Centro Studi di Geopolitica e Strategia Marittima
Roma, Lungotevere delle Armi, 24

Geopolitica-mente
Riflessioni per comprendere il mondo
n. 26 - Settembre 2023

Artificial Intelligence e geopolitica

Introduzione

L'*Artificial Intelligence*, Intelligenza Artificiale (AI/IA), è una tecnologia in uso da più di quindici anni ma che recentemente ha catturato l'attenzione dei ricercatori, degli innovatori e del pubblico in generale. L'AI si riferisce allo sviluppo di sistemi informatici capaci di svolgere compiti che tipicamente richiedano competenze o discernimento superiori rispetto all'ordinaria applicazione di semplici regole ("se A allora B"). Questi compiti comprendono un ampio spettro di elementi: dal riconoscimento di pattern in dati o immagini, alla classificazione in categorie, e molto altro ancora. Il Machine Learning (ML) è la branca dell'AI che si concentra su algoritmi che migliorano le proprie performance con il numero delle osservazioni, "imparando" quindi dai dati. Attraverso algoritmi e modelli statistici, il ML consente ai sistemi di riconoscere pattern complessi e fare previsioni (*prediction*) sui dati futuri, ammesso che i pattern riconosciuti persistano, per esempio in materia di andamenti dei prezzi di borsa, traffico di utenti su siti di compravendita di biglietti aerei).

La *Generative AI,* di cui fanno parte i *Large Language Models* (LLM), resi noti dall'avvento di ChatGPT e di simili applicazioni, sono un'altra branca dell'IA e stanno guadagnando sempre maggiore importanza. I LLM sono creati con l'intento di comprendere e generare testo in modo analogo a come lo farebbe un umano, rendendo questi algoritmi preziosi per funzioni come l'elaborazione del linguaggio naturale, la generazione di contenuti e persino la conversazione. Altri tipi di AI Generativa (non LLM) sono in grado di comporre musica o produrre immagini nello stile di autori specifici, dopo averne analizzato le opere.

Dietro lo sviluppo di questi sofisticati algoritmi c'è Big Tech, ossia il gruppo di aziende tecnologiche più innovative al mondo, americane, ma non solo. Ovviamente parliamo di Google e Facebook, ma anche di Tesla, OpenAI, SpaceX, Amazon, Alibaba, Spotify, Microsoft e tante altre, magari meno note al grande pubblico. Alcune di queste aziende sviluppano algoritmi per potenziare la propria offerta: ottimizzare le raccomandazioni di film o musica, offrire la pagina che meglio risponda alle ricerche dell'utente, e così via. Altre invece sviluppano i propri modelli di AI come prodotti finali: ChatGPT, Bard e LLaMa (algoritmi LLM) non sono altro che interfacce grafiche per gli algoritmi stessi. Il prodotto proposto è l'uso diretto dell'AI.

Foto di Pavel Danilyuk. Pexels

L'AI è uno strumento completamente trasversale, e può essere applicata virtualmente in qualsiasi ambito. In medicina, a partire da radiografie o risonanze, consente di ottenere diagnosi più accurate di quelle dei medici specializzati. In finanza, gli *hedge fund* la usano per cercare di anticipare i mercati (Renaissance Technologies - l'Hedge Fund di maggiore successo fra quelli puramente *algoritmici* - è, con successo, tra i maggiori utilizzatori e creatori di algoritmi), mentre le

banche vi ricorrono per monitorare operazioni potenzialmente fraudolente. Nelle industrie si usa l'AI per rendere i processi produttivi più efficienti.

Elementi Tecnici

Senza voler essere pedanti, vale la pena di porre l'accento su un aspetto spesso trascurato. Il termine *Intelligence* in AI viene tradotto con "intelligenza". Tuttavia, una traduzione migliore potrebbe essere "Informazione". Un modo più appropriato per riferirsi alla "Artificial Intelligence" dovrebbe quindi essere "Informazione Sintetica"; i computer, infatti, non sono (ancora) né intelligenti né senzienti. Gli algoritmi AI sono creati con lo scopo di analizzare informazioni e successivamente, dopo esser stati opportunamente *addestrati* (configurati), crearne o trarne altre in modo sintetico. Questi algoritmi, quindi, deducono informazioni dai dati, ma non ragionano.

Occorre inoltre non confondere sistemi AI con sistemi autonomi. Un aereo di linea è perfettamente in grado di atterrare autonomamente. Tuttavia, non è equipaggiato con sistemi AI. Il computer di bordo dell'aereo ne conosce posizione, direzione e velocità, sa come modificarle, e ha anche in memoria i dati della pista. Per atterrare autonomamente, il computer usa gli algoritmi deterministici progettati dagli ingegneri e memorizzati al suo interno.

In estrema semplificazione, gli algoritmi di AI usano dati in input forniti (serie storiche, tabelle, immagini), li elaborano, e forniscono un output, ossia la risposta, in base ai dati forniti.

La risposta dell'algoritmo è determinata dal suo *addestramento*. Gli algoritmi di AI e ML sono caratterizzati da una complessità senza precedenti. Per avere un'idea, GPT-4 è basato su un trilione di parametri: un numero smisurato. Questi vanno calibrati accuratamente per ottenere un corretto funzionamento dell'algoritmo. Il processo di calibrazione è responsabile della produzione dell'algoritmo finale. Gli algoritmi finali sono di fatto impossibili da comprendere per un umano; il nostro cervello, infatti, non è in grado di far fronte alla loro complessità. Esistono quindi algoritmi "istruttori" che addestrano algoritmi "candidati" fino al raggiungimento della soglia di soddisfazione.

È quindi molto importante comprendere quali siano gli obiettivi degli algoritmi. Tipicamente questi algoritmi sono preposti ai seguenti scopi:

- Categorizzare: in base ad un set di dati noto, con categorie ben definite, l'algoritmo associa un dato a lui ignoto a una categoria (riconoscere tumori da immagini, distinguere segnaletica stradale, eccetera);
- Predire: analizzando dati passati, svolgere predizioni su dati futuri (provare a determinare quali azioni avranno un costo maggiore in futuro);
- Emulare: riconoscere i pattern intrinseci di un determinato set di dati e produrre nuovi dati sintetici che rispettino lo stesso pattern (comporre musica, testi o immagini nello stile di autori noti).

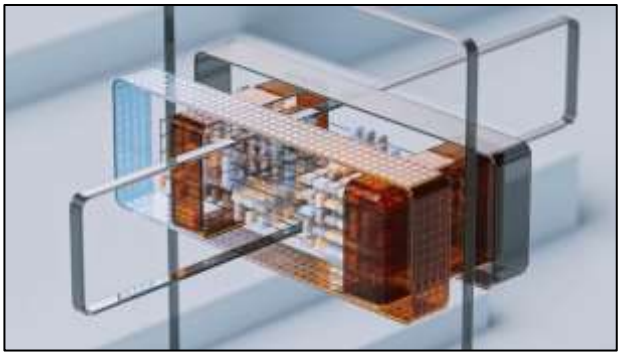

Foto di Google Deepmind. Pexels

Il punto cruciale, quello più temuto, è l'attuazione automatica degli output di questi algoritmi senza controllo o supervisione umana. Un'automobile come la Tesla è in grado di riconoscere la segnaletica stradale con i suoi algoritmi di *computer vision*, e le relative raccomandazioni (frenare, accelerare, azionare il volante) vengono eseguite dalla funzione di pilota automatico in modo *autonomo*. Gli algoritmi inseriti in contesti di autonomia totale diventano allora problematici. Per quanto siano stati opportunamente addestrati, infatti, le raccomandazioni che verrebbero attuate automaticamente, non sono sempre chiare agli umani. Inoltre, un algoritmo potrebbe essere configurato per raggiungere un obiettivo senza che effetti collaterali imprevisti o imprevedibili siano parte integrante dell'addestramento. Quindi, in caso di input incompleti o insufficienti, l'AI potrebbe generare risposte inattese o incomprensibili.

Geopolitica

I riflessi geopolitici dello sviluppo dell'AI si articolano su tre pilastri fondamentali: lo sviluppo degli algoritmi,

la disponibilità di processori adeguati a eseguirli e le dinamiche di finanziamento necessarie allo sviluppo degli uni e degli altri. Il settore finanziario che investe in queste innovazioni di punta è principalmente il *Venture Capital* (VC) che opera con logiche standardizzate basate sul flusso internazionale di capitali. Il punto di caduta di quanto precede è rappresentato dal conflitto tra una piena autonomia strategica e l'apparente convenienza di delocalizzare produzioni.

Unicità nella Supremazia Tecnologica

Le grandi potenze si sono sempre adoperate per essere tecnologicamente all'avanguardia, sia per finalità economiche, sia per poter disporre di vantaggi in caso di conflitto. Le grandi innovazioni sono state talvolta guidate, assorbite o controllate dallo Stato in quanto principale, se non unico, fruitore delle tecnologie sviluppate. In linea di massima le aziende commerciali non usano queste tecnologie all'interno dei loro prodotti/servizi se non in alcuni casi molto specifici (radar meteorologici e GPS sugli aerei di linea, per esempio), e comunque con limitazioni tecniche.

Rischi e Benefici

I rischi collegati a queste tecnologie derivano anche dai molteplici domini di applicazione. È abbastanza immediato pensare a ripercussioni militari (droni autonomi e armi intelligenti). Meno ovvia, ma non meno impattante è la possibilità di analizzare enormi quantità di dati. Tenendo sempre a mente che questi algoritmi possono sia "comprendere" che generare dati, è facile immaginare, e già accade, come si possano generare immagini, video o testi che seppur non "veri" siano "verosimili". La disinformazione sistematica è già ora usata sia per disseminare fake news che per creare intere campagne di disinformazione in modo automatico. Oltre alle possibili ingerenze in paesi terzi in tema politico, queste tecnologie potrebbero essere usate anche internamente per la sorveglianza di massa.

Lo Stato non detta legge

Per quanto riguarda l'AI il panorama è estremamente diverso rispetto al passato, o quanto meno rispetto ad altre tecnologie sensibili. Potendo applicare tecniche molto simili su domini completamente diversi, le aziende che sviluppano gli algoritmi non hanno necessariamente lo Stato come principale interlocutore; anzi, questo, con i suoi vincoli legislativi e amministrativi, è talvolta ritenuto un interlocutore scomodo, in grado addirittura di generare cattiva pubblicità.

I governi, inoltre, hanno molte difficoltà a tenere il passo con gli avanzamenti tecnologici. A parte gli Stati Uniti (che comunque faticano a ridurre il divario con i grandi attori privati), gli apparati statali non dispongono delle competenze per comprendere appieno queste tecnologie né tantomeno per assimilarle in tempi rapidi. Tutt'al più sono in grado di acquistare prodotti o servizi (quasi) come un qualsiasi altro cliente. Alcune aziende nate al di fuori delle sfere puramente statali (come Lockheed Martin, Leonardo, Thales, BAE) sono ben contente di lavorare con enti di natura governativa: Palantir, SpaceX e Anduril ne sono ottimi esempi. Molte altre invece lo sono meno, a livello della dirigenza o del personale. Quando Google negozia contratti con governi per scopi non puramente commerciali, è estremamente criticata dall'interno.

Foto di Google Deepmind. Pexels

La Strategia degli Stati Uniti

Gli Stati Uniti hanno un approccio *totale*. Il governo cerca di rimanere al passo incorporando rapidamente tecnologie ovunque possano per scopi militari e non. Inoltre, sono in prima linea sia per creare le migliori

condizioni affinché l'evoluzione tecnologica avvenga entro i propri confini, sia per impedirne quanto più possibile l'accesso ai propri avversari.

Gli USA stanno mettendo in sicurezza la risorsa chiave senza la quale è impossibile usare gli algoritmi: i processori. A molti piace parlare di *picks and shovels* (picconi e pale) per alludere all'infrastruttura. La difesa di Taiwan da parte degli Stati Uniti è legata intrinsecamente alla presenza sul territorio dell'azienda Taiwan Semiconductor Manufacturing Company (TSMC) e l'ultima visita della presidente della Camera Nancy Pelosi nelle sedi di TSMC lo testimonia.

Altro importante tassello della strategia USA, è quello di controllare quanto più possibile gli investimenti legati all'AI. Questo settore, così come quello più generale dell'innovazione tecnologica, è alimentato finanziariamente soprattutto dall'industria di *Venture Capital* (VC). I fondi VC raccolgono capitali e li investono nelle startup innovative, permettendone la nascita e accelerandone la crescita. Gli apparati statali USA non escludono comunque il diretto finanziamento dell'ecosistema startup, sia a livello nazionale che internazionale. Uno dei più importanti fondi VC del settore è In-Q-Tel, che è direttamente finanziato dalla CIA; un altro, più recente e ancora per ora meno importante, è il Nato Innovation Fund (NIF), finanziato insieme al resto dell'Alleanza.

A chiusura del cerchio, il presidente Joe Biden ha recentemente firmato un ordine esecutivo che vieta di investire in *tecnologie sensibili* in paesi *attenzionati*, e recentemente è stato approvato il Chips act per facilitare un re-shoring delle tecnologie relative ai processori con l'obiettivo di creare lavoro e contrastare l'avversario Cinese.

Europa

A livello di Unione Europea si è molto concentrati sulla regolamentazione per tutelare i cittadini e la privacy, e sulla *AI Explainability*: incorporare nell'algoritmo stesso un "manuale di istruzioni" che gli permetterebbe di auto-spiegarsi, garantendone trasparenza e comprensione da parte degli utenti. Inoltre, l'Europa ha vietato l'uso dell'intelligenza artificiale per la sorveglianza della popolazione ed è in prima linea per la tutela della privacy sul modello *General Data Protection Regulation* (GDPR).

Tuttavia, l'Europa non ha una postura strategica unitaria. Il Regno Unito ha delineato una sua strategia nazionale nel 2021 che si concentra maggiormente sui benefici economico-finanziari delle tecnologie AI. La Francia, già nel 2018, incaricò il celebre matematico vincitore della medaglia Fields, Cédric Villani, di delineare la strategia nazionale. Da allora la Francia ha sviluppato considerevoli competenze commerciali e di ricerca (pubblica e privata), attirando attori internazionali e creando un florido ecosistema indigeno. Anche l'Italia ha una sua strategia nazionale in materia; gli obiettivi sono importanti e necessari, ma decisamente poco ambiziosi; si concentrano sul sostegno alla ricerca (che purtroppo nel nostro paese è generalmente sotto finanziata nel pubblico e insufficiente, se non inesistente, nel privato), sulla promozione dell'ecosistema startup autoctono (che purtroppo stenta a decollare e siamo, secondo tutte le statistiche, il fanalino di coda in Europa Occidentale e non solo), e infine sull'integrazione nella pubblica amministrazione dei dati in lingua italiana (l'intelligenza artificiale "pensa" prevalentemente in inglese; l'uso di altre lingue ne limitano la qualità).

Al di là della "Cortina Digitale"

In Cina, dove lo Stato è onnipresente, il governo usa le tecnologie AI ad ampio spettro, come per la sorveglianza massiccia della popolazione con l' approccio one person, one file, ed è molto attivo nell'incorporare algoritmi AI negli armamenti; un approccio antipodale rispetto a quello Europeo. Anche la Russia è molto attiva sul fronte AI, incorporandola sia in droni autonomi, sia nelle azioni propagandistiche o di disturbo. Questi aspetti delineano alcune caratteristiche della strategia globale di queste potenze: il controllo totale della società, benché motivata da meriti propri, permette alla Cina anche di meglio concentrarsi sulla proiezione internazionale dei propri interessi; con il ricorso all'AI la Russia tenta invece di compensare la propria inferiorità militare rispetto al comparto atlantico.

Conclusione

L'argomento dell'Intelligenza Artificiale è decisamente troppo complesso per essere esaurito in un singolo articolo, e la disamina delle potenziali ripercussioni

tecnologiche ed economiche positive o negative richiederebbe riflessioni più approfondite.

Qui si è cercato di evidenziare l'approccio che le principali potenze mondiali nutrono nei confronti dell'intelligenza artificiale, delineandone gli aspetti in grado di suscitare competizione e attriti internazionali: l'AI è già, e sarà sempre più, un ulteriore tema di contrasto fra potenze. Algoritmi, processori e tecnologie collegate sono le chiavi che permettono di navigare in un mondo sempre più basato sul possesso di dati e sulla loro elaborazione. Quanti più dati posseggano, e quanto meglio li possano analizzare ed elaborare, tanto più potenti e influenti saranno governi, stati, e grandi gruppi privati.

A questo punto, sembrano emergere due prevalenti considerazioni. Da una parte assistiamo, e continueremo a farlo, ad una metaforica "corsa allo spazio" in cui i blocchi. (capitanati da USA e Cina, ma attenzione anche alla non allineata India) competono per la supremazia tecnologica, anche ben oltre l'intelligenza artificiale, a livello di sistema paese. Dall'altra sarà interessante capire come evolveranno le relazioni tra gli stati e Big Tech. Le multinazionali dietro lo sviluppo dell'AI non operano sotto un ombrello di interesse strategico, e sono attive negli Stati Uniti, in Europa e in Cina. In Cina il rapporto fra Stato e Azienda è sicuramente più stretto di come lo si intende in Occidente, ma la questione si pone in ambo i blocchi. È vero che le grandi aziende si adeguano per ora alle richieste dei paesi in cui operano; per altri versi, tuttavia, gli stati dovrebbero garantirsi competenze necessarie al mantenimento di un sufficiente controllo sulla rilevante tecnologia. Un possibile approccio potrebbe essere quello di agire direttamente e con proprie risorse nello sviluppo tecnologico, nell'ambito delle proprie finalità, limitando la propria dipendenza dal settore privato.

Giulio BOFFO