'evoluzione del mondo digitale.
- I dati di per sé assumono un significato relativo, ma collegati tra loro, analizzati e rielaborati da algoritmi, possono fornire modelli predittivi, utilizzabili per anticipare le risposte degli individui, e quindi anche influenzarne il comportamento per finalità diverse (dal marketing elettorale fino alla pianificazione di attacchi informatici e fisici).
- L'intelligenza artificiale si sviluppa e si evolve attingendo alla disponibilità di una enorme quantità di dati, unita al miglioramento della tecnologia e della connettività, nonché alla capacità di imparare dai dati stessi per generare nuovi contenuti, secondo un processo di apprendimento automatico.

- Il fulcro del sistema è l'algoritmo, che oggi, per lo più, identifica un software costituito, a sua volta, dai codici sorgenti o linguaggio sorgente, che rappresentano le istruzioni, fornite dagli operatori umani per eseguire una certa funzione o risolvere un determinato problema.
- Tali istruzioni possono essere assimilate a scatole nelle quali vengono inseriti i dati necessari a ottenere i risultati voluti.
 - Oltre ad algoritmi semplici, che utilizzano determinate categorie di dati e operano secondo il modello impostato dal relativo ideatore – con esiti prevedibili o facilmente interpretabili, vi sono una serie di algoritmi complessi, che evolvono attraverso un processo di machine learning, secondo logiche che possono risultare incomprensibili, nonché algoritmi “senzienti”, in grado di superare il cosiddetto test di Turing, ovvero di equiparare il funzionamento della mente umana.

The Black Box Dilemma

- Il problema più critico si pone quando l'apprendimento delle macchine rende difficile, o impossibile, capire cosa stiano imparando e quali decisioni stiano adottando (Black Box Dilemma).





Il Pentagono studia, ad esempio, la possibilità di sistema di attacco e di difesa basati sull'IA



Ma le black box
sono sicure ?

E se iniziassero a
ragionare senza
alcun intervento
umano ?

- L'intreccio tra IA e big data può produrre impatti che si estendono ben al di là di un particolare settore, per influenzare le sorti di intere società.
 - È il caso, ormai emblematico, di Cambridge Analytica, la società che, utilizzando i dati degli utenti di Facebook, raccolti attraverso l'applicazione “mydigitalife”, è stata in grado di manipolare l'opinione pubblica in vista delle elezioni statunitensi, al punto che ci si domanda se elezioni libere ed eque siano ancora possibili.

- Una raccolta massiva di dati associati all'uso dell'intelligenza artificiale può incidere sensibilmente sui diritti e le libertà delle persone, non solo nell'ambito di processi consapevolmente mirati a influenzare il comportamento degli individui, dei consumatori, e perfino le decisioni di una collettività, ma anche per effetto di rischi intrinseci al funzionamento dell'IA.
- Simili rischi possono verificarsi, ad esempio, quando si affidano all'IA processi decisionali tipicamente umani, con esiti difficilmente prevedibili a priori, anche in dipendenza delle funzioni di addestramento o auto-addestramento della macchina, che possono condurre a risultati fortemente pregiudizievoli per interi gruppi di persone.

- L'uso dell'intelligenza artificiale investe ogni aspetto del vivere sociale, sotto il profilo economico, politico, sanitario, ambientale, e non si limita ai modelli aziendali o ai sistemi di gestione dell'amministrazione pubblica, ma ingenera una serie di trasformazioni nelle abituali interazioni con il mondo esterno, anche in termini di militari a partire dal contesto abitativo e urbano.
- Tali cambiamenti implicano la necessità di valutare adeguatamente i benefici connessi all'impiego di nuove tecnologie e i rischi per le persone fisiche e la società, in una logica di compatibilità che garantisca uno sviluppo affidabile e sicuro dell'intelligenza artificiale e la salvaguardia dei principi etici, come richiesto dal Consiglio e dal Parlamento europeo.

Una sfida anche per le situazioni di crisi in corso

- L'interesse per la tecnologia AI è in crescente espansione anche in ambito militare. Paesi come la Cina, gli Stati Uniti, la Russia ma anche più piccoli come la Turchia, la Corea e l'Iran stanno correndo per adottare tale tecnologia con l'obiettivo di ottenere o rafforzare un vantaggio militare sugli avversari.
- Indipendentemente dal fatto che si tratti di una vera corsa agli armamenti AI, di fatto gli investimenti militari in questo settore stanno crescendo.
- Il mercato militare dell'AI potrebbe raggiungere i 12 miliardi di dollari nel 2025 con un tasso di crescita annuo del 13% e dove si prevede che il segmento dell'apprendimento automatico guiderà il mercato fino al 2025.

Nei conflitti armati

- Gli investimenti crescenti nell'integrazione della tecnologia AI nei sistemi autonomi e armi autonome ha favorito la crescita del mercato dell'AI nel settore militare, suscitando grandi aspettative sul breve termine.
- Mentre la ricerca sul deep learning, il ramo più avanzato dell'AI, è spesso collaborativa, le potenzialità attribuite all'AI in campo militare hanno invece intensificato la concorrenza tra le grandi potenze.
- I leader cinesi, russi, iraniani e statunitensi, in particolare, non solo vedono l'AI come una tecnologia strategica per la competitività nel futuro ma prevedono che eserciterà un impatto così forte da poter sconvolgere la natura stessa della guerra (principi), delle Forze militari in combattimento e potrebbe in un modo o nell'altro perfino cambiare l'equilibrio tra grandi potenze.

Sipa USA via AP



Nei conflitti in corso in Medio Oriente e in Europa Centrale

- La guerra russa contro l'Ucraina sta diventando anche un esteso campo di sperimentazione relativo alla promozione dell'uso dell'intelligenza artificiale (IA) nel settore militare.
- In particolare, si tratta di sistemi d'arma automatizzati, come diversi tipi di droni che stanno sempre più condizionando gli eventi sui campi di battaglia.
- E in Medio Oriente la sperimentazione ha già una forma definita.

AI, Informazione e Media

- I conflitti in Ucraina e a Gaza, insieme ai focolai di tensione che esistono da tempo in tutto il mondo, sfoceranno quasi certamente in un'esacerbazione dei contrasti a causa di misinformazione e disinformazione.
 - Non sarebbe la prima volta.
- Nel maggio 2023, un'immagine trasmessa dal canale informativo russo RT.com ha mostrato un'esplosione totalmente fasulla che si sarebbe prodotta vicino al Pentagono, a Washington DC.
- I social media hanno dato ampia diffusione a quest'immagine falsa, a cui il mercato azionario ha reagito per alcuni minuti.
 - Nel novembre 2023, su TikTok è stato pubblicato un video falso che mostrava le strade di Parigi traboccanti di rifiuti; per quanto si potesse dimostrare che si trattava di un montaggio, ha comunque generato interesse e commenti.



Fake



- Quest'anno (2024) sono previste circa sessanta elezioni generali, tra cui: UE, Bangladesh, India, Iran, Pakistan, Russia e Stati Uniti.
 - C'è ampiamente la possibilità di nuocere.
 - Il partito repubblicano USA ha pubblicato un annuncio contro l'attuale Presidente che illustra la situazione in caso di rielezione di Joe Biden: sciame di migranti che attraversano gli Stati Uniti, soldati che pattugliano le strade vuote delle città e un'imminente guerra mondiale. All'inizio c'è un'avvertenza quasi invisibile secondo cui l'annuncio è "costruito interamente con immagini elaborate con l'intelligenza artificiale".
 - Ciò nonostante, quest'annuncio solleva un interrogativo: se è notoriamente falso, perché pubblicarlo? A meno che non si abbia la sensazione che questo tipo di immagini di grande impatto possano influenzare le intenzioni di voto dei cittadini.

AI e Deep Fakes

- Che si tratti di fenomeni come i *deep fakes*, la disinformazione, l'antropomorfizzazione delle tecnologie di intelligenza artificiale, o la circolazione di teorie complottiste sui social media, la questione è destinata a prendere sempre più spazio nei dibattiti pubblici.
 - Inganni intelligenti?



- I deepfake sono stati definiti come video sintetici che assomigliano molto a video reali, video iper-realistici nei quali il volto di una persona è stato analizzato da un algoritmo di deep learning e successivamente sovrapposto sul volto di un attore in un video, video che sovrappongono il volto di una persona sul corpo di un'altra , resi possibili da algoritmi facili da usare”, video manipolati, o altre rappresentazioni digitali prodotte da una sofisticata intelligenza artificiale, che produce suoni e immagini finzionali che appaiono come reali, un tipo di media sintetici, ovvero media (che includono immagini, audio e video) che sono o manipolati o completamente generati attraverso l'intelligenza artificiale, “video falsificati attraverso l'intelligenza artificiale che presentano nuove strade multi-sensoriali per manipolare la percezione della realtà.



I rischi e le incertezze sono infinite, quasi banali (e indefinibili)

- Il contributo dei sociologi, in questo contesto, è quello di essere degli «investigatori dell'ordinario».
 - Per studiare i fenomeni più eccezionali e perfino spaventosi è necessario addestrarsi a osservare ciò che sta sotto i nostri occhi ma che spesso viene liquidato come (ancora) irrilevante.
- Accogliere quindi l'insegnamento degli «investigatori dell'ordinario» può aiutare a sviluppare i mezzi analitici e anche pratici per comprendere e intervenire nei processi sociali e tecnologici che caratterizzeranno gli anni a venire.
 - Questo è e sarà il nostro contributo.

Intelligenze artificiali e Media

- Riconoscere che l'inganno è prima di tutto “banale”, che è un qualcosa di integrale al rapporto con i media, non significa rinunciare a esaminare gli effetti anche eccezionali che fenomeni come la disinformazione o la propaganda ingannevole possono avere sul dibattito pubblico e sulla sfera politica, sociale e culturale.
 - Esiste, infatti, una continuità di fondo tra forme di inganno che sono normalizzate e funzionali alle nostre interazioni quotidiane con i media e forme di inganno che non sono altrettanto inoffensive, ma che si sviluppano sulla base delle stesse dinamiche: così, ad esempio, l'impatto dei deep fakes va ricondotto non solo alle tecnologie di intelligenza artificiale ma anche e soprattutto all'impressione di realtà costruita dall'audiovisivo fin nelle sue applicazioni più comuni.
- Per questa ragione, lo studio dell'ordinario rimane un'arma efficace che lo studioso della cultura ha disposizione per comprendere e intervenire sulla realtà contemporanea.

Sono un lettore

- e vedo che l'intelligenza artificiale si piazza, come rilevanza rivoluzionaria riguardo alla vicenda umana, tra la scoperta del fuoco e l'invenzione dell'elettricità; qualcosa che può generare in un tempo brevissimo e in prospettiva di medio termine, comunque ravvicinata per gli standard di diffusione e incidenza delle tecnologie generaliste che abbiamo conosciuto in questi decenni, incrementi di produttività fantastici, a due cifre percentuali, dunque risultati decisamente superiori ai mezzi impiegati, lavoro capitali strumenti di produzione e tecnologie tradizionali.

Un salto: dal fuoco all'elettricità

- Ma il motore a scoppio, le applicazioni dell'elettricità, i computer erano tecnologie generaliste;
- l'IA ha il tratto specifico di applicarsi alla struttura e alla fonte dell'intelligenza umana.
- Ma il nostro modo di comunicare e, dunque, di esistere è spesso intraducibile, irriducibile.
- L'ia non è un altro dispositivo che deve essere regolamentato.

Per riassumere

- Queste probabilmente sono le quattro principali opportunità che l'intelligenza artificiale offre alla società:
- 1) La realizzazione autonoma di noi stessi, ovvero chi possiamo diventare;
- 2) L'agire umano, ovvero cosa possiamo fare;
- 3) Le capacità individuali e sociali, ovvero cosa possiamo conseguire;
- 4) La coesione sociale, ovvero come possiamo interagire gli uni con gli altri e con il mondo.

- L'Intelligenza Artificiale può essere utilizzata per:
 - favorire la natura umana e le sue potenzialità, generando in tal modo opportunità;
- sottoutilizzata, creando in tal modo costi e poche opportunità;
- sovrautilizzata o utilizzata male, creando in tal modo rischi.

- Le parole acute di Karl Kraus di un secolo fa appaiono ancora attuali:
- «La cultura è esausta [...] un giorno si vedrà l'umanità che si è sacrificata alle grandi opere che essa stessa ha creato per facilitarsi la vita. Siamo stati abbastanza complicati da costruire la macchina e siamo troppo primitivi per farci servire da essa».