CAMERA DI COMMERCIO
VENEZIA GIULIA
TRIESTE GORIZIA

LA GEOPOLITICA DELL'ALGORITMO

Position Paper

Maggio 2024

Rapporto realizzato dalla Camera di Commercio, Industria, Artigianato e Agricoltura Venezia Giulia in collaborazione con The European House - Ambrosetti per la terza edizione del

festival del CAMBIAMENTO®

Rapporto realizzato dalla Camera di Commercio, Industria, Artigianato e Agricoltura Venezia Giulia in collaborazione con The European House - Ambrosetti.

Indice

Prefazione

La Venezia Giulia, in virtù della propria storia e posizione geografica al centro dell'Europa, si pone quale snodo strategico dei principali transiti commerciali via terra e mare e polo di innovazione tecnologica, con una naturale vocazione ad intercettare e anticipare i grandi cambiamenti nella società e nell'economia: è anche per questo motivo che, nel 2022, la Camera di commercio Venezia Giulia ha lanciato il "Festival del Cambiamento", un evento che intende connotare l'immagine della Venezia Giulia su temi all'avanguardia, in accordo con le sue caratteristiche di territorio "di frontiera" e pionieristico sul fronte della scienza e dell'innovazione, e di attivare visibilità e nuove relazioni per attività produttive, commerciali e di ricerca.

La manifestazione, che vede il coinvolgimento e il sostegno dei più importanti enti pubblici e di alcuni dei principali operatori privati del territorio nazionale, regionale e giuliano, vuole affermarsi come l'evento di riferimento in Italia sui grandi temi legati al cambiamento della società e dell'economia, coinvolgendo in due giorni di dibattiti esperti di livello internazionale su strategie e scenari di sviluppo per intercettare e anticipare i grandi cambiamenti in corso in Italia, ma con un respiro europeo e internazionale. Il Festival vuole anche massimizzare il coinvolgimento di imprese, istituzioni, università e società civile, per favorire l'elaborazione di proposte e idee innovative per orientare il futuro del nostro Paese ed affrontare con successo le nuove dinamiche della "grande onda" del cambiamento, in un'epoca storica di grande accelerazione e incertezza.

La terza edizione del Festival del Cambiamento si tiene il 6 e 7 maggio 2024 a Trieste e Gorizia, richiamando esperti, *policymaker* e *business leader* dall'Italia e da tutto il mondo e metterà al centro i temi di maggiore attualità nel dibattito pubblico sugli impatti per le imprese, la società e i territori.

A supporto del dibattito nelle sessioni del Festival del Cambiamento 2024, la Camera di commercio Venezia Giulia e The European House - Ambrosetti hanno elaborato questo *Position Paper* che esamina come le nuove tecnologie digitali stanno influenzando lo scenario geopolitico internazionale, al punto che oggi si parla sempre più di "geopolitica digitale". La crescente intersezione tra geopolitica e applicazione della tecnologia degli algoritmi è solo la punta dell'iceberg che vede, a monte, la corsa alla supremazia tecnologica tra le principali potenze globali.

Questi strumenti informatici, attraverso l'automazione e l'analisi dei dati, hanno il potere di guidare scelte che ogni giorno impattano sulle vite di milioni di persone. Nel complesso scenario della *data economy*, è quindi opportuno comprendere non solo quali sono i possibili rischi legati ad un potenziale abuso delle soluzioni di Intelligenza Artificiale (come minacce di *cybersecurity*, tutela della *privacy*, disinformazione e influenza dell'opinione pubblica), ma anche approfondire le opportunità per utilizzare l'IA come strumento a tutela della sicurezza nazionale, della democrazia e di rafforzamento della collaborazione tra Paesi.

Antonio Paoletti
Presidente
Camera di Commercio, Industria, Artigianato e Agricoltura Venezia Giulia

Executive Summary. I 10 punti più importanti dello Studio

1. La **geopolitica digitale** esplora il ruolo crescente delle tecnologie digitali – in particolare, gli **algoritmi** e l'**Intelligenza Artificiale** (IA) – nella conformazione delle relazioni e delle dinamiche geopolitiche globali. Nel confronto su scala globale non rilevano solo la posizione geografica, la dotazione di risorse naturali e finanziarie, o la situazione demografica, per definire il potere politico e le relazioni tra Stati, ma – con la rapida diffusione delle tecnologie digitali nelle attività della vita quotidiana e del *business* – si è via via consolidata una nuova dimensione in cui acquisiscono un valore differenziante la **connettività, i flussi e la gestione di informazioni e le tecnologie digitali avanzate**. Gli algoritmi e l'IA si affermano così come strumenti strategici, capaci di **processare enormi quantità di dati e influenzare decisioni economiche, sociali e politiche**, spaziando dalla sicurezza nazionale alla gestione delle infrastrutture critiche, fino alla possibilità di influenzare l'opinione pubblica e, in campo militare, guidare guerre nel *cyber*-spazio.
2. Gli studi sull'Intelligenza Artificiale (iniziati in fase embrionale negli anni Sessanta del XX secolo) ha conosciuto un'**accelerazione significativa negli ultimi 15 anni**, suddivisibile in 3 momenti distinti di sviluppo. La prima fase, tra il 2010 e 2016, è stata caratterizzata dall'innovazione nelle reti neurali, che ha permesso rapidi progressi nel **riconoscimento delle immagini** e nel ***deep learning***. La fase successiva, tra il 2016 e il 2022, ha visto l'introduzione di modelli di reti neurali ancora più avanzati, che hanno impostato nuovi *standard* nell'elaborazione del linguaggio naturale. La terza fase, iniziata nel 2022, è testimoniata dalla rapida maturazione dell'**Intelligenza Artificiale Generativa**, con l'introduzione e la diffusione di strumenti che hanno reso queste tecnologie accessibili a un vasto pubblico, innescando – allo stesso tempo – un dibattito globale sul loro impatto sulla società.
3. Questa rivoluzione digitale sta investendo molteplici settori e sta determinando numerose conseguenze. In prima linea vi è l'**industria della difesa**, che sta vivendo una trasformazione profonda segnata dall'importanza della ***cybersecurity*** e dell'**IA** come componenti chiave delle **strategie di sicurezza moderna**. Si osserva un incremento sostanziale degli investimenti in tecnologie digitali, che non solo aumentano la capacità di difesa tradizionale, ma anche migliorano la risposta alle nuove minacce informatiche e tecnologiche: ad esempio, la quota della spesa militare degli USA destinata ai sistemi intelligenti è quasi **triplicata** tra il 2022 e il 2023, a conferma dell'impegno crescente verso l'adozione di tecnologie all'avanguardia per mantenere la superiorità strategica e operativa.
4. Si è intensificata la **competizione tra le potenze globali per il dominio tecnologico**, con particolare enfasi sulla **R&S sull'IA** e sull'accesso alle **materie prime critiche** per lo sviluppo tecnologico, riflettendo un *focus* strategico sull'innovazione e sul controllo delle tecnologie chiave. Ad esempio, al 2022 la Cina guida la **classifica globale dei brevetti sull'IA** (61,1% del totale, seguita dagli **USA** con il **20,9%**), così come gode del maggior **controllo degli approvvigionamenti di materie prime critiche**, con una *leadership* di mercato su **11 materie prime critiche** sulle 34 censite dal *Critical Raw Materials Act* dell'Unione Europea ed è il principale fornitore europeo per il **56% delle materie prime critiche importate nell'UE**.
5. L'**Intelligenza Artificiale Generativa**, essendo una tecnologia ***general purpose***, ha il potenziale di trasformare profondamente svariati settori della società, sollevando sfide etiche e sociali rilevanti, anche sul fronte geopolitico. È possibile identificare **4 principali ambiti** in cui l'uso degli strumenti di IA può comportare **effetti sia positivi che negativi**, a seconda di

come questa tecnologia sia utilizzata: ***cybersecurity*; tutela dei dati e *privacy*; influenza dell'informazione e dell'opinione pubblica; diplomazia digitale**.

6. La ***cybersecurity***, sempre più integrata con l'IA, è fondamentale nel proteggere le infrastrutture critiche e migliorare l'efficienza della sicurezza informatica da **attacchi *cyber***, più che **triplicati dal 2014 ad oggi**. Riflettendo il riconoscimento collettivo dell'importanza dell'IA nella **prevenzione**, **rilevazione** e **risposta** agli attacchi informatici, si stima che **il mercato globale della *cybersecurity AI-based* crescerà del 28% entro il 2030**. Tuttavia, lo sviluppo nel campo dell'intelligenza artificiale non è privo di **conseguenze negative**: queste tecnologie possono essere sfruttate per effettuare **attacchi informatici più sofisticati e frequenti**. Infatti, si registra un incremento annuale degli attacchi del 70% in Italia e del 14% a livello mondiale.

7. A livello geopolitico, i **dati** conferiscono potere. Governi che possiedono o controllano grandi quantità di dati possono **influenzare la politica interna e internazionale**. La gestione dei dati e la raccolta di informazioni da un lato presenta grandi opportunità, ma dall'altro solleva interrogativi su sicurezza e uso appropriato di queste informazioni, con potenziali rischi di **violazioni della *privacy* e del consenso**. Normative, come il **GDPR** europeo, mirano a mitigare questi rischi attraverso *standard* di protezione rigorosi e garantendo ai cittadini un controllo maggiore sui propri dati, ma le differenze normative tra i Paesi creano un contesto complesso e poco trasparente per imprese e multinazionali.

8. L'**influenza dell'opinione pubblica** tramite tecnologie digitali e IA offre opportunità e sfide. La capacità degli algoritmi di personalizzare i contenuti che riceviamo ogni giorno è diventata uno strumento potente, migliorando l'esperienza-utente e favorendo l'**educazione** e la **mobilitazione** su temi importanti. Tale personalizzazione porta con sé anche notevoli rischi, soprattutto se utilizzata per diffondere disinformazione su larga scala, mirando a specifici gruppi demografici attraverso il ***targeting*** con messaggi che possono essere distorti o falsi, ma estremamente persuasivi. La diffusione di ***fake news*** e i c.d. ***deepfake*** (aumentati del 3.000% nel 2023 grazie al perfezionamento e all'estesa accessibilità dell'IA Generativa), rende la disinformazione notevolmente efficace, minacciano la stabilità delle democrazie.

9. La **diplomazia digitale**, basata sull'impiego delle nuove tecnologie digitali, ha a disposizione strumenti che permettono a Stati e organizzazioni internazionali di comprendere e reagire alle dinamiche globali con un livello di velocità, dettaglio e previsione senza precedenti, grazie a ***Big Data Analytics* e analisi predittive, *sentiment analysis*, strumenti per sicurezza e difesa, analisi per l'elaborazione di strategie geopolitiche e comunicazione transculturale**.

10. Seppure vi siano approcci e visioni diverse nella gestione dell'IA nello scenario geopolitico, per garantire una **gestione sostenibile dell'Intelligenza Artificiale nelle relazioni internazionali**, avendo sempre al centro del processo decisionale l'individuo, occorre seguire **determinati principi**: A) Una **gestione etica** dell'IA nelle relazioni internazionali deve ruotare innanzitutto attorno alla **trasparenza**; ciò implica una chiara divulgazione delle **metodologie**, dei **criteri** e dei **dati utilizzati** dagli algoritmi, permettendo una comprensione e una verifica indipendente delle decisioni prese. B) Va perseguita una **garanzia di responsabilità, sicurezza e affidabilità delle decisioni *AI-oriented***. Infatti, nonostante i sistemi di Intelligenza Artificiale debbano operare in mondo affidabile e sicuro, in caso di *bias* o errori, i governi devono saper rispondere delle proprie azioni anche quando intraprese sulla base delle raccomandazioni dell'IA. C)Un utilizzo responsabile dell'Intelligenza Artificiale dovrebbe fondarsi su **equità** e **inclusività**, con l'obiettivo di un impegno continuo per la revisione e l'aggiustamento degli algoritmi, assicurando che operino senza fenomeni discriminatori. Occorre, in sintesi, favorire la convergenza tra la dimensione della "macchina" e quella dell'essere umano, senza fare prevalere la prima sulla seconda.

Capitolo 1.

L'avvento della geopolitica digitale

Cos'è la Geopolitica Digitale

Per approfondire la crescente interdipendenza tra geopolitica e tecnologia, è essenziale comprendere cosa si intende per "**geopolitica digitale**".

La geopolitica tradizionale si occupa dello studio delle influenze geografiche sul potere politico e delle relazioni tra Stati, considerando fattori strategici come la posizione geografica, la dotazione di risorse naturali e finanziarie, o la situazione demografica.

Con la rapida diffusione delle tecnologie digitali nelle attività della vita quotidiana e del *business*, anche la geopolitica ha via via abbracciato una nuova dimensione in cui la posizione fisica è meno rilevante rispetto alla **connettività**, ai **flussi e alla gestione di informazioni**, e alla **dotazione di tecnologie digitali avanzate**. In tale scenario, gli **algoritmi** – definibili come serie di istruzioni o regole programmabili per eseguire calcoli o altre operazioni sui dati – sono diventati uno strumento cruciale in questo nuovo campo. Nella geopolitica digitale, quindi, gli algoritmi non solo processano **enormi quantità di dati**, ma possono anche influenzare **decisioni economiche**, **sociali e politiche su scala globale**. Questo include l'automazione delle decisioni in ambiti centrali per ogni sistema territoriale, come la sicurezza nazionale, la finanza e la gestione delle infrastrutture critiche[1].

La rilevanza degli algoritmi nella geopolitica si manifesta attraverso il loro ruolo nel modellare il comportamento individuale e collettivo, la sorveglianza, la disinformazione, e la conduzione della guerra cibernetica, nonché nel loro impiego in attività di diplomazia e processi di negoziazione.

Allo stesso tempo, la capacità di controllare o influenzare l'architettura di questi sistemi algoritmici rappresenta **una forma di potere significativa**[2]. Nella pratica, ciò significa che la supremazia nel campo delle tecnologie avanzate – come l'**Intelligenza Artificiale** e il ***Machine Learning*** - può tradursi per uno Stato in un **vantaggio geopolitico** tangibile.

Pertanto, la geopolitica digitale si configura come lo studio su come gli Stati e gli attori non statali utilizzano la **tecnologia digitale per raggiungere obiettivi strategici**, definendo così una nuova forma di diplomazia e confronto sullo scacchiere internazionale. L'**accesso ai dati**, la **gestione delle infrastrutture di rete**, la **standardizzazione tecnologica** e la **protezione della *privacy*** diventano così questioni strategiche centrali e, soprattutto, leve di competizione nella lotta per la supremazia geopolitica su scala globale[3].

Lo sviluppo degli algoritmi dalle origini ad oggi

Con l'avvento della computazione moderna nel Ventesimo secolo i algoritmi hanno assunto un ruolo centrale nella tecnologia, consentendo l'automazione e il trattamento efficace di grandi quantità di dati. Con l'evoluzione dell'*hardware* informatico negli anni '40 e '50, gli algoritmi hanno iniziato a diventare sempre più sofisticati[4]. La loro importanza è cresciuta esponenzialmente con lo sviluppo di Internet e delle tecnologie digitali, permettendo applicazioni che vanno dalla ricerca

[1] Fonte: Brookings Institution, "*The geopolitics of AI and the rise of digital sovereignty*", 2022.

[2] Fonte: RAND, "*AI and Geopolitics*", 2023.

[3] Fonte: Goldman Sachs, "*The generative world order: AI, geopolitics and power*", 2023.

[4] Fonte: Encyclopedia Britannica, "*Algorithms and complexity*", 2023.

semplice di informazioni su motori di ricerca a complessi algoritmi di intelligenza artificiale che possono apprendere e adattarsi. Negli ultimi decenni, l'introduzione del *machine learning* e dell'intelligenza artificiale ha portato gli algoritmi a un nuovo livello. Queste tecnologie permettono ai sistemi di migliorare le loro prestazioni senza essere esplicitamente programmati, ma piuttosto attraverso l'apprendimento da grandi volumi di dati. Oggi, gli algoritmi non solo facilitano operazioni quotidiane in innumerevoli settori, ma aiutano anche a guidare decisioni complesse in ambiti che spaziano dalla medicina alla finanza, e ovviamente, alla geopolitica[5]. Questo rapido sviluppo testimonia la crescente complessità e pervasività degli algoritmi nel tessuto della società moderna, sottolineando il loro ruolo critico nell'era digitale[6].

L'Intelligenza Artificiale (IA) rappresenta il culmine dello sviluppo degli algoritmi, un campo tecnologico che si propone di emulare o superare alcune delle capacità cognitive umane.

Si può parlare di Intelligenza Artificiale quando una macchina ha sviluppato la capacità di:

- **comprensione** di informazioni complesse;
- **apprendimento** all'interno di un determinato ambiente;
- **astrazione** dalla realtà circostante;
- **ragionamento** per pianificare le azioni successive.

Dopo una prima fase sperimentale in cui sono stati elaborati i concetti più generali di intelligenza artificiale, infatti, i grandi temi di ricerca nel campo dell'IA si sono concentrati su tre diversi campi:

- la **rappresentazione della conoscenza**, che fa leva su quella branca della matematica che concentra le proprie attività nella definizione di linguaggi che consentano di formalizzare la conoscenza acquisita, ovvero di "tradurla" in modelli matematico-statistici – detti appunto modelli formali – tali da servire da base di calcolo per la macchina;
- l'**apprendimento automatico** (*machine learning*) che, come si argomenterà più avanti, consiste nella realizzazione di sistemi, basati su osservazioni o esempi, capaci di sintetizzare la nuova conoscenza (classificazioni, riformulazioni, ecc.);
- l'**elaborazione cognitiva** (*cognitive computing*), che interessa lo sviluppo di sistemi che imitano il funzionamento del cervello umano e che include sia lo sviluppo di *software* che di elementi di *hardware*.

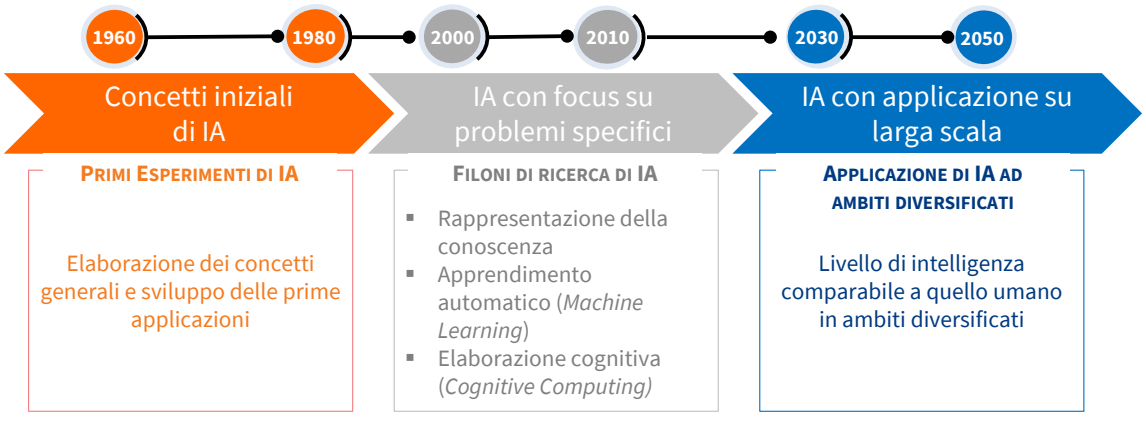


Figura 1. L'evoluzione dell'intelligenza artificiale nel corso del tempo e i principali filoni di ricerca attuali.
Fonte: elaborazione The European House - Ambrosetti su fonti varie, 2024.

[5] Fonte: Built In, "*The future of AI: how Artificial Intelligence will change the world*", 2024.

[6] Fonte: Data Science Central, "*How Machine Learning is changing the world*", 2020.

L'IA ha attraversato diverse fasi di sviluppo a partire dalla propria formulazione. Un interessante approccio è quello fornito dall'agenzia statunitense DARPA (*Defence Advanced Research Projects Agency*) che ha efficacemente sintetizzato in tre diverse fasi di sviluppo le caratteristiche dell'Intelligenza Artificiale. Ciascuna fase si caratterizza per una diversa combinazione delle varie componenti dell'IA, ovvero dei parametri con cui è possibile valutare l'intelligenza di una macchina (nello specifico: comprensione, apprendimento, astrazione e ragionamento).

Le fasi di sviluppo individuate secondo questa logica sono:

1. **Conoscenza artigianale** (*handcraft knowledge*).
2. **Apprendimento statistico** (*statistical learning*).
3. **Adattamento contestuale** (*contextual adaptation*).

Nella fase di **conoscenza artigianale**, gli ingegneri hanno lavorato per creare un insieme di regole che descrivesse la conoscenza in un ambito ben definito. I sistemi che rientrano in questa fase sono, pertanto, concepiti per ragionare su un problema molto preciso senza alcuna capacità di apprendere e con scarsa capacità di ragionare in situazioni di incertezza.

Esempi di questa "fase sperimentale" dell'IA possono essere considerati Deep Blue, che nel 1996 e 1997 sfidò il campione del mondo di scacchi Garry Kasparov, oppure le prime applicazioni di sistemi dedicati alla logistica e alla gestione delle merci che si limitavano a eseguire i comandi per cui erano stati programmati.

La successiva fase è denominata dal DARPA **apprendimento statistico** e si origina a partire dall'accresciuta disponibilità di dati e di capacità di calcolo che si sviluppa dagli anni Ottanta. Le soluzioni di intelligenza artificiale che rientrano in questa categoria sono, quindi, sviluppate sulla base di complessi modelli statistici creati a monte. Questi modelli non fissano regole da seguire, ma **forniscono alla macchina gli elementi di calcolo da applicare a un dominio particolare**. Sulla base del modello, esercitandosi su un *database* sempre più ampio, il sistema di IA impara a classificare e a fare previsioni su nuovi casi che gli sono presentati in seguito.

Rientra in questa fase di Intelligenza Artificiale la vittoria di IBM Watson contro i campioni del quiz televisivo statunitense "Jeopardy!" nel 2011, primo segnale di un'IA capace di sconfiggere un umano in un test non matematico con domande complesse sulla base dell'analisi di un'enorme quantità di dati e informazioni da processare. Un secondo esempio è offerto da AlphaGo (programma di intelligenza artificiale sviluppato da DeepMind, società di proprietà di Alphabet) che nel 2016 sfidò e sconfisse a Seoul il campione in carica del gioco di strategia cinese Go, Lee Sedol.

Un ruolo fondamentale in questa specifica fase di sviluppo dell'IA è quindi svolto quindi dalla disponibilità di una base dati sempre più estesa (*in primis*, i *Big Data*) per affinare e rendere più precisi i modelli statistici. Non a caso le applicazioni chiave dell'apprendimento statistico, in cui negli ultimi anni sono stati compiuti progressi enormi in termini di accuratezza, sono il **riconoscimento vocale e quello visivo**. La centralità dell'apprendimento basato su esempi pregressi in questa fase spiega lo **stretto legame tra la capacità di sviluppo di applicazioni di IA e il possesso dei dati.**

La futura fase evolutiva dell'IA e attualmente in forte fase di sviluppo, è quella del c.d. **adattamento contestuale**. In questo stadio, gli ingegneri potranno creare sistemi in grado di costruire modelli per categorie di fenomeni del mondo reale e non più basati solamente sull'ampia base dati sottostante. I sistemi, attraverso questi modelli, **apprendono e ragionano man mano che si presentano nuovi casi**, facendo riferimento al loro precedente schema comportamentale, applicando eventualmente questi schemi anche a **campi totalmente diversi da quelli di partenza**. Relativamente alle componenti dell'IA, i sistemi che si svilupperanno nella fase di adattamento contestuale saranno caratterizzati da **livelli medio-alti** di percezione, apprendimento, astrazione e ragionamento e potranno così **intrattenere una continua interazione con il mondo reale**.

Questa interazione consentirà di rendere concrete e applicate su larga scala applicazioni quali, ad esempio, il veicolo a guida autonoma.

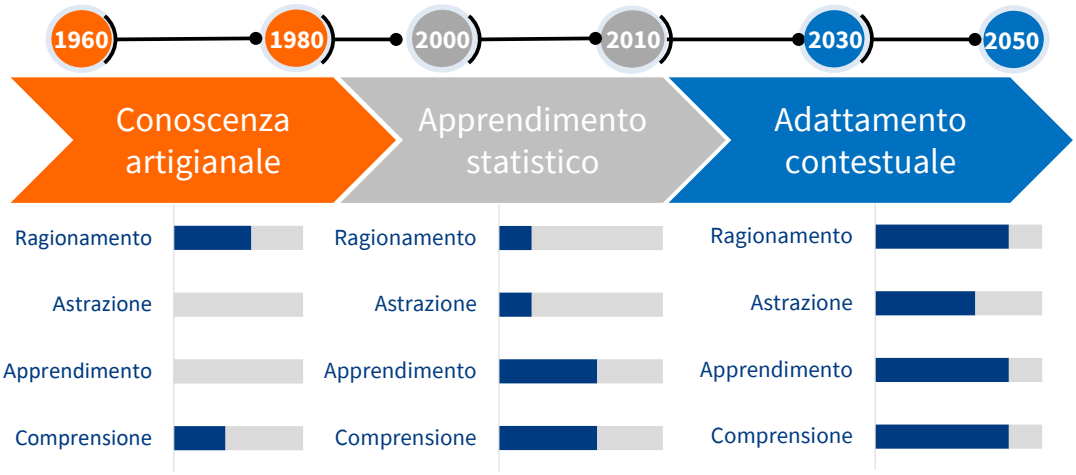


Figura 2. Le tre fasi dell'Intelligenza Artificiale e i livelli delle principali componenti per ognuna delle fasi stesse. *Fonte: rielaborazione The European House - Ambrosetti su dati DARPA, 2024.*

Se si analizzano i **passi in avanti compiuti negli ultimi 15 anni** (tra il 2010 e oggi, ovvero il periodo in cui l'IA ha conosciuto i maggiori miglioramenti in termini di potenziamento), si possono individuare **3 ulteriori fasi di sviluppo** dell'Intelligenza Artificiale[7]:

- **Dal 2010 al 2016**, le innovazioni nella progettazione delle reti neurali hanno trasformato l'IA. Grazie a questi nuovi sistemi, l'IA ha compiuto rapidi progressi nel **riconoscimento delle immagini** e nel ***deep learning***, specialmente attraverso programmi come AlexNet e il già citato AlphaGo.
- I progressi dell'IA **tra il 2016 e il 2022** hanno portato all'introduzione di modelli di reti neurali molto influenti, tra cui il Bidirectional Encoder Representations di Google e GPT di OpenAI. Questi modelli hanno stabilito nuovi *benchmark* nell'elaborazione del linguaggio naturale, aiutando a migliorare rapidamente la **comprensione del testo e la comprensione linguistica dell'Intelligenza Artificiale**.
- Infine, la terza era, **dal 2022 ai giorni nostri**, ha visto la maturazione in tempi sempre più rapidi dell'**Intelligenza Artificiale Generativa** e la diffusione pervasiva di strumenti di IA generativa per un ampio uso pubblico. In questo breve periodo di tempo, programmi come ChatGPT e DALL-E di OpenAI, Bard di Google o Claude di Anthropic, solo per citarne alcuni, sono diventati ampiamente disponibili presso il grande pubblico, stimolando il dibattito sugli impatti dell'IA sul lavoro.

Le prospettive dell'Intelligenza Artificiale Generativa

L'ultima versione di Intelligenza Artificiale di cui possiamo oggi usufruire è la versione **Generativa.** L'IA Generativa è un ambito di utilizzo dell'Intelligenza Artificiale che sfrutta algoritmi avanzati per **generare contenuto in vari formati**, come video, immagini, audio, testi, codici o altre tipologie di *output*.

Questa applicazione dell'AI Generativa **crea contenuti unici in diversi formati**, a differenza dell'intelligenza artificiale generale che abbraccia un insieme molto più ampio di tecniche e

[7] Si veda: American Enterprise Institute, "*The Age of Uncertainty—and Opportunity: Work in the Age of AI*", 2024.

applicazioni, focalizzandosi non solo sulla creazione, ma anche sull'analisi, la classificazione, e il processamento di dati[8].

Figura 3. I principali ambiti di applicazione e servizi dell'Intelligenza Artificiale Generativa. *Fonte: elaborazione The European House - Ambrosetti, 2024.*

Con l'IA Generativa si può creare **una nuova modalità di interazione tra l'uomo e le macchine, i dati e, più in generale, il mondo digitale**. In questo processo l'essere umano rappresenta l'elemento chiave sia come generatore di *input* che come beneficiario degli *output*, mentre l'IA Generativa riflette la capacità delle macchine di **emulare le funzioni cognitive umane nel processo creativo**, creando contenuto originale, attingendo sia da dati non strutturati, quali contenuti web, sia da dati strutturati, che comprendono *database* organizzati e informazioni sistematiche. La dualità dei dati riflette la versatilità e l'adattabilità dell'IA Generativa, essendo in grado di navigare e sintetizzare una vasta gamma di informazioni.

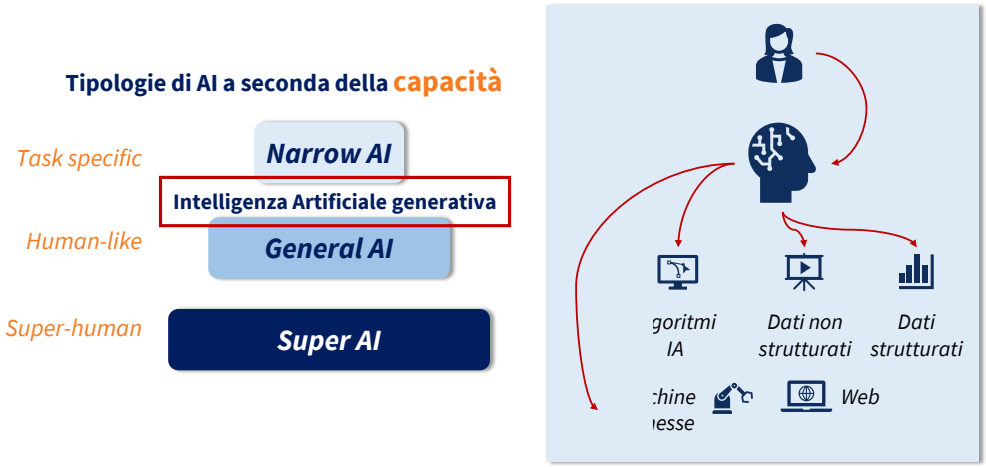


Figura 4. Il funzionamento dell'Intelligenza Artificiale Generativa nel suo ciclo di interazione con l'uomo e la sfera digitale. *Fonte: elaborazione The European House - Ambrosetti e Microsoft Italia, 2024.*

L'integrazione dell'Intelligenza Artificiale Generativa nel tessuto della geopolitica digitale costituisce un'**evoluzione significativa**. Infatti i risvolti di tale tecnologia nella geopolitica sono vasti e complessi[9]: ad esempio, in campo strategico, l'IA Generativa potrebbe essere utilizzata per sviluppare simulazioni geopolitiche avanzate, creando scenari ipotetici per aiutare i *decision-maker* a valutare incertezze future. Nel campo dell'informazione, potrebbe essere impiegata per generare notizie false realistiche o i c.d. *deepfake*, che potrebbero minare la stabilità politica o influenzare elezioni e altri processi democratici. Del resto, l'impatto dell'IA pone interrogativi etici e sociali significativi[10]: la gestione della *privacy* dei dati, il rischio di *bias* nei sistemi decisionali

[8] Per approfondimenti si veda lo Studio Strategico di The European House - Ambrosetti e Microsoft Italia "AI 4 Italy: impatti e prospettive dell'intelligenza artificiale generativa per l'Italia e il *Made in Italy*", 2023.

[9] Fonte: IEP - Internet Encyclopedia of Philosophy, "*Ethics of Artificial Intelligence*", 2024.

[10] Fonte: IBM, "*What is AI ethics?*", 2023.

automatizzati e le potenziali conseguenze sul mercato del lavoro sono solo alcuni degli aspetti che la società deve affrontare nell'era dell'IA[11].

Nel complesso, si prevede che su scala globale il mercato dell'Intelligenza Artificiale Generativa crescerà in modo sostenuto nel prossimo decennio, **passando dagli attuali 67 miliardi di Dollari** (ad un tasso di crescita media annua del 68% dal 2020 al 2023) **a più di 1,3 trilioni di Dollari entro il 2032**, per effetto della inarrestabile diffusione e adozione di strumenti di IA Generativa (come, ad esempio, ChatGPT di OpenAI).

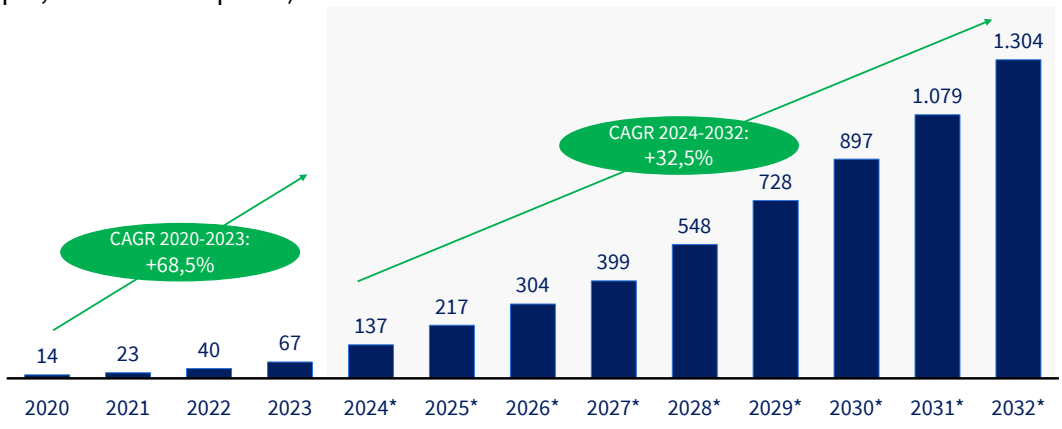


Figura 5. Valore del mercato dell'Intelligenza Artificiale Generativa nel mondo (fatturato in miliardi di Dollari), 2020 – 2032[e]. (*) Stima. *Fonte: elaborazione The European House - Ambrosetti su dati Bloomberg, 2024.*

Le prospettive di sviluppo sono confermate anche dagli **investimenti aziendali in Intelligenza Artificiale realizzati a livello globale negli ultimi 10 anni** (crescita media annua di **+29,2% tra il 2013 e il 2023**). In particolare, **il 2021 è stato l'anno *record* degli investimenti nel settore dell'IA** (337,4 milioni di Dollari), con incrementi in quasi tutte le categorie. La variazione nei volumi di investimento negli anni successivi potrebbe riflettere una stabilizzazione del mercato o la realizzazione di strategie di investimento a lungo termine avviate nell'anno di picco.

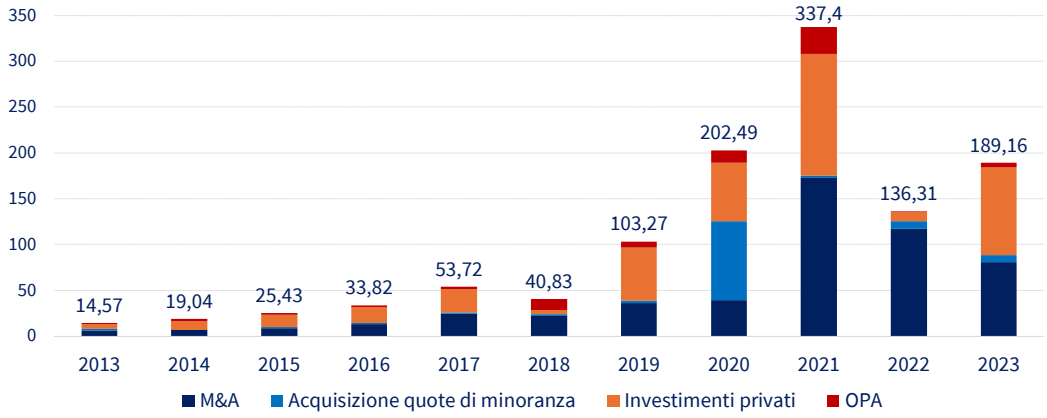


Figura 6. Investimenti aziendali globali in IA per attività di investimento (investimenti in milioni di Dollari), 2013-2023. *Fonte: elaborazione The European House - Ambrosetti su dati Quid e Stanford University, 2024.*

Coerentemente con l'andamento mondiale, non stupisce che nell'anno fiscale 2023 il solo Governo statunitense abbia stanziato **1,8 miliardi di Dollari per le spese di R&S sull'Intelligenza Artificiale**, con un *budget* richiesto per il 2024 in crescita del 4,5%. Dal 2018 ad oggi, negli USA i finanziamenti per la R&S sull'IA sono **più che triplicati**, ad un tasso medio annuo composto di crescita del 22,3%. Con riferimento ai finanziamenti per l'anno 2023, l'ammontare più alto è in capo alla National Science Foundation (NSF, con 418,4 milioni di Dollari), alla Defense Advanced

[11] Si veda: Brookings Institution, "*Artificial intelligence, geopolitics and information integrity*", 2020.

Research Projects (DARPA, con 400,5 milioni di Dollari) e al National Institutes of Health (NIH, con 288,2 milioni di Dollari), complessivamente pari al 62% del *budget* pubblico allocato negli USA per la ricerca sull'IA. Seguono le agenzie federali di Difesa, Energia ed Agricoltura, a conferma della trasversalità delle applicazioni dell'IA in più campi.

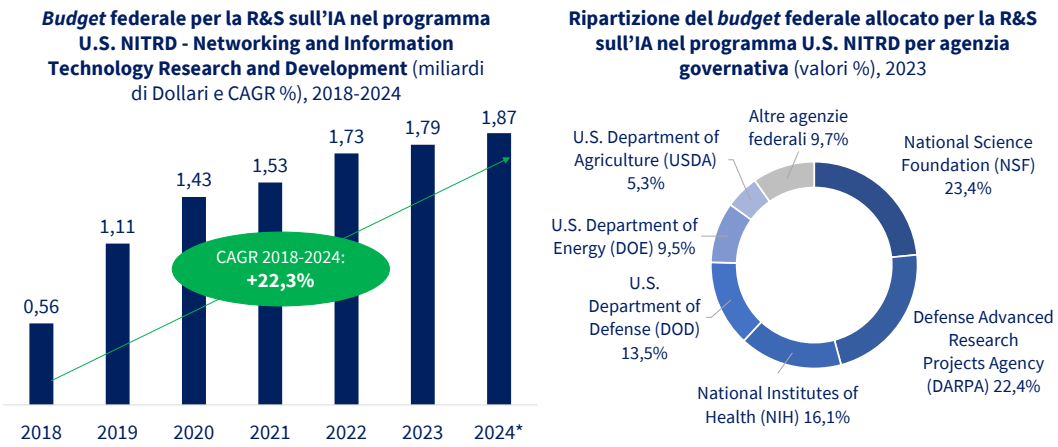


Figura 7. *Budget* federale per la R&S sull'IA nel programma U.S. NITRD - Networking and Information Technology Research and Development (miliardi di Dollari e CAGR %; grafico di sinistra), 2018-2024; ripartizione del *budget* federale allocato per la R&S sull'IA nel programma U.S. NITRD per agenzia governativa (valori %; grafico di destra), 2023. (*) *Budget* richiesto dalle agenzie. *Fonte: elaborazione The European House - Ambrosetti su dati National Science and Technology Council e Stanford University, 2024.*

Capitolo 2.
La "*data economy*" nello scenario della geopolitica e dell'industria della difesa

L'importanza degli algoritmi e il loro impatto pervasivo sulla società

Gli algoritmi sono diventati una componente fondamentale del tessuto socio-economico della società contemporanea, influenzando decisioni e processi in una vasta gamma di settori. Questi strumenti informatici, attraverso l'automazione e l'analisi dei dati, hanno la capacità di **guidare scelte che impattano ogni giorno sulla vita e sulle scelte di milioni di persone**[12]:

- In ambito economico, gli algoritmi determinano **dinamiche di mercato e decisioni aziendali** con una rapidità e una scala precedentemente inimmaginabili: ad esempio, le piattaforme di *trading* azionario utilizzano algoritmi per eseguire operazioni in frazioni di secondo, influenzando le fluttuazioni di mercato.
- Nel settore *retail*, algoritmi di analisi predittiva **modellano le scorte e le strategie di *pricing***, ottimizzando le vendite e la catena di distribuzione in tempo reale.
- Nel sistema delle reti sociali, gli algoritmi hanno un impatto profondo sulla distribuzione delle informazioni e sulla modulazione delle interazioni umane; i *social media* utilizzano algoritmi per personalizzare i *feed* degli utenti, determinando quali notizie e opinioni vengono più frequentemente esposte, **influenzando così la percezione pubblica e il dibattito culturale**, con l'effetto di determinare potenziali ripercussioni su elezioni, movimenti sociali e questioni di grande rilevanza pubblica.
- Politici e decisori pubblici si affidano sempre più a sistemi basati su algoritmi per sviluppare politiche pubbliche. L'analisi dei *Big Data* aiuta a prevedere tendenze demografiche, economiche e sanitarie, permettendo di anticipare necessità di infrastrutture o interventi in ambito sanitario, educativo e di sicurezza nazionale[13].

Tuttavia, l'uso pervasivo degli algoritmi – come sarà trattato nel Capitolo 3 – solleva anche **questioni etiche e di equità**. Il rischio del c.d. **"*bias* algoritmico"**, in base al quale pregiudizi esistenti nei dati possono portare a decisioni ingiuste o discriminatorie, rappresenta un fenomeno di crescente preoccupazione. La trasparenza e la regolamentazione di questi sistemi automatizzati diventano quindi cruciali per garantire che i dati forniti attraverso sistemi di IA influenzino la società in modo equo e benefico. In conclusione, mentre gli algoritmi influenzano e trasformano in modo significativo il modo in cui viviamo, lavoriamo e interagiamo, è cruciale affrontare le sfide che accompagnano la loro adozione per assicurare che il loro impatto sulla società sia positivo e inclusivo.

Come cambia la geopolitica nell'era dell'informazione

Nell'era dell'informazione, gli algoritmi e l'Intelligenza Artificiale stanno ridisegnando la rete delle relazioni internazionali e della geopolitica con un **impatto decisivo su sicurezza nazionale, competitività economica e stabilità politica**. Queste tecnologie non sono semplicemente strumenti tecnologici, ma si sono trasformate in **leve di potere e influenza a livello globale**[14].

---

[12] Fonte: IDSS, "*How algorithms impact society*", 2023.

[13] Fonte: The Harvard Gazette, "*Great promise but potential for peril*", 2020.

[14] Si veda: Brookings Institution, "*The geopolitics of AI and the rise of digital sovereignty*", 2022.

La Quarta Rivoluzione Industriale, guidando innovazioni in settori come l'automazione, la robotica e l'analisi dei *Big Data* è stata propedeutica allo sviluppo accelerato – dal 2020 – delle **tecnologie che abilitano l'Intelligenza Artificiale** (come *High Performance Computing*, *Digital Twin*, connettività ultra-veloce 5G e 6G, *Quantum Computing* e metaverso) e alla piena realizzazione del **paradigma dell'Industria 5.0** che, secondo la visione della Commissione Europea[15], completerà il paradigma di *Industry* 4.0 grazie alla spinta di ricerca e innovazione verso una transizione verso un'**industria sostenibile, centrata sull'uomo e resiliente**: una Quinta Rivoluzione Industriale che dovrebbe favorire un **rapporto di lavoro più equilibrato e collaborativo** tra le tecnologie sempre più intelligenti e gli esseri umani.

Potenze globali come gli Stati Uniti d'America, la Cina e l'Unione Europea investono massicciamente in IA per guadagnare un vantaggio competitivo che può definire la propria *leadership* economica futura. Questo spostamento verso l'alta tecnologia sta ridefinendo le catene di valore globali e i modelli di *business*, rendendo la competenza algoritmica un indicatore chiave di potenza economica. In tal senso, USA e Cina sono attualmente coinvolti in una nuova "guerra fredda tecnologica", in cui la supremazia nel campo dell'IA potrebbe determinare il prossimo *leader* globale in termini di innovazione e potenza militare[16].

Nel campo della **sicurezza nazionale**, gli algoritmi sono utilizzati dalla sorveglianza di massa alla *cybersecurity*. Ad esempio, sistemi avanzati di riconoscimento facciale sono impiegati per il monitoraggio delle frontiere, mentre algoritmi sofisticati identificano schemi in dati criptati per prevenire attacchi cibernetici. Questi strumenti aumentano la capacità di uno Stato di proteggere i suoi cittadini e le sue infrastrutture critiche, ma sollevano anche preoccupazioni riguardanti la tutela della *privacy* e il rischio di esercitare forme di controllo autoritario.

Gli algoritmi influenzano anche la **stabilità politica interna ed esterna** dei Paesi. Le tecniche di manipolazione dell'informazione, come le campagne di disinformazione digitale, possono alterare l'opinione pubblica, destabilizzare regimi politici o influenzare il risultato di elezioni democratiche[17].

Esempi recenti includono l'uso di algoritmi per diffondere notizie false o polarizzanti durante le elezioni in vari Paesi, evidenziando come la tecnologia possa essere usata sia come strumento di coesione che di discordia. La Russia ha impiegato tattiche di guerra informatica e *cyber*-spionaggio che hanno sfruttato algoritmi avanzati per compromettere infrastrutture critiche e influenzare l'opinione pubblica, dimostrando come gli strumenti digitali possono essere integrati anche in operazioni militari e politiche.

In sintesi, l'importanza degli algoritmi nell'era dell'informazione si manifesta attraverso il loro ruolo critico nei meccanismi di esercizio di potere geopolitico, sottolineando la necessità di una comprensione profonda e di una gestione prudente di queste tecnologie per garantire sicurezza e stabilità a livello globale.

Lo spostamento dell'industria della difesa verso il campo digitale e le applicazioni di uso duale

Il settore della difesa svolge un ruolo fondamentale in ambiti chiave per il funzionamento e lo sviluppo di ogni sistema territoriale, a tutti i livelli, ponendo le condizioni per la sua **sicurezza, stabilità e crescita**.

[15] Si veda: Commissione Europea, "*Industry 5.0 - Towards a sustainable, human-centric and resilient European industry*", 2021.

[16] Fonte: RAND, "*AI and Geopolitics*", 2023.

[17] Fonte: Goldman Sachs, "*The generative world order: AI, geopolitics and power*", 2023.

L'industria della difesa è testimone di una trasformazione significativa, caratterizzata da un crescente spostamento verso il campo digitale. Questo cambiamento si manifesta attraverso investimenti massicci nella *cybersecurity*, che si affiancano e integrano i dispositivi *hardware* tradizionali: il rafforzamento delle capacità e della dotazione di *device* digitali risponde alla necessità di affrontare sfide di sicurezza emergenti in un mondo sempre più digitalizzato e interconnesso.

Gli investimenti nel settore della difesa non solo stanno aumentando nel loro complesso (+3,3% medio annuo tra il 2001 e il 2022), ma si stanno anche diversificando come tipologia di tecnologie impiegate. Nel 2022, la spesa militare mondiale ha raggiunto il **valore *record* di 2,24 trilioni di Dollari**, anche a seguito del rafforzamento delle dotazioni militari richieste dallo scoppio del conflitto tra Russia e Ucraina e dalle crescenti tensioni nel Mar Cinese Meridionale, con gli Stati Uniti d'America che rappresentano circa il 40% della spesa militare totale a livello globale.

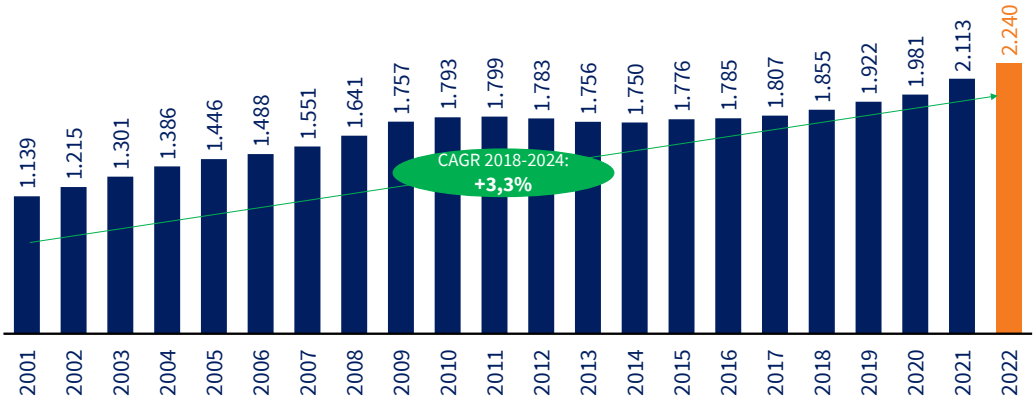


Figura 8. Andamento della spesa militare globale (miliardi di Dollari a prezzi costanti 2021), 2001-2022. *Fonte: elaborazione The European House – Ambrosetti su dati IMF e SIPRI, 2024.*

Inoltre, il finanziamento non è più limitato a dispositivi fisici come veicoli e armamenti, ma include ora *software* avanzati per la protezione delle infrastrutture critiche[18]. Questi programmi sono progettati per respingere attacchi informatici, monitorare minacce e proteggere dati sensibili attraverso tecnologie di crittografia e sistemi di gestione dell'identità e degli accessi[19]. In tale contesto di evoluzione, l'Intelligenza Artificiale permette alle imprese del settore della difesa e della sicurezza di fornire velocemente prodotti e servizi di alta qualità, sostenibili e misurati rispetto alle esigenze in rapido mutamento del mercato.

L'Intelligenza Artificiale trova infatti diverse applicazioni nel settore Aerospazio, Difesa & Sicurezza (AD&S) come:

- l'utilizzo a bordo degli elicotteri per migliorare la sorveglianza durante le operazioni di controllo dei confini;
- il monitoraggio dello stato di salute delle unità in missione, intervenendo con indicazioni precise e adatte alla situazione in caso di necessità;
- l'equipaggiamento di droni e veicoli autonomi, da un lato, migliorando la capacità di sorveglianza e intervento e, dall'altro, riducendo la necessità di esposizione diretta del personale militare.

[18] Fonte: U.S. Department of Defence, "*Digital transformation, AI important in keeping battlefield edge, leaders say*", 2022.

[19] Fonte: Microsoft for Defense and Intelligence, "*Secure the digital defense ecosystem and improve interoperability*", 2023.

A conferma di questo cambiamento e della crescente importanza che l'Intelligenza Artificiale sta assumendo nella modernizzazione delle capacità di difesa, **la spesa militare degli Stati Uniti d'America in sistemi intelligenti è quasi triplicata tra il 2022 e il 2023**.

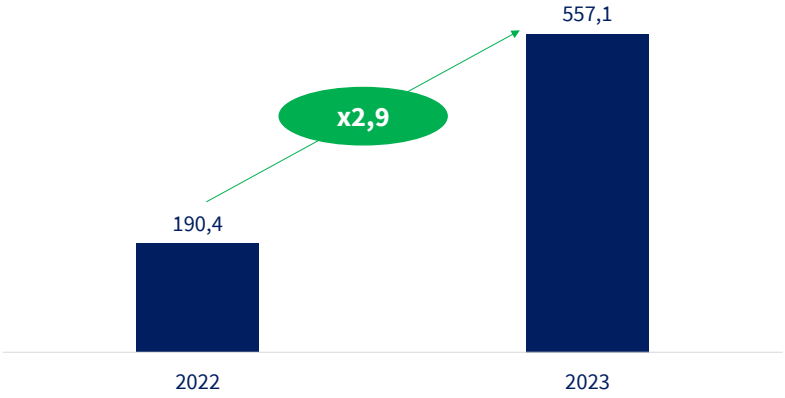


Figura 9. Spesa militare destinata all'Intelligenza Artificiale negli Stati Uniti d'America (milioni di Dollari), 2022 – 2023. *Fonte: elaborazione The European House – Ambrosetti su dati Brookings Institution, 2024.*

Anche la Commissione Europea sta discutendo (primavera 2024) di potenziare gli investimenti su tecnologie-chiave per la guerra convenzionale di prossima generazione, attraverso lo sviluppo – nell'ambito dei progetti da finanziare con il Fondo Europeo per la Difesa – di sistemi di aerei da combattimento collaborativi senza equipaggio, sistemi terrestri multiuso senza equipaggio e sistemi intelligenti funzionali per le future piattaforme navali.

Un altro aspetto fondamentale dell'evoluzione del settore della difesa e della sicurezza è il c.d. "***digital use***", ovvero lo ***spillover*** **tecnologico dal settore militare a quello civile**. Sono considerati "duali" i beni e le tecnologie che non sono esclusivamente destinati ad un uso militare ma trovano applicazione anche in più settori economici.

Innovazioni oggi molto diffuse – come Internet, i navigatori satellitari e i sensori – sono state sviluppate e applicate originariamente in ambito militare e successivamente trasferite in ambito civile. La **ricerca con finalità militari** ha ricoperto nel corso della storia il **ruolo di precursore**. Infatti, la ricerca, come attività di analisi e sperimentazione, a livello pratico e teorico, al fine di migliorare l'esistente e creare nuovi strumenti, è nata, in primo luogo, in ambito militare, per dare vita ad innovazioni tali da garantire la superiorità operativa o strategica di popoli e nazioni. In campo aerospaziale, questo processo di osmosi è stato ancora più evidente: i **sistemi di "comando e controllo"**, con relativa sensoristica, hanno trovato ampio riuso nella gestione del traffico civile aereo, marittimo e ferroviario. Oggi i mezzi di Aeronautica e Marina Militare possono avere un impiego in operazioni di assistenza umanitaria, come attività di soccorso in mare dei migranti o di protezione civile.

I grandi progetti avviati a livello nazionale nel settore AD&S nel tempo hanno generato importanti ricadute economiche, scientifiche e politiche non solo per i Paesi che li hanno lanciati, ma anche per la collettività grazie alla successiva applicazione duale.

Due esempi di particolare notorietà sono:

- il **progetto "Apollo"**, lanciato dagli USA per dimostrare la propria superiorità tecnologica rispetto a quella sovietica nell'esplorazione spaziale e nella difesa missilistica;
- il sistema di posizionamento e navigazione di precisione, basato sulla **costellazione satellitare "Galileo"**, di matrice europea.

Focus – Il progetto "Apollo" e il ruolo della DARPA nello sviluppo di tecnologie duali

L'impresa che ha portato l'uomo a camminare sulla luna è alla base del percorso che ha permesso di realizzare **almeno 30.000 oggetti** (ad esempio, il tessuto impermeabile Gore-Tex, il velcro, i rivestimenti in teflon) e ha dato un fortissimo impulso allo sviluppo di **tecnologie rivoluzionarie** (si pensi alla ricerca sperimentale che ha portato agli autoveicoli a guida autonoma e allo sviluppo della tecnologia che ha portato a Siri di Apple, fino al *quantum computing* e al *deep learning*).

Fondata nel 1958, la **DARPA** (Defence Advanced Research Projects Agency) è il principale ente di ricerca del Dipartimento della Difesa statunitense, che opera all'interno di un ecosistema dell'innovazione che coinvolge *partner* accademici, aziendali e governativi.

A questa agenzia federale, la cui missione è quella di effettuare investimenti-chiave in **tecnologie innovative per la sicurezza nazionale**, si devono molte delle principali innovazioni applicate in ambito militare negli ultimi 65 anni (ad esempio, le basi concettuali di ARPANET e lo sviluppo dei protocolli digitali che hanno portato ad Internet, GPS, tecnologia *stealth*). Il ruolo strategico della DARPA è testimoniato dalla richiesta di *budget* da parte della Presidenza statunitense pari a 4,37 miliardi di Dollari per l'anno fiscale 2025 (rispetto ai 4,12 miliardi di Dollari per il 2024). Parte del *budget* della DARPA serve a finanziare specifici progetti della NASA che, dalla sua nascita, ha portato alla creazione di **più di 2.000 *spin-off*** su progetti che trovano applicazioni in svariati settori, diversi da quello spaziale in senso stretto (scienze della vita, *Information Technology*, energia, edilizia, ecc.).

Dal 2018, attraverso la campagna "AI Next" e con il successivo programma "AI Forward", la DARPA ha investito più di 2 miliardi di Dollari per far progredire l'IA per scopi di sicurezza nazionale. Oggi, circa il 70% dei programmi DARPA beneficia dell'Intelligenza Artificiale e della tecnologia di apprendimento automatico e sono in corso investimenti in più di 30 programmi per esplorare e sviluppare una gamma completa di tecniche di IA.

Fonte: elaborazione The European House - Ambrosetti su dati DARPA, 2024

Focus – Le ricadute della ricerca in ambito spaziale sull'ambito civile: il caso del sistema europeo "Galileo"

Galileo è il sistema globale di navigazione satellitare (GNSS) dell'Unione Europea progettato per inviare segnali radio per il posizionamento, la navigazione e la misurazione del tempo: avviato dall'UE e dall'Agenzia Spaziale Europea (ESA) nei primi anni Duemila come alternativa autonoma ai sistemi di navigazione satellitare americano GPS e al russo Glonass, ha l'obiettivo di garantire una sovranità europea – e quindi indipendenza e autonomia – in tale campo.

Il progetto è interamente **concepito per usi civili** e, grazie ad una costellazione di 28 satelliti e un segmento terrestre mondiale, è già oggi **il servizio di navigazione satellitare più preciso al mondo**, non soggetto alle limitazioni o alle interruzioni tipiche di altri sistemi pensati per scopi militari.

Galileo presenta enormi potenzialità di impiego nei più diversi settori, in considerazione della costante crescita del mercato dei prodotti e servizi che sfruttano il sistema satellitare: in particolare, il **nuovo servizio ad alta precisione** si indirizza ad applicazioni come l'agricoltura di precisione, la prospezione delle risorse, i rilievi terrestri e idrografici, fino ad applicazioni emergenti quali la robotica, la guida autonoma di automobili, treni, navi e droni, il volo in formazione dei satelliti, oltre al *gaming* e al *marketing* con realtà aumentata.

Fonte: elaborazione The European House - Ambrosetti su dati Agenzia Spaziale Europea, 2024.

Dunque, oggi la linea di separazione tra ambito civile e ambito militare è sempre più sottile, con un'inversione di tendenza rispetto al passato: la Difesa, infatti, dipende sempre più da tecnologie sviluppate in ambito civile, in particolare quelle connesse ad elettronica, comunicazioni e informatica, che presentano ritmi di innovazione e sviluppo superiori rispetto a quelle sviluppate in ambito militare. Gli sviluppi in questi settori – nanotecnologie, nuovi materiali, fonti energetiche, ecc. – sono campi di innovazione irrinunciabili per mantenere la crescita economica globale e hanno molteplici applicazioni tecnologiche duali.

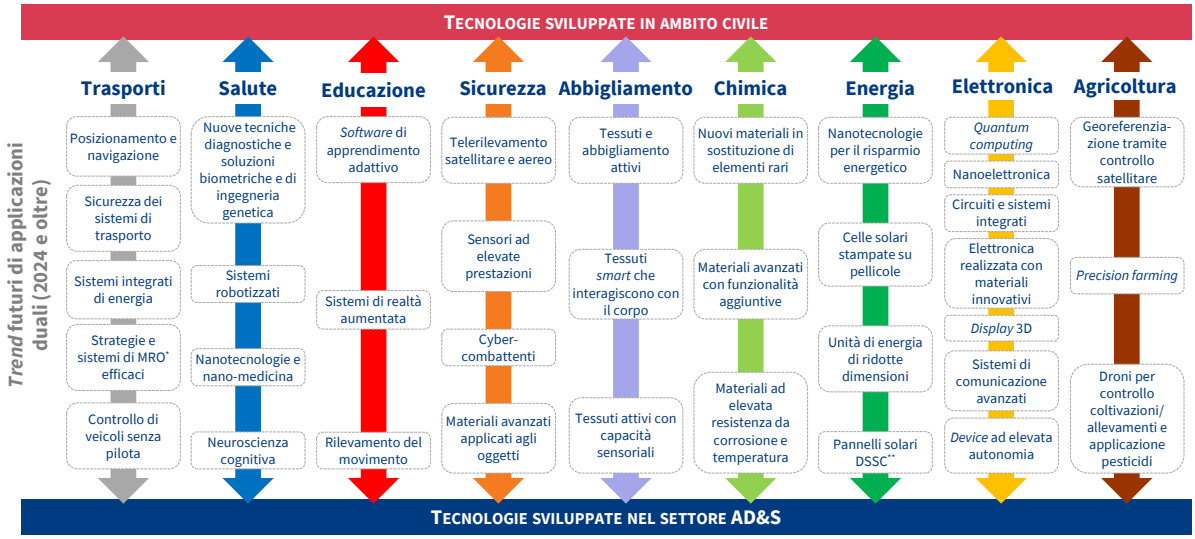


Figura 10. Ambiti di applicazione duale delle tecnologie del futuro. (*) MRO: *Maintenance, Repair and Overhaul*; (**) DSSC: *Dye-Sensitized Solar Cell*. *Fonte: elaborazione The European House – Ambrosetti, 2024.*

Capitolo 3.
La corsa delle potenze mondiali per il dominio su tecnologie, competenze digitali e materie prime critiche

Nel panorama internazionale attuale, la competizione per il dominio tecnologico rappresenta un cruciale campo di battaglia dove potenze globali come Stati Uniti d'America, Cina e Russia vedono il progresso tecnologico come un elemento fondamentale per rafforzare la loro influenza e potenza globale. Questa corsa per la supremazia tecnologica è particolarmente evidente nel campo dell'Intelligenza Artificiale (IA), che si è affermata come una delle principali frontiere dell'innovazione e che sposterà gli equilibri e le alleanze tra le potenze globali.

In questo contesto, l'industria della tecnologia e del digitale risulta ancora dominata da **grandi gruppi statunitensi**, come dimostra la presenza di Apple, Alphabet e Meta ai vertici della classifica dei gruppi tecnologici globali, anche se, da alcuni anni, si sta rafforzando il ruolo di **gruppi tecnologici cinesi, sudcoreani e giapponesi**.

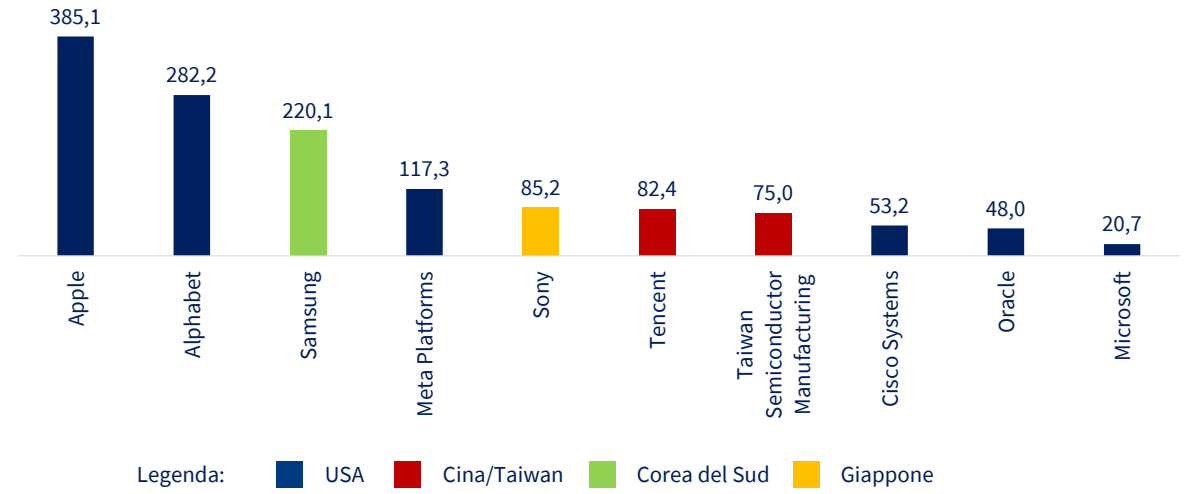


Figura 11. Primi 10 gruppi tecnologici a livello globale per Paese di appartenenza (miliardi di Dollari), 2023.
Fonte: elaborazione The European House – Ambrosetti su dati Forbes, 2024.

La competizione per il dominio tecnologico tra le super potenze mondiali si gioca anche sul campo dei **brevetti**, ambito in cui emerge, al contrario, la ***leadership* della Cina**, con più di 1,6 milioni di domande di brevetto nel 2022, seguita da USA (594 mila), Giappone (289 mila), Corea del Sud (237 mila) e dall'Ufficio Brevetti Europeo (EPO, con quasi 194 mila).

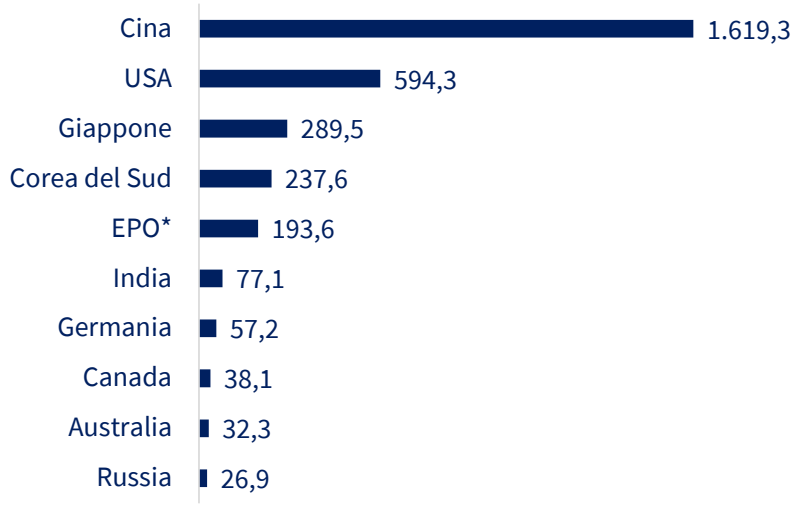


Figura 12. Numero di domande di brevetti per Paese (migliaia), 2022. (*) EPO: European Patent Office. *Fonte: elaborazione The European House – Ambrosetti su dati World Intellectual Property Organization (WIPO), 2024.*

Il divario delle potenze occidentali rispetto alla Cina emerge con maggiore evidenza se si esamina la competizione su brevetti tecnologici nel campo dell'Intelligenza Artificiale. Infatti, al 2022 **la Cina guida la classifica globale dei brevetti sull'IA (61,1% del totale**, +44,2 punti percentuali rispetto al 2010), seguita dagli **Stati Uniti d'America**, con il **20,9%** del totale e in riduzione di oltre 33 punti percentuali rispetto al 2010. Un'analoga sorte è toccata all'asse dei Paesi europei, la cui incidenza sul totale mondiale è passata dal 7,5% al 2%.

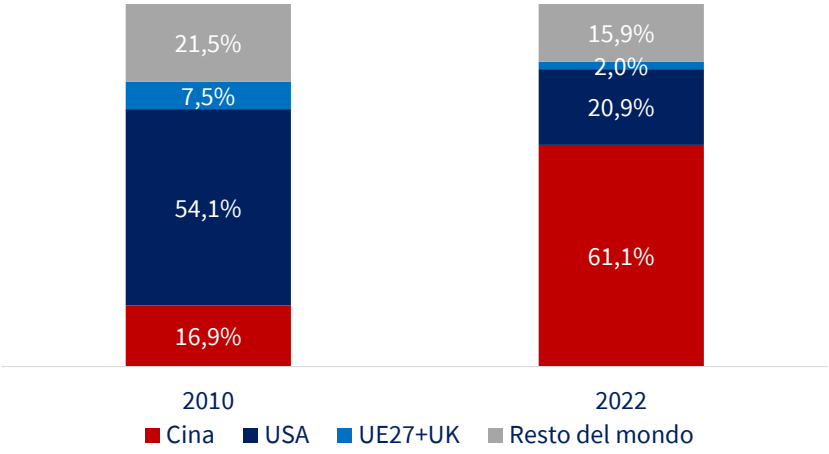


Figura 13. Ripartizione del numero di brevetti riconosciuti sull'Intelligenza Artificiale per area geografica (valori %): confronto tra 2010 e 2022. *Fonte: elaborazione The European House – Ambrosetti su dati Center for Security and Emerging Technology e Stanford University, 2024.*

Allo stesso modo, Corea del Sud, USA, Giappone e Cina sono nella *Top* 5 globale per numero di brevetti riconosciuti sull'Intelligenza Artificiale in rapporto alla propria popolazione.

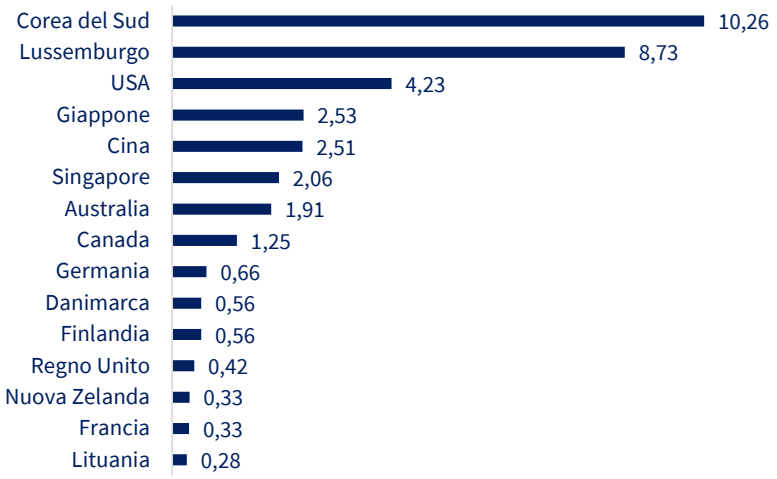


Figura 14. Numero di brevetti riconosciuti sull'Intelligenza Artificiale ogni 100.000 abitanti, 2022. *Fonte: elaborazione The European House – Ambrosetti su dati Center for Security and Emerging Technology e Stanford University, 2024.*

Se si considera invece la **nazionalità delle principali aziende in base al numero di domande di brevetto pubblicate sull'AI**, ben 12 delle prime 20 aziende sono multinazionali **giapponesi**, a sottolineare il peso significativo del Sol Levante in questo ambito tecnologico. Tuttavia, i portafogli più rilevanti di brevetti nell'IA sono detenuti da **gruppi statunitensi**, con IBM che domina la classifica con 8.920 famiglie di brevetti, seguita da Microsoft con 5.930. La **Repubblica di Corea** non è da meno, vantando due conglomerati (Samsung e LG Corporation) nella top 20, a cui si aggiungono due rappresentanti della **Germania** (Siemens e Bosch), mostrando così una distribuzione geografica piuttosto eterogenea delle potenze dominanti nell'AI. La maggior parte delle aziende elencate tra le prime 30 richiedenti nella figura sono conglomerati attivi nel settore dell'elettronica di consumo, settori delle telecomunicazioni e/o del software, sebbene ci sia anche un servizio elettrico (SGCC) e un produttore di automobili (Toyota) incluso. Dal punto di vista delle **università e pubbliche organizzazioni di ricerca nel campo dell'intelligenza artificiale**, la maggioranza (17) si trova in **Cina** e il resto nella **Repubblica di Corea**. Del resto, l'Accademia delle Scienze cinese (CAS) si posiziona al primo posto nella classifica generale dei primi 30 richiedenti mentre l'Istituto di Ricerca Elettronica e Telecomunicazioni coreano (ETRI) si posiziona al secondo.

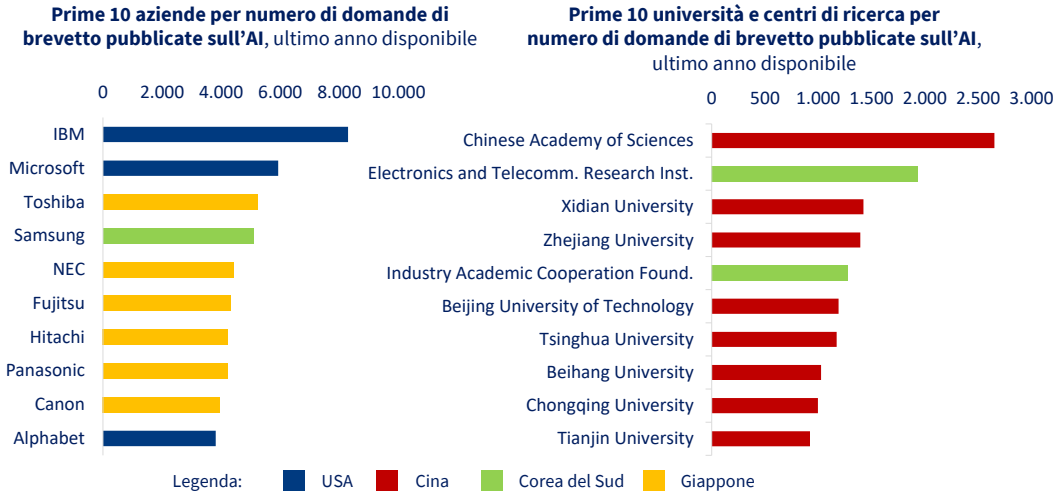


Figura 15. Prime 10 aziende e università nel mondo per numero di domande di brevetto pubblicate sull'IA, ultimo anno disponibile. *Fonte: elaborazione The European House – Ambrosetti su dati World Intellectual Property Organization (WIPO), 2024.*

Focus – La "*Swiss AI Initiative*" per un'Intelligenza Artificiale trasparente e affidabile

Nella corsa per rafforzare il proprio dominio digitale e tecnologico è d'interesse il caso della Svizzera che, con un approccio virtuoso, attraverso la "***Swiss AI Initiative***" punta a diventare un ***hub* globale di riferimento** in cui sviluppare e implementare l'Intelligenza Artificiale. Questa iniziativa, varata dal Politecnico di Zurigo e di Losanna, ha permesso il lancio del nuovo supercomputer **Alps**, uno dei computer più potenti al mondo, sviluppato appositamente per soddisfare le esigenze delle applicazioni nel campo dell'IA. Questo nuovo calcolatore consente agli scienziati svizzeri di accedere a una potenza di calcolo che è disponibile solo alle più grandi aziende tecnologiche, offrendo quindi alla Svizzera un notevole vantaggio competitivo rispetto ai rivali internazionali.

La "*Swiss AI Initiative*" non solo sostiene l'avanzamento tecnologico ma pone anche un forte accento sulla **trasparenza** e sull'**accessibilità**: l'obiettivo è sviluppare nuovi modelli linguistici di grandi dimensioni (LLM) che siano aperti e comprensibili, garantendo che le innovazioni rispettino i criteri legali, etici e scientifici. Oltre a rafforzare la ricerca scientifica, l'iniziativa intende essere un mezzo per **proteggere la sovranità digitale** della Svizzera, assicurando che il Paese elvetico possa mantenere un controllo indipendente sulle proprie innovazioni tecnologiche senza dipendere da multinazionali estere, promuovendo un'innovazione indipendente pur renderendo le competenze sviluppate trasferibili a imprese, alle università e alla società in generale.

Fonte: elaborazione The European House - Ambrosetti su fonti varie, 2024.

Focus – L'approccio collaborativo del modello francese per l'*open source* dell'IA Generativa

In un contesto in cui il mondo dell'IA è dominato dalle *Big Tech*, l'alternativa a questa concentrazione è offerta dall'IA Generativa *open source*. Il governo francese è stato tra i primi a sostenere il pluralismo e a promuovere un modello di concorrenza quasi perfetto.

Coerentemente con questa posizione, la Francia ha attivato un **fondo da 500 milioni di Euro per attrarre talenti in IA generativa** e ha sostenuto la crescita di Mistral AI e la nascita di Kyutai Lab:

- Mistral AI è specializzata nello sviluppo di modelli linguistici di grandi dimensioni e si propone come piattaforma aperta per verticalizzare l'IA in diversi settori d'uso; utilizza un modello di cooperazione tanto dirompente da riuscire a raccogliere, nel solo mese di ottobre 2023, 385 milioni di Euro di finanziamento.
- Kyutai è il primo laboratorio europeo di ricerca aperta in Intelligenza Artificiale, focalizzato sullo sviluppo di grandi modelli multimodali che utilizzano testi, immagini, video e codici aperti per rendere l'algoritmo più trasparente e capace.

Il modello francese presenta diversi punti di forza, primo fra tutti, l'autonomia energetica, assicurata dallo Stato, indispensabile, per addestrare modelli di intelligenza artificiale energivori. Kyutai, dal suo canto, ha l'ambizione di mettere in campo due dei principali vettori dell'Intelligenza Artificiale: la massa critica di competenze necessarie e la disponibilità degli ambienti per sviluppare i modelli di IA.

Fonte: elaborazione The European House - Ambrosetti su fonti varie, 2024.

Una terza dimensione, oltre alla R&S tecnologica e brevettuale, su cui si basa la competizione digitale tra potenze mondiali è l'**approvvigionamento delle materie prime critiche**, definite tali per: a) l'**importanza economica**, ovvero utilizzo delle materie prime in tecnologie e applicazioni industriali; b) il **rischio di fornitura**, ovvero la concentrazione in singoli Paesi della produzione mondiale di materie prime e il relativo rischio di approvvigionamento[20].

[20] La Commissione Europea considera una materia prima come critica quando presenta, allo stesso tempo, un rischio di fornitura >1,0 (su un indice da 0 a 6) e una importanza economica >2,8 (su un indice da 0 a 9).

Le materie prime critiche sono infatti oggi rilevanti per molteplici ecosistemi industriali e rientrano in tecnologie chiave per la politica energetica, economica, industriale, la difesa e appunto per l'**industria digitale**. Il *Critical Raw Materials Act*, emanato a marzo 2023 dalla Commissione Europea, ha stabilito che, entro il 2030, estrazione, raffinazione e riciclo dovranno soddisfare, rispettivamente, almeno il 10%, 40% e 15% del fabbisogno europeo di materie prime critiche e ha identificato le materie prime utili allo sviluppo di quattro ambiti strategici: **energie rinnovabili, mobilità elettrica, digitale e difesa e aerospazio**. Il censimento europeo di 34 materie prime critiche ha consentito di individuarne 17 classificabili come "strategiche" (considerando le terre rare distinte in leggere e pesanti)[21]. Nello specifico:

- Il **settore digitale** dipende ampiamente da componenti elettronici che richiedono terre rare, dispositivi fondamentali per il processamento dei dati e l'apprendimento automatico, che sono al centro dell'IA. *Data storage* e *server* e prodotti di elettronica rappresentano il 90% della domanda di chips (con la previsione di raddoppiare a livello globale da qui al 2030).
- Nella **difesa** e nell'**aerospazio**, l'IA viene impiegata per una ampia varietà di applicazioni: l'UE ha elaborato lo *Strategic Compass*, che fissa un nuovo livello di ambizione per la difesa e la sicurezza Europea, con la *Space Economy* (di cui droni e satelliti fanno parte) che rappresenta un abilitatore ed è attesa crescere del 56% al 2030 nell'UE.

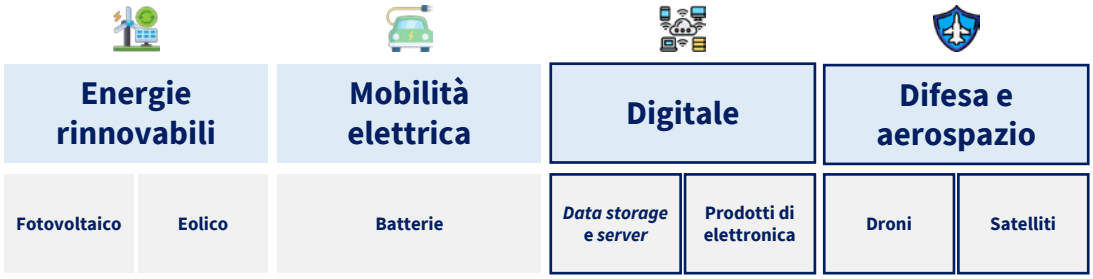


Figura 16. Gli ambiti strategici per l'UE come definiti nel *Critical Raw Materials Act* e le relative tecnologie strategiche che prevedono l'utilizzo di materie prime critiche. *Fonte: elaborazione The European House – Ambrosetti su dati Commissione Europea, 2024.*

34 materie prime critiche censite nel 2023 (di cui 17 materie prime strategiche)

Afnio	Alluminio/bauxite	Antimonio	Arsenico	Barite	Berillio
Bismuto	Boro/Borato	Carbone da coke	Cobalto	Elio	Feldspato
Fluorite	Fosforite	Fosforo	Gallio	Germanio	Grafite naturale
Litio	Magnesio	Manganese	Metalli del gruppo del platino*	Nichel	Niobio
Rame	Scandio	Silicio metallico	Stronzio	Tantalio	Titanio
Terre rare leggere**	Terre rare pesanti***	Tungsteno	Vanadio		

Figura 17. Le materie prime censite dalla Commissione Europea, 2023. Nota: sono evidenziate in rosso le materie prime strategiche. (*) Platino, Palladio, Rodio, Rutenio, Iridio. (**) Cerio, Lantanio, Neodimio, Praseodimio, Samario. (***) Disprosio, Erbio, Europio, Gadolinio, Olmio, Lutezio, Terbio, Tulio, Itterbio, Ittrio. *Fonte: elaborazione The European House – Ambrosetti su dati Commissione Europea, 2024.*

[21] La Commissione Europea le definisce "strategiche" le "materie prime rilevanti per le tecnologie che supportano la duplice transizione verde e digitale e gli obiettivi della difesa e dell'aerospazio". Rame e Nickel non sono propriamente materie prime critiche, in quanto non soddisfano i criteri relativi a rischio di fornitura e importanza economica, ma sono stati inseriti ugualmente dalla Commissione Europea perché ritenute materie prime strategiche.

Considerati il loro **esteso utilizzo** e l'alto **rischio di fornitura** con gravi rischi legati alla sicurezza negli approvvigionamenti, la **competizione per l'ottenimento di queste materie critiche** si è fortemente accentuata. Il mercato per le materia identificate è infatti molto **concentrato**, aumentando così i rischi associati all'interruzione della fornitura. Per 17 delle 34 materie prime critiche il grado di concentrazione nei primi 3 Paesi fornitori supera il valore del 90%.

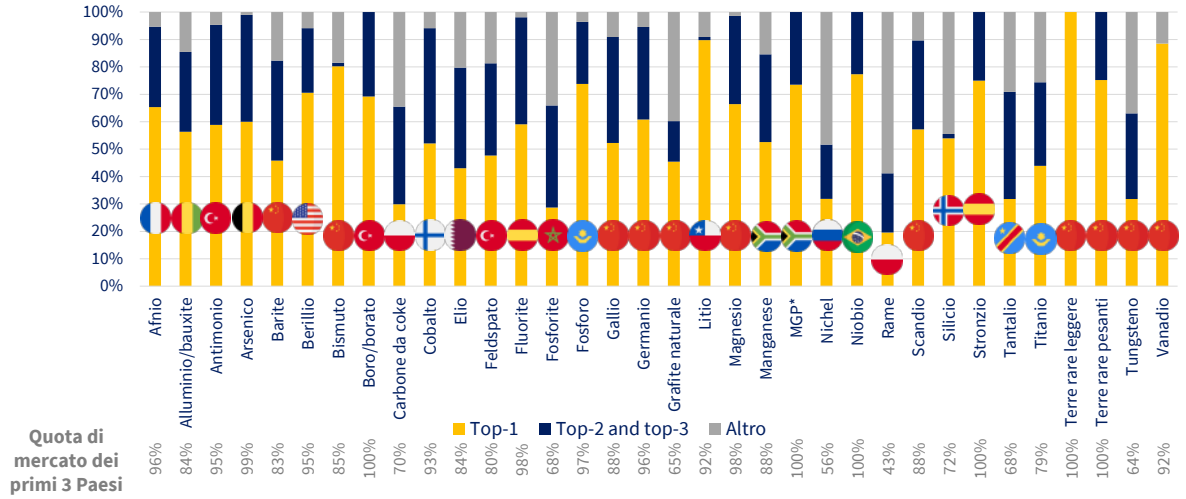


Figura 18. Grado di concentrazione per l'approvvigionamento di materie prime critiche, 2023. Nota: la Commissione Europea, tramite il *Critical Raw Materials Act*, ha fissato una soglia massima di dipendenza da un singolo Paese pari al 65%. Ad oggi, questo limite è superato da: boro, gallio, litio, magnesio, MGP, niobio, scandio, stronzio, terre rare. Le materie prime critiche per cui un Paese dell'UE risulta il primo fornitore in UE sono: afnio, arsenico, carbone da coke, cobalto, fluorite, rame, stronzio. (*) MGP: metalli del gruppo del platino. *Fonte: elaborazione The European House – Ambrosetti su dati Commissione Europea, 2023.*

La Cina vanta il maggior controllo degli approvvigionamenti (mercato *leader* per 11 materie prime critiche su 34) [22] ed è il principale fornitore europeo per il **56% delle materie prime critiche oggi importate in UE** (ad esempio, fornisce l'85% delle terre rare leggere e il 100% delle terre rare pesanti).

Con l'obiettivo di diventare entro il 2050 la prima potenza mondiale nelle tecnologie del futuro, la Cina ha infatti con il suo **13° Piano Quinquennale** (2016-2020) posto al centro della propria pianificazione la questione dei metalli strategici, puntando ad accrescere la propria posizione di *leadership* e preservare le proprie **riserve nazionali** in caso di forte domanda sui mercati. Questo obiettivo ambizioso è raggiungibile per un Paese che vanta un **ricco sottosuolo di risorse naturali** – il che lo rende un importante produttore per diversi mercati. Il ruolo della Cina non si basa però solo sulla produzione domestica, ma anche sulla **capacità di raffinazione e sugli investimenti in giacimenti minerari in Paesi terzi**: oltre **80 miliardi di Euro** sono infatti stati investiti tra il 2005 e il 2021 verso solo i primi 10 Paesi per ammontare di investimenti diretti esteri in attività estrattive e di raffinazione.

[22] La Cina ha una posizione dominante per diverse materie prime, tra cui Tungsteno (con l'82% della produzione e il 57% delle riserve), Terre rare (con il 72% della produzione e il 37% delle riserve) e Grafite (con il 68% della produzione e il 24% delle riserve). Fonte: elaborazione The European House – Ambrosetti su dati United States Geological Survey, 2024.

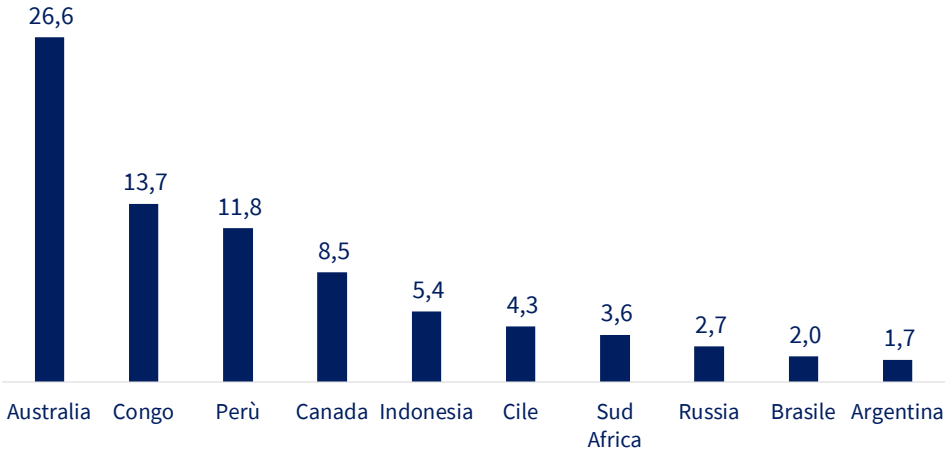


Figura 19. *Top*-10 dei Paesi per investimenti diretti esteri cinesi in attività estrattive e di raffinazione di metalli (miliardi di euro), 2005-2021. *Fonte: elaborazione The European House – Ambrosetti su dati China Global Investment Tracker ed IRENA, 2023.*

Il primato cinese è confermato anche dalla nazionalità dei **principali estrattori e raffinatori di terre rare per fatturato annuo**. Questo mercato, infatti, vede ai vertici società cinesi con controllo statale, contrapposte da aziende australiane e statunitensi controllate da fondi di investimento.

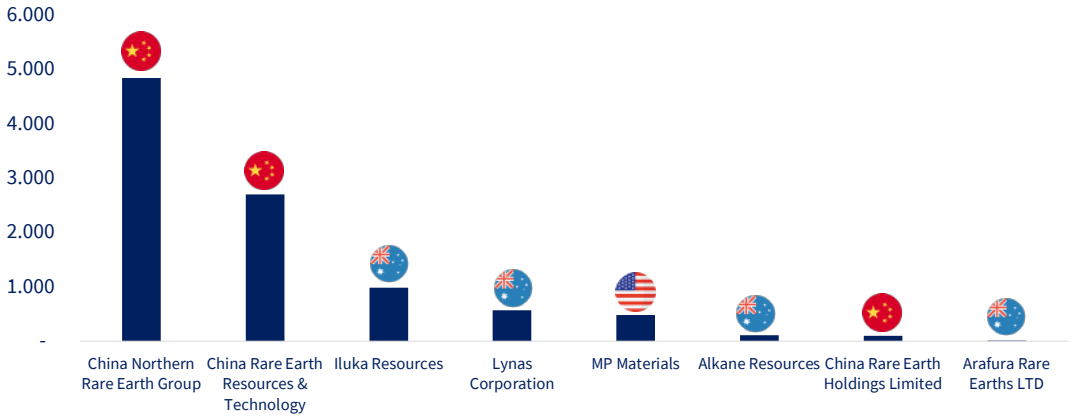


Figura 20. I principali estrattori e raffinatori di terre rare per fatturato annuo (valori assoluti in milioni di Euro), 2022. *Fonte: elaborazione The European House – Ambrosetti su dati Reuters e dati individuali delle aziende, 2023.*

Capitolo 4.
Il ruolo e le applicazioni dell'Intelligenza Artificiale nello scenario geopolitico globale: minaccia o opportunità?

L'IA Generativa è una tecnologia *general-purpose* che può trasformare radicalmente la società e l'economia: questo comporta **sfide etiche e sociali rilevanti**.

Oltre all'evoluzione del settore della Difesa nella direzione del *digital warfare*, di cui si è trattato nel Capitolo 2, si possono individuare alcune aree in cui l'applicazione degli strumenti dell'Intelligenza Artificiale **può generare impatti positivi o negativi a seconda del modo in cui questa tecnologia viene impiegata**:

- *cybersecurity*;
- tutela dei dati e *privacy*;
- influenza dell'informazione e dell'opinione pubblica;
- diplomazia digitale.

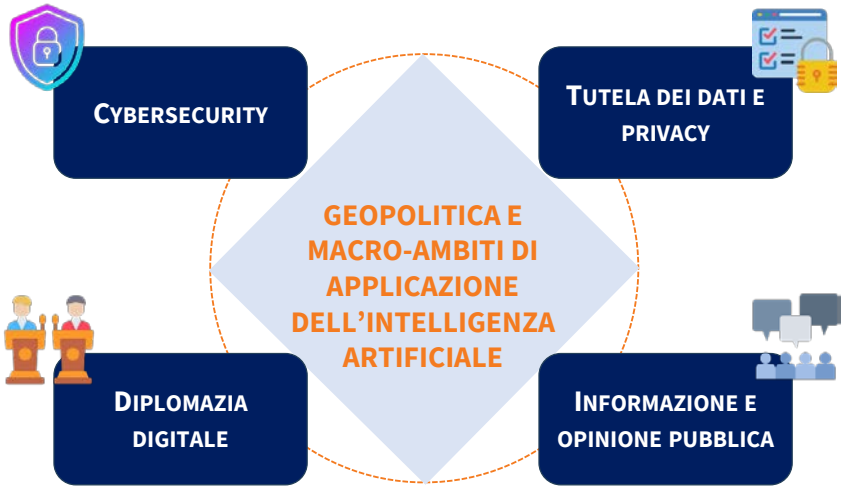


Figura 21. I principali macro-ambiti di applicazione dell'Intelligenza Artificiale nello scenario della geopolitica. *Fonte: elaborazione The European House – Ambrosetti, 2024.*

Lo sviluppo dell'IA generativa può generare **rischi specifici collegati sia allo sviluppo della tecnologia** (nella fase di *design*, addestramento e *fine tuning* del modello di IA Generativa), **che alla sua adozione di scala**: in ambito geopolitico, i rischi connessi all'IA includono *bias* e imparzialità nei modelli, la possibile produzione di *output* falsi o imprecisi di modelli IA, la mancanza di trasparenza, l'esposizione a minacce per la sicurezza e la *privacy* (violazione di dati su cui non si dispone della proprietà intellettuale, come informazioni aziendali o industriali) o la diffusione di *fake news* e contenuti manipolati per influenzare l'opinione pubblica o l'esito di determinate attività politico-sociali.

Allo stesso tempo, l'IA può offrire **un valido supporto nella mitigazione di questi rischi**, fornendo informazioni affidabili e precise, così come analisi predittive e/o correttive di possibili deviazioni rispetto ad un uso corretto e trasparente di questo strumento.

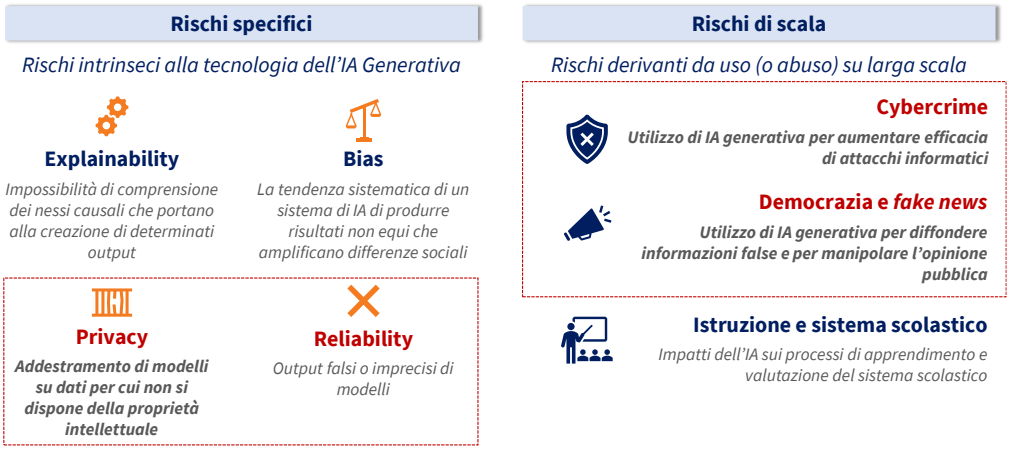


Figura 22. I possibili rischi, specifici e di scala, legati all'applicazione dell'Intelligenza Artificiale nella società contemporanea, nel sistema d'impresa e nello scenario della geopolitica (evidenziate in colore rosso). *Fonte: elaborazione The European House - Ambrosetti e Microsoft Italia, 2024.*

Sicurezza informatica e minacce cibernetiche: gli impatti sulla geopolitica

Lo sviluppo e l'impiego degli algoritmi può avvenire tanto nella difesa delle infrastrutture critiche quanto nella prevenzione e analisi di potenziali minacce cibernetiche.

Gli algoritmi di IA svolgono un ruolo cruciale non solo nel **rafforzare la sicurezza delle infrastrutture digitali, ma anche di quelle fisiche**. È possibile, ad esempio, monitorare reti per rilevare comportamenti anomali che potrebbero indicare attacchi informatici, così come sorvegliare impianti fisici per prevenire accessi non autorizzati o sabotaggi. La capacità dell'IA di apprendere e di adattarsi ai nuovi scenari di minaccia in tempo reale la rende uno strumento indispensabile per la *cybersecurity* e la protezione fisica. L'IA aiuta a identificare e mitigare una vasta gamma di minacce, dalle intrusioni *malware* agli attacchi di *phishing*, *ransomware*, e anche incursioni fisiche. Le strategie basate sull'Intelligenza Artificiale possono includere la segmentazione della rete, l'analisi comportamentale degli utenti, la risposta automatica agli incidenti e il monitoraggio avanzato degli accessi fisici, migliorando notevolmente l'efficacia delle misure di sicurezza tradizionali[23].

Nonostante questi benefici, l'impiego dell'IA in *cybersecurity* e nella protezione fisica presenta anche rischi significativi, tra cui il potenziale abuso di queste tecnologie per condurre attacchi sofisticati. La regolamentazione internazionale, come le linee guida congiunte sviluppate da CISA e dal *National Cyber Security Centre* (NCSC) britannico, mira a definire *standard* di sicurezza per lo sviluppo di sistemi di IA robusti e sicuri, minimizzando il rischio di attacchi che sfruttano le vulnerabilità presenti in applicazioni, reti o *hardware*[24].

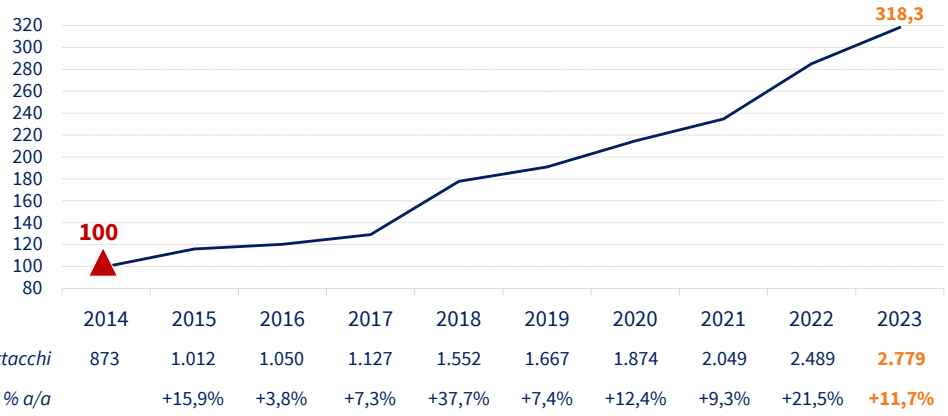
La *cybersecurity* è un campo cruciale nel panorama della sicurezza contemporanea che si occupa della **protezione delle reti, dei sistemi e dei programmi informatici dagli attacchi digitali**. Con l'accelerazione della trasformazione digitale e la crescente dipendenza da infrastrutture tecnologiche in ogni aspetto della vita quotidiana e professionale, la sicurezza informatica è diventata una necessità inderogabile.

Gli attacchi *cyber* possono prefigurarsi obiettivi diversi (dal furto di dati sensibili alla distruzione di infrastrutture critiche): il 2023 ha registrato un impressionante incremento negli incidenti di

[23] ISC2, "*Enhancing cybersecurity through AI: A look into the future*", 2023.

[24] CISA, "*Cybersecurity best practices*", 2024.

sicurezza di pubblico dominio e di particolare gravità [25], stabilendo un nuovo *record* per la frequenza degli attacchi (+12% nel 2023), **più che triplicati rispetto ai livelli del 2014** (da 873 a quasi 2.800).



	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Numero di attacchi	873	1.012	1.050	1.127	1.552	1.667	1.874	2.049	2.489	**2.779**
Variazione % a/a		+15,9%	+3,8%	+7,3%	+37,7%	+7,4%	+12,4%	+9,3%	+21,5%	**+11,7%**

Figura 23. Andamento dei *cyber* attacchi gravi di dominio pubblico su scala globale (numero indice, anno 2014 = base 100; valori assoluti e variazione % annua), 2014 - 2023. *Fonte: elaborazione The European House – Ambrosetti su dati Clusit, 2024.*

Questa situazione ha evidenziato più che mai la centralità della *cybersecurity* nel proteggere reti, sistemi e programmi informatici dagli attacchi digitali, portando ad un forte incremento negli investimenti dell'industria globale della *cybersecurity*, le cui proiezioni indicano una crescita dei ricavi dai 218 a 583 miliardi di Dollari tra il 2020 e il 2030, ad un tasso medio annuo composto del +9,5%. In tale contesto, è evidente come l'industria della *cybersecurity* si intrecci in maniera sempre più complessa e profonda con lo sviluppo dell'Intelligenza Artificiale: si stima infatti che **il mercato globale della *cybersecurity* basata sull'IA crescerà del 28% medio annuo entro il 2030**, riflettendo il riconoscimento collettivo dell'importanza critica dell'IA nella prevenzione, rilevazione e risposta agli attacchi informatici.

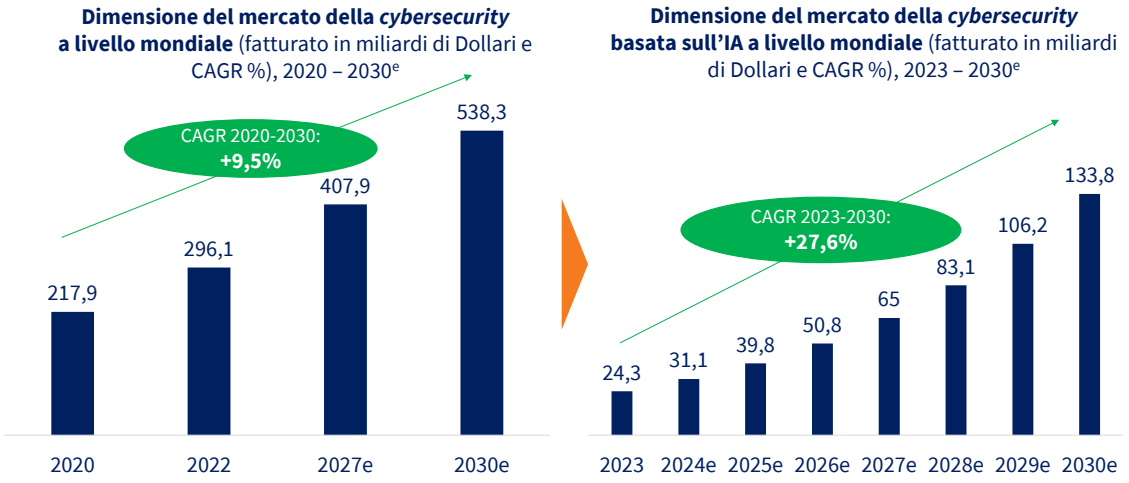


Figura 24. Dimensione del mercato della *cybersecurity* a livello mondiale (fatturato in miliardi di Dollari; grafico di sinistra), 2020 – 2030e; dimensione del mercato della *cybersecurity* basata sull'IA a livello mondiale (fatturato in miliardi di Dollari; grafico di destra), 2023 – 2030e. *Fonte: elaborazione The European House – Ambrosetti su dati GlobeNewswire e Techopedia, 2024.*

[25] Si tratta di *cyber* attacchi noti, andati a buon fine e di particolare gravità, che hanno avuto impatti significativi in termini economici, tecnologici, legali, reputazionali sulle organizzazioni vittima degli stessi. Fonte: Clusit, "Rapporto Clusit 2024 sulla sicurezza ICT in Italia", 2024.

Le minacce *cyber* rappresentano oggi una delle più grandi sfide per la sicurezza globale, coinvolgendo una varietà di attori, ciascuno con motivazioni diverse e complesse. Questi attori possono essere classificati in tre categorie principali: **attori statali, non statali e gruppi terroristici**.

Gli **attori statali** (c.d. "*Nation-State hacker*") sono sostenuti da governi nazionali e spesso hanno risorse significative a loro disposizione. Queste operazioni sono di solito molto sofisticate e possono includere le seguenti tipologie:

- **spionaggio informatico**: molti Stati utilizzano *cyber* attacchi per acquisire segreti commerciali, tecnologie avanzate, o informazioni politiche sensibili da altre nazioni. Questo tipo di spionaggio può servire a rafforzare la loro sicurezza nazionale o posizione economica globale;
- **sabotaggio**: alcuni Stati potrebbero cercare di disturbare le infrastrutture critiche di un Paese nemico (come reti elettriche, idriche o di comunicazione), per esercitare pressione politica o militare;
- **manipolazione elettorale**: l'interferenza nelle elezioni di un altro Paese attraverso *cyber* attacchi può avere l'obiettivo di favorire l'insediamento di *leader* politici favorevoli o creare disordine e sfiducia verso le istituzioni democratiche.

Gli **attori non statali** includono *hacker* individuali e organizzazioni criminali che spesso cercano guadagno economico tramite attività illegali come:

- ***ransomware***: questi attacchi implicano il blocco dell'accesso agli archivi digitali di un'entità e richiedendo un riscatto per il loro sblocco; possono colpire ospedali, scuole o enti governativi, causando non solo perdite economiche ma anche crisi nelle operazioni quotidiane;
- **frode bancaria e furto di identità**: l'accesso a informazioni finanziarie personali permette a questi criminali di sottrarre fondi o aprire conti fraudolenti, portando a significative perdite economiche per gli individui colpiti;
- **DDoS (*Distributed Denial of Service*)**: questi attacchi sovraccaricano i *server web* per rendere i siti internet inaccessibili, spesso per estorcere denaro per cessare l'attacco o semplicemente per danneggiare la reputazione dell'entità attaccata[26].

Due casi di particolare gravità e risonanza mediatica sono stati gli **attacchi cibernetici WannaCry e NotPetya**, avvenuti entrambi nel **2017**, che si può considerare il primo anno in cui hanno iniziato a diffondersi attacchi *hacker* su scala globale e di proporzioni mai viste in precedenza, con l'obiettivo di colpire enti governativi, infrastrutture critiche e imprese.

[26] Fonte: CubeCyber, "*Types of cyber threat actors and their motivations*", 2020.

Focus – L'attacco WannaCry: il primo caso di *cyber weapon* diffuso su scala globale

L'attacco *ransomware* WannaCry del maggio 2017, poche settimane prima dell'attacco NotPetya, è uno degli esempi più eclatanti di cybercriminalità perpetrata da **attori non statali**. Questo attacco ha avuto un impatto globale, **infettando centinaia di migliaia di computer in oltre 150 Paesi**.

Sono state colpite anche infrastrutture critiche (ad esempio, in alcuni ospedali, WannaCry ha cifrato tutti i dispositivi, apparecchiature medicali comprese) e alcune imprese sono state costrette a fermare o a rallentare le linee di produzione industriale. Si ritiene che questa arma cibernetica che sfrutta una vulnerabilità dei sistemi Windows, nota come EternalBlue, sia stata sottratta ed utilizzata su scala globale dal gruppo di hacker "*The Shadow Brokers*".

WannaCry ha messo in evidenza le potenziali minacce poste da gruppi di *hacker* ben organizzati. Le analisi tecniche del codice del *ransomware* hanno mostrato somiglianze con quello usato in precedenti attacchi attribuiti al Lazarus Group, un'entità *hacker* che si ritiene operi sotto l'egida della Corea del Nord, sebbene il governo nordcoreano abbia negato ogni coinvolgimento. L'identità precisa degli autori rimane oggetto di speculazioni, ma le prove suggeriscono che dietro l'attacco vi siano stati degli *hacker* piuttosto che attori statali ufficiali.

L'attacco del 2017 ha evidenziato la **vulnerabilità critica delle infrastrutture informatiche globali** e ha spinto verso un rinnovato *focus* sulla sicurezza dei sistemi e sulla gestione delle vulnerabilità note: WannaCry ha, in sostanza, agito da "campanello d'allarme" sulla crescente minaccia rappresentata da gruppi di *hacker* criminali nell'era digitale.

Fonte: elaborazione The European House - Ambrosetti su fonti varie, 2024.

Focus – L'attacco *cyber* NotPetya: la svolta nel settore della *cyberwarfare*

L'operazione NotPetya rappresenta uno dei casi più gravi e costosi di aggressione cibernetica a livello globale. Iniziato a giugno 2017, questo attacco ha avuto come primo bersaglio aziende ucraine, sfruttando un *software* di aggiornamento fiscale ampiamente utilizzato in Ucraina. Attraverso tale programma, il *malware* si è rapidamente diffuso a livello internazionale attraverso le vulnerabilità presenti nei protocolli dei sistemi operativi Windows, **colpendo aziende e infrastrutture in più di 60 Paesi**.

Contrariamente alle apparenze iniziali, NotPetya non era un semplice *ransomware* volto ad estorcere denaro criptando i dati e chiedendo un riscatto in Bitcoin, ma si è rivelato essere un *wiper malware* finalizzato a **distruggere dati e causare interruzioni di infrastrutture critiche**. L'impatto dell'attacco è stato di ampia portata, con stime di **perdite economiche totali superiori ai 10 miliardi di Dollari**. Grandi gruppi internazionali di trasporti, logistica o produzioni manifatturiere hanno subito gravi danni economici, dovuti principalmente alla sospensione delle operazioni e alla distruzione di dati critici.

L'accusa pubblica dell'operazione NotPetya come un'azione del governo russo è stata formalizzata da diversi governi occidentali, che hanno interpretato l'attacco come parte di una strategia più ampia per destabilizzare l'Ucraina e, al contempo, dimostrare la propria capacità di influenzare e manipolare gli equilibri geopolitici attraverso la guerra cibernetica.

Questo episodio ha segnato un momento significativo nella storia della *cybersecurity*:

- da un lato, ha evidenziato l'impiego degli attacchi informatici come **strumenti di politica estera e armi in contesti geopolitici complessi**
- dall'altro, ha sottolineato la crescente necessità per tutte le nazioni di **rafforzare le proprie difese *cyber*** di fronte a potenziali attacchi informatici di altri Stati (finanziati, sofisticati e capaci di prendere di mira qualsiasi organizzazione).

Fonte: elaborazione The European House - Ambrosetti su fonti varie, 2024.

Infine, i **gruppi terroristici** utilizzano il *cyber*-spazio per promuovere le loro agende ideologiche o politiche, con iniziative come:

- **propaganda**: utilizzano Internet per diffondere il loro messaggio, reclutare nuovi membri e incitare ad atti di violenza;
- **attacchi a infrastrutture critiche**: mirano a causare distruzione fisica o psicologica attraverso attacchi a infrastrutture vitali o strumenti di comunicazione di massa, spesso con l'obiettivo di instillare paura o costringere governi a cedere a richieste politiche;
- **finanziamento delle loro operazioni**: il crimine cibernetico fornisce una fonte di finanziamento attraverso frodi *online*, estorsioni e altre attività illecite[27].

***Focus* – L'attacco *cyber* aTV5 Monde**

Nell'aprile 2015, il gruppo terroristico ISIS ha condotto un attacco informatico di grande impatto contro **TV5 Monde**, **una delle maggiori reti televisive francesi**. L'attacco ha portato alla **temporanea disabilitazione delle trasmissioni della rete e al controllo dei suoi *account* sui *social media***. Gli *hacker* hanno sfruttato questi canali per diffondere messaggi di propaganda, inclusi minacce e sostegno alla causa di ISIS. L'attacco si è distinto per la sua sofisticatezza: gli aggressori hanno usato tecniche di *phishing* per ottenere accesso agli *account e-mail* e alle *password* degli amministratori di rete di TV5 Monde. Ciò ha permesso loro di infiltrarsi nei sistemi di controllo delle trasmissioni e nei profili *social* della rete. L'incidente ha avuto un forte impatto sia materiale che psicologico, evidenziando la vulnerabilità delle istituzioni di fronte alle capacità *cyber* dei gruppi terroristici.

Questo episodio ha anche mostrato come i gruppi terroristici, tra cui l'ISIS, siano in grado di eseguire operazioni *cyber* complesse non solo per creare disordine, ma anche per **influenzare l'opinione pubblica**. Ha anche messo in luce la necessità per le organizzazioni di tutto il mondo di adottare misure di sicurezza *cyber* più solide, per proteggersi da minacce che stanno diventando sempre più sofisticate e diversificate. L'attacco a TV5 Monde ha segnato un punto di svolta nella percezione del *cyber* terrorismo e ha sottolineato quanto sia fondamentale integrare la sicurezza informatica nelle strategie di difesa nazionale e internazionale contro il terrorismo.

Fonte: elaborazione The European House - Ambrosetti su fonti varie, 2024.

Anche in Italia, gli attacchi *cyber* sono aumentati notevolmente negli ultimi anni (tra i casi di particolare gravità, si è passati **da 39 a 310 tra il 2019 e il 2023**, con oltre il 47% del totale concentrato nell'ultimo anno ed una crescita media annua di gran lunga superiore all'andamento globale, ovvero +70% in Italia rispetto al +14% nel mondo), colpendo vari settori cruciali come gli enti pubblici, la sanità, l'industria manifatturiera e il settore finanziario-assicurativo. L'analisi realizzata da Clusit sull'anno 2023 evidenzia un incremento significativo degli attacchi mirati ad **organi governativi, militari o delle forze dell'ordine**, che hanno ricevuto il 19% degli attacchi totali (+50% rispetto al 2022), seguito dall'**industria** con il 13% (pari ad un quarto del totale degli attacchi rivolti al comparto manifatturiero a livello globale). Più in generale, si rileva una tendenza globale a mirare alle infrastrutture critiche (stabilimenti industriali, banche, ospedali, ecc.), in particolare durante la pandemia da COVID-19, che ha accelerato la digitalizzazione e quindi anche la vulnerabilità a tali attacchi[28]. La gravità degli attacchi *cyber* è aumentata, con una maggiore frequenza di attacchi di livello "critico" e "alto", confermando un aumento della sofisticazione e dell'impatto potenziale di tali attacchi, richiedendo una risposta più robusta e coordinata per la sicurezza cibernetica[29].

[27] Fonte: RAND, "*The motivations of cyber threat actors and their use and monetization of stolen data*", 2018.

[28] Fonte: Clusit, "Rapporto Clusit 2024 sulla sicurezza ICT in Italia", 2024.

[29] Fonte: Agenda Digitale, "*Crescono gli attacchi cyber in Italia, ma anche le difese: ecco il quadro*", 2022.

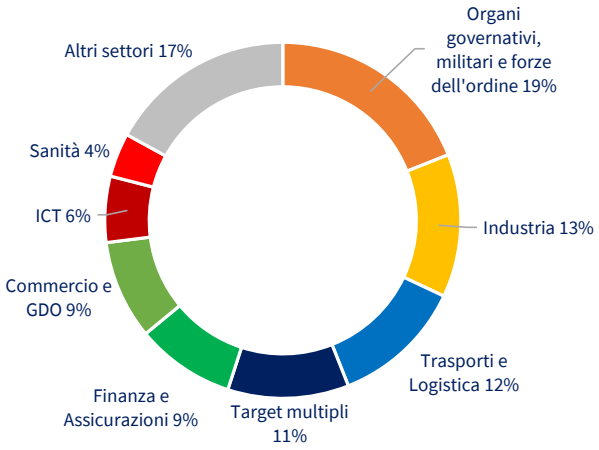


Figura 25. Ripartizione degli attacchi *cyber* in Italia per settore di attività (valori %), 2023. *Fonte: elaborazione The European House – Ambrosetti su dati Clusit, 2024.*

Privacy e tutela dei dati: gli impatti sulla geopolitica

Nell'era della "*data economy*", la **raccolta massiva di informazioni** da parte di enti governativi e aziende private ha sollevato interrogativi critici su ***privacy*, sorveglianza, consenso e proprietà dei dati**[30]. Considerati il "**nuovo petrolio**" dell'economia mondiale, i dati sono diventati una **risorsa strategica cruciale**, in grado di influenzare gli equilibri di potere e le dinamiche geopolitiche a livello globale[31]. Oggi, la **sorveglianza attraverso tecnologie avanzate** permette una raccolta di informazioni senza precedenti, spesso al di fuori del controllo diretto degli individui. Ciò solleva preoccupazioni significative riguardo al **consenso**. Normative come il **GDPR dell'UE** cercano di imporre regole severe su trasparenza e consenso, ma le differenze normative tra i Paesi creano un contesto complesso in cui le imprese e le multinazionali devono muoversi, spesso sfruttando queste discrepanze a proprio vantaggio. Un altro aspetto fondamentale è la questione della **proprietà dei dati**. Sebbene gli individui possano considerare i loro dati personali come di proprietà privata, enti governativi e corporazioni tendono a considerarli come una risorse da sfruttare: questo controllo sui dati coinvolge non solo chi può accedervi, ma anche chi può usarli e trarne vantaggio, amplificando le sfide legate alla *privacy* e al controllo economico e politico[32].

A livello geopolitico, i dati conferiscono potere. Governi che possiedono o controllano grandi quantità di dati possono **influenzare la politica interna e internazionale**, dal potenziamento delle capacità di sorveglianza alla manipolazione dell'opinione pubblica, fino al tentativo di influenzare le elezioni attraverso la disinformazione. Analogamente, le *Big Tech* che gestiscono enormi quantità di dati, possono esercitare influenza economica e politica che equivale o supera quello di intere singole nazioni.

In questo contesto, i conflitti emergono quando le normative sulla protezione dei dati impediscono il **flusso internazionale di dati**, creando tensioni tra Paesi con approcci divergenti alla *privacy*. Tali tensioni possono influenzare alleanze internazionali e relazioni geopolitiche, con blocchi come l'UE che spingono per **maggiori protezioni** e altri che adottano **politiche più permissive** per favorire l'economia o la sorveglianza[33].

[30] Fonte: Pew Research Center, "*How Americans View Data Privacy*", 2023.

[31] Fonte: Brookings Institution, "*Police surveillance and facial recognition*', 2022.

[32] Fonte: VPNOverview, "*Big Data and Privacy: what is it and what are the risks*?", 2023.

[33] Fonte: CSIS, "*Digital dragnets: examining the government's access to your personal data*", 2022.

Come anticipato, le **normative internazionali sulla protezione dei dati** sono al centro di **numerosi conflitti geopolitici**, poiché i Paesi cercano di bilanciare la sicurezza nazionale, la *privacy* degli individui e le esigenze economiche. La protezione dei dati è regolata da molteplici **leggi nazionali** che possono variare significativamente da un Paese all'altro.

Ad esempio, il **GDPR europeo** impone rigidi standard per la raccolta, l'uso e la condivisione dei dati personali, richiedendo il consenso esplicito degli utenti e garantendo loro un controllo significativo sulle proprie informazioni. Questo regolamento, infatti, richiede che le aziende ottengano il consenso esplicito per la raccolta di dati e che forniscano agli utenti un controllo significativo sui loro dati. Inoltre, il GDPR ha introdotto il concetto di **"adeguatezza" per la trasmissione di dati personali al di fuori dell'UE**, il che significa che i paesi terzi devono garantire un livello di protezione dei dati comparabile a quello dell'UE per poter ricevere dati da essa[34].

Al contrario, altre nazioni come gli **USA** hanno adottato un **approccio più flessibile** e **settoriale** alla protezione dei dati, concentrando le regolamentazioni su specifici settori economici piuttosto che su un'ampia legislazione orizzontale. Questo ha creato sfide significative per le aziende multinazionali che devono navigare attraverso più regolamenti e garantire la conformità su scala globale[35]. Le tensioni emergono particolarmente quando queste diverse normative si scontrano. Ad esempio, le aziende europee che operano negli Stati Uniti possono trovarsi in una posizione difficile se i requisiti statunitensi per la divulgazione di dati a fini di sicurezza nazionale entrano in conflitto con le restrizioni imposte dal GDPR. Questi conflitti possono portare a **sanzioni significative** e **complessità legali**. Inoltre, l'evoluzione del quadro normativo in nazioni come la Cina e la Russia, dove le leggi sulla localizzazione dei dati richiedono che i dati sui cittadini siano archiviati e trattati fisicamente all'interno del Paese, aggiunge ulteriori sfide. Queste leggi sono spesso viste come **barriere al commercio e al flusso libero di informazioni** e possono essere interpretate come tentativi di **protezionismo digitale** o di **controllo governativo sull'informazione**.

Focus – L'AI Act dell'Unione Europea

L'**Unione Europea** ha introdotto l'**AI Act** (approvato a marzo 2024 dal Parlamento Europeo e in attesa dell'approvazione formale del Consiglio dell'Unione Europea), un tentativo di regolamentare l'uso dell'Intelligenza Artificiale all'interno dell'UE in modo che rispetti gli *standard* elevati di protezione dei dati già stabiliti dal GDPR: si tratta della prima normativa mondiale di **regolazione sistemica**.

L'AI Act mira a garantire che le applicazioni di IA siano **sicure e trasparenti**, classificando i sistemi di IA in base al rischio che presentano e imponendo **requisiti di conformità più severi per quelli considerati ad alto rischio**. Gli impatti attesi dell'AI Act sul business sono significativi. Le aziende che sviluppano o utilizzano sistemi di IA nell'UE dovranno assicurarsi che i loro prodotti rispettino le **rigide normative** in materia di trasparenza, sicurezza dei dati e protezione dei diritti umani. Ciò potrebbe comportare investimenti sostanziali in termini di tempo e risorse per garantire che i sistemi di IA siano conformi, ma potrebbe anche offrire opportunità di mercato per soluzioni di IA che eccellono nel rispetto della *privacy* e della sicurezza dei dati.

Inoltre, il regolamento mira a stabilire un equilibrio tra **promuovere l'innovazione tecnologica** e **mitigare i rischi potenziali associati all'Intelligenza Artificiale**, come la discriminazione algoritmica o gli errori di automazione che possono avere gravi ripercussioni sulla vita delle persone.

Fonte: elaborazione The European House - Ambrosetti su dati Commissione Europea, 2024.

[34] Fonte: 'Commissione Europea, "*Adequacy decisions*", 2024.

[35] Fonte: Thales Group, "*Beyond GDPR: data protection around the world*", 2021.

Focus – L'iniziativa UNESCO per tutelare dati e standardizzare regole sull'IA

Nel contesto delle normative internazionali sulla protezione dei dati e degli sforzi per armonizzare la regolamentazione dell'intelligenza artificiale, un'importante iniziativa è stata varata dall'**UNESCO** per stabilire ***standard* etici globali** sull'Intelligenza Artificiale. L'obiettivo è promuovere l'uso dell'IA in modo che rispetti i diritti umani universali, facilitando il dialogo e la cooperazione internazionale in un campo altrimenti frammentato dalle diverse regolamentazioni nazionali. L'iniziativa riconosce le potenzialità dell'IA nel promuovere lo sviluppo e il benessere umano, ma anche i rischi significativi che possono emergere in assenza di un quadro normativo coerente e rispettoso dei principi etici. L'UNESCO si propone, quindi, di fornire una piattaforma comune per il dialogo tra governi, aziende, società civile e comunità scientifiche, promuovendo una comprensione condivisa e l'adozione di pratiche migliori.

A tal fine, l'UNESCO ha pubblicato la **prima Guida per l'Intelligenza Artificiale Generativa nell'educazione e nella ricerca**, con l'obiettivo di aiutare gli Stati Membri a realizzare azioni immediate, pianificare politiche di lungo termine e assicurare uno sviluppo di queste nuove tecnologie incentrato sull'essere umano. La Guida propone i passi per arrivare ad una regolamentazione degli strumenti di Intelligenza Artificiale generativa, tra i quali, in primo luogo, esigere la **protezione dei dati personali** e stabilire un **limite minimo di età** per interagire con le piattaforme di IA Generativa.

Fonte: elaborazione The European House - Ambrosetti su dati UNESCO, 2024.

Intelligenza Artificiale e informazione, tra rischio di manipolazione dell'opinione pubblica e tutela dei principi democratici

La deriva dell'uso degli algoritmi come strumento di disinformazione e influenza

Gli algoritmi svolgono un ruolo centrale nell'era digitale, guidando non solo i flussi di informazione ma anche le percezioni pubbliche e personali. La capacità degli algoritmi di personalizzare i contenuti che riceviamo ogni giorno attraverso piattaforme di *social media* e altri canali digitali è diventata uno strumento potente. Questa personalizzazione può migliorare l'esperienza utente, ma porta con sé anche notevoli rischi, soprattutto quando viene utilizzata per diffondere disinformazione su larga scala.

L'attività di disinformazione si avvale degli algoritmi per mirare specifici gruppi demografici con messaggi che possono essere distorti o completamente falsi, ma incredibilmente persuasivi. Questo è possibile perché gli algoritmi sono capaci di analizzare vasti volumi di dati in tempo reale, imparando continuamente sulle preferenze e i comportamenti degli utenti, e possono quindi personalizzare i messaggi in modo che risonino in maniera più profonda con le convinzioni e i pregiudizi individuali. Questa precisione nel *targeting*, infatti, rende la disinformazione notevolmente efficace. I contenuti possono essere progettati per aggravare le divisioni sociali, rafforzare stereotipi esistenti o persino influenzare l'opinione pubblica su temi dibattuti (come, ad esempio, le elezioni, la politica sanitaria o il cambiamento climatico). Inoltre, la capacità degli algoritmi di generare e diffondere automaticamente contenuti rende questa forma di manipolazione scalabile, potendo raggiungere milioni di persone in un tempo incredibilmente breve.

Focus – Il caso Cambridge Analytica

Il caso di **Cambridge Analytica** rappresenta uno degli esempi più noti e controversi di come i dati degli utenti possano essere utilizzati per **influenzare l'opinione pubblica e manipolare il comportamento elettorale**.

Cambridge Analytica è stata una società di analisi dei dati che, attraverso la raccolta di un enorme quantità di dati e informazioni, era in grado di **creare modelli comportamentali e psicologici** che rispecchiassero le diverse tipologie di utenti che navigano in rete. L'azienda ha condotto numerose campagne elettorali in vari Paesi in via di sviluppo. Ma la vera svolta è avvenuta nel 2016, anno in cui si è occupata della corsa alla Presidenza degli Stati Uniti d'America. Con l'obiettivo di influenzare il **comportamento elettorale** durante la campagna elettorale, Cambridge Analytica ha raccolto i dati personali di milioni di utenti di Facebook senza il loro consenso per costruire **profili psicografici degli elettori**. Questi profili sono stati quindi usati per sviluppare **strategie di comunicazione mirate e personalizzate**, con l'obiettivo di influenzare il comportamento elettorale. Per questo nel 2018, la società si è trovata al centro di un grave scandalo internazionale: nonostante vi fossero già da anni indagini giornalistiche che denunciavano la raccolta illecita di dati personali da parte di Cambridge Analytica, le attività illecite sono venute alla luce nel marzo del 2018 a seguito delle dichiarazioni rese dall'ex dipendente Christopher Wylie. Le sue rivelazioni circa il *modus operandi* della società, pubblicate sui quotidiani The Guardian e New York Times il 17 marzo 2018, fecero scalpore: "*Abbiamo sfruttato Facebook per raccogliere i profili di milioni di persone. E abbiamo costruito modelli per sfruttare ciò che sapevamo su di loro e mirare ai loro demoni interiori. È su questa base che l'intera società è stata costruita*".

Fonte: elaborazione The European House - Ambrosetti su fonti varie, 2024.

In tale contesto dove gli algoritmi modellano le percezioni pubbliche e personali, la tecnologia dei c.d. ***deepfake*** emerge come un nuovo e potente **strumento di disinformazione**. Questi **contenuti audiovisivi** altamente realistici, generati da tecniche di apprendimento profondo, possono modificare la realtà in modi estremamente convincenti, presentando sfide senza precedenti per la verifica dei fatti e la fiducia nelle fonti mediatiche. Gli scopi per cui vengono utilizzati i *deepfake* sono molteplici:

- **falsificazione di identità**: i *deepfake* vengono utilizzati per rubare l'identità di una persona e utilizzarla, ad esempio, per bypassare sistemi di autenticazione visiva;
- **manipolazione di contenuti video**: i *deepfake* sono la base, insieme alle *fake news*, delle campagne di disinformazione utilizzate da media e partiti politici disonesti; inoltre, vengono utilizzati per alterare la reputazione di personalità famose;
- **simulazione di fatti non accaduti**: per lo stesso motivo di cui sopra, i *deepfake* possono essere usati per simulare eventi e diffondere notizie inesatte o false;
- **truffe su mezzi di comunicazione**: con un *deepfake* è possibile effettuare truffe ed estorsioni, simulando la presenza di una specifica persona in videochiamata o la voce di una persona, ad esempio per autenticarsi tramite comandi vocali.

Il collegamento con le manipolazioni algoritmiche è tangibile. Mentre la prima utilizza dati per affinare il *targeting* dei suoi messaggi, i *deepfake* spostano questa capacità su un altro livello, permettendo la creazione di contenuti completamente nuovi che possono essere indistinguibili dalla realtà. Questo rappresenta un salto significativo nella **capacità di influenzare l'opinione pubblica**; ad esempio, un video *deepfake* potrebbe far mostrare una personalità politica dire o fare qualcosa che in realtà non ha mai detto o fatto[36].

[36] Due esempi di *deepfake* divenuti virali sui media sono un presunto video di Volodymyr Zelensky, Presidente dell'Ucraina, intento ad arrendersi durante il conflitto con la Russia (marzo 2022) oppure il video creato nel 2018

In questo scenario dove i *deepfake* stanno già ridefinendo i confini della realtà virtuale, strumenti basati sull'Intelligenza Artificiale come **OpenSora di Open AI** (o come il suo *competitor* cinese Vidu), capace di creare in pochi secondi *videoclip* realistici di alta qualità secondo le indicazioni comunicate dall'utente, rappresentano una estensione delle capacità di **manipolazione digitale.** Questi strumenti AI facilitano la creazione di contenuti artificiali, dalla grafica alle interazioni testuali, con applicazioni alla stessa industria creativa e cinematografica, ma possono essere impiegati anche nella generazione di *deepfake* o nella simulazione di dialoghi realistici.

L'**accessibilità** di queste tecnologie significa che non solo gli Stati o le grandi organizzazioni, ma anche **individui privati** possono partecipare alla creazione e diffusione di disinformazione, rendendo ancora più difficile controllare la veridicità dei contenuti *online*. Lo stimolo determinato dallo sviluppo dell'IA al *deepfake* è sottolineato da una recente analisi[37] da cui emerge che i tentativi di truffa basati su *deepfake* sono aumentati del **3.000%** nel 2023. Secondo tali dati, le cause di questa crescita esponenziale sono da ricercarsi in questi fattori:

- perfezionamento dei *deepfake* grazie all'**IA generativa**, come DALL-E;
- accesso ad applicazioni di IA per la creazione di *deepfake* direttamente *online*, a **basso costo** o **senza costi**;
- **facilità di esecuzione** della creazione dei *deepfake*;
- **truffe di media complessità** in grandissime quantità, con guadagni unitari bassi, ma molto alti come valore cumulato.

La regolamentazione della sfera digitale come leva di contrasto alla disinformazione

Per fronteggiare tale minaccia crescente della disinformazione e proteggere l'integrità dell'ecosistema informativo, governi, organizzazioni internazionali e piattaforme *social* hanno adottato una serie di strategie. Le misure adottate sono volte a mitigare gli impatti della **disinformazione su elezioni**, **dibattiti pubblici e coesione sociale**.

I governi di varie nazioni hanno implementato politiche che monitorano e segnalano casi di disinformazione. Ad esempio, in **Germania**, il ***Network Enforcement Act* (NetzDG)**, introdotto nel 2017, obbliga le piattaforme *online* (come Facebook, Twitter e YouTube) a rimuovere il contenuto che è manifestamente illegale, come l'incitamento all'odio e le notizie false, entro 24 ore dalla segnalazione. In caso di inadempienza, le aziende possono ricevere multe di importo elevato[38].

In parallelo, organizzazioni e istituzioni internazionali come l'Unione Europea e le Nazioni Unite hanno avviato iniziative per combattere la disinformazione a livello globale. L'**UE**, ad esempio, ha lanciato il "***Code of practice on disinformation***" che impegna le piattaforme digitali ad adottare misure per ridurre la diffusione di contenuti falsi e ingannevoli. Questi sforzi includono l'etichettatura delle informazioni verificate, la promozione di contenuti autentici e la collaborazione con verificatori di fatti indipendenti[39]. L'**UNESCO**, attraverso il "***Media and information literacy***", lavora a livello internazionale per promuovere l'educazione ai *media* e all'informazione nei sistemi scolastici di tutto il mondo. Questo programma si concentra sul fornire

dall'attore e regista Jordan Peele e BuzzFeed, che mostra l'ex Presidente statunitense Barack Obama mentre pronuncia un avvertimento sui pericoli delle *fake news*: sebbene fosse stato concepito come esperimento educativo e di sensibilizzazione, dimostra chiaramente come i *deepfake* possano essere utilizzati per manipolare la percezione dell'opinione pubblica o distorcere la verità, con conseguenze potenzialmente gravi.

[37]Fonte: Onfido, "*Identity Fraud Report 2024"*, 2024.

[38] Fonte: CEPS, "*Germany's NetzDG: A key test for combatting online hate"*, 2018.

[39] Fonte: Commissione Europea, "*The 2022 Code of Practice on Disinformation"*, 2022.

agli studenti le competenze necessarie per analizzare criticamente le fonti e i contenuti, riconoscendo e respingendo la disinformazione.

Le piattaforme tecnologiche, riconoscendo il loro ruolo nella facilitazione della diffusione della disinformazione, stanno implementato anche dal loro lato strategie limitanti la diffusione di *fake news* e disinformazione, come dimostrano alcune azioni specifiche:

- **Twitter** ha introdotto una serie di misure per combattere la disinformazione durante le elezioni e la pandemia, come etichettare i *tweet* che contengono informazioni discutibili o ingannevoli e ridurre la visibilità dei contenuti segnalati come falsi, pur mantenendo la trasparenza su chi sia l'autore del *tweet*[40].
- **Facebook** ha creato un **programma di *fact-checking* di terze parti**, collaborando con organizzazioni certificate dall'International *Fact-Checking Network* per verificare i fatti dei contenuti condivisi sulla sua piattaforma. I post che vengono trovati falsi vengono declassati nel feed di notizie, riducendone la diffusione[41].
- **Google** ha lanciato iniziative per migliorare la qualità delle informazioni mostrate nelle sue ricerche, soprattutto durante crisi come le elezioni o emergenze sanitarie. Ha infatti implementato *tag* che identificano le fonti affidabili e ha finanziato campagne per aumentare la consapevolezza sull'importanza della verifica dei fatti.

Tuttavia, nonostante questi sforzi, il problema della disinformazione rimane complesso e in evoluzione, richiedendo una vigilanza continua (con modelli di *fact-checking* basati sull'IA) e l'adattamento delle strategie a nuove sfide e tecnologie.

La diplomazia nell'era digitale

Nell'era digitale, la diplomazia sta subendo una profonda trasformazione grazie all'integrazione degli algoritmi e dell'IA nel processo decisionale. Infatti, è nato un nuovo concetto di diplomazia, la **diplomazia digitale**, che si riferisce all'uso delle tecnologie digitali, compresa l'IA, nelle pratiche diplomatiche per promuovere gli interessi nazionali, gestire le relazioni internazionali e influenzare l'opinione pubblica a livello globale. Questi strumenti offrono agli Stati e alle organizzazioni internazionali la possibilità di comprendere meglio e reagire alle dinamiche globali con un livello di dettaglio e previsione senza precedenti. Le applicazioni dell'IA nelle relazioni diplomatiche e internazionali sono molteplici e possono essere riassunte in:

- ***Big Data Analytics* e analisi predittive**: gli algoritmi e l'IA sono sempre più utilizzati per analizzare enormi quantità di dati provenienti da fonti varie, come i *social media*, i dati finanziari, e le immagini satellitari. Questa capacità si traduce in una migliore comprensione delle tendenze globali, come i cambiamenti nei sentimenti politici o le fluttuazioni economiche. Sulla base di queste informazioni, la politica può identificare potenziali aree di instabilità o opportunità per la cooperazione prima che diventino evidenti attraverso i canali tradizionali. Ad esempio, l'analisi dettagliata dei dati può rivelare l'emergere di movimenti sociali o economici che potrebbero influenzare la politica internazionale o la stabilità regionale. La previsione di crisi internazionali è un altro ambito fondamentale in cui gli algoritmi stanno avendo un impatto significativo. Modelli predittivi alimentati da dati storici e attuali permettono di anticipare eventi come conflitti, crisi economiche o disastri ambientali: queste previsioni permettono ai governi di prepararsi meglio a gestire o prevenire queste situazioni, riducendo potenzialmente i danni e promuovendo interventi più efficaci.

[40] Fonte: Brookings Institution, "*Twitter, the EU, and self-regulation of disinformation*", 2023.

[41] Fonte: Meta, "*Disinformazione sottoposta a fact-checking*", 2024.

- ***Sentiment analysis***: gli algoritmi possono essere impiegati per monitorare l'opinione pubblica su questioni geopolitiche attraverso i *social media* e altri canali *online*. Le Ambasciate e i Ministeri degli esteri possono utilizzare queste informazioni per comprendere meglio le opinioni e le preoccupazioni dei cittadini stranieri e adattare di conseguenza le proprie strategie di comunicazione.
- **Sicurezza e difesa**: l'IA può essere impiegata dai governi e dagli enti diplomatici per migliorare la sorveglianza delle frontiere, la rilevazione di minacce e lo sviluppo di sistemi di difesa avanzati. Inoltre, gli algoritmi di apprendimento automatico vengono utilizzati per migliorare la *cybersecurity* e prevenire attacchi informatici, come già trattato in precedenza.
- **Analisi per l'elaborazione di strategie geopolitiche**: gli algoritmi possono essere utilizzati per analizzare i discorsi e le azioni dei *leader* politici e delle organizzazioni internazionali, fornendo *insight* sulle strategie diplomatiche e sui rapporti internazionali.
- **Comunicazione transculturale**: gli strumenti di traduzione automatica basati sull'IA consentono ai diplomatici di comunicare più facilmente con colleghi e *partner* internazionali che parlano lingue diverse. Questi strumenti possono facilitare la negoziazione di accordi internazionali e la gestione delle relazioni bilaterali.

Capitolo 5.
I principi alla base delle scelte strategiche per uno sviluppo sostenibile nella geopolitica digitale

Modelli a confronto nella gestione della geopolitica digitale

In un contesto globale caratterizzato da un'intensa competizione tecnologica e da una crescente digitalizzazione, l'Europa (e con essa l'Italia) si è impegnata a definire e consolidare una **posizione strategica che garantisca il necessario equilibrio tra innovazione e rispetto dei diritti individuali**.

Negli ultimi anni, i Governi stanno intensificando gli sforzi per regolamentare le tecnologie emergenti, soprattutto l'Intelligenza Artificiale Generativa, riconoscendo la necessità di guidare lo sviluppo tecnologico **secondo principi etici e normativi ben definiti**.

L'Europa, in particolare, si è distinta per un approccio alla regolamentazione digitale che si propone di individuare una **"terza via"** tra il **"modello liberale"**, orientato al mercato, degli **Stati Uniti d'America**, e il **"modello autoritario"**, fortemente controllato dallo Stato centrale, prevalente in **Cina**[42]. Questa terza via europea è profondamente radicata nella **tutela della *privacy*** e nella **sicurezza dei dati personali**, come dimostrato dal Regolamento Generale sulla Protezione dei Dati (GDPR), che ha stabilito nuovi *standard* globali per la *privacy* e la gestione dei dati. Il GDPR europeo ha segnato un passo significativo verso la **creazione di uno spazio digitale sicuro e affidabile**, con l'obiettivo di porre enfasi sulla **trasparenza** e sul **consenso esplicito**. Nel solco del GDPR, l'Europa ha fatto un ulteriore passo avanti con la recente proposta dell'**AI Act**, che mira a regolamentare l'uso dell'Intelligenza Artificiale. L'AI Act intende **codificare la responsabilità etica e legale nell'uso dell'IA**, classificando le applicazioni di IA in base al rischio che presentano e imponendo requisiti rigorosi per quelle considerate ad alto rischio.

Queste due regolamentazioni riflettono l'intenzione dell'UE di garantire che le tecnologie di IA siano sicure, trasparenti e non discriminatorie, cercando di stabilire un equilibrio tra il sostegno all'innovazione tecnologica e la mitigazione dei rischi associati all'IA, come la possibile erosione della *privacy*, l'incremento del controllo sociale e la manipolazione delle informazioni. L'**Italia**, quale Stato Membro dell'UE, segue queste direttive e si impegna attivamente nella formulazione e nell'attuazione di politiche che riflettano questi valori condivisi.

L'approccio europeo, quindi, offre una via alternativa equilibrata che potrebbe rivelarsi vitale per la costruzione a tendere di una **società digitale equa e sostenibile** in contrapposizione al **modello statunitense** – dominato dalle *Big Tech*, che tende a promuovere un approccio orientato al mercato dove la regolamentazione è minimale e i tempi dell'innovazione sono rapidi – e il **modello cinese** – caratterizzato da un **controllo statale estensivo**, con le tecnologie digitali impiegate come strumenti di sorveglianza e controllo sociale, nonché come mezzo per rafforzare la posizione economica e geopolitica[43].

[42] Brookings Institution, "*The EU and U.S. diverge on AI regulation: A transatlantic comparison and steps to alignment*", 2023.

[43] Politico, "*Europe's new data protection rules export privacy standards worldwide"*, 2018.

Verso una gestione sostenibile dell'IA nelle relazioni internazionali

L'emergere dell'Intelligenza Artificiale come fattore predominante nella tecnologia moderna ha trasformato non solo il commercio, l'economia e la vita quotidiana di tutti noi, ma anche il tessuto delle relazioni internazionali. Le capacità dell'IA di analizzare grandi volumi di dati e fornire intuizioni in tempo reale offrono strumenti senza precedenti per la diplomazia e la sicurezza globale. Tuttavia, il potere dell'IA comporta anche una grande responsabilità, ponendo diversi rischi etico-sociali.

Una gestione equa e responsabile dell'Intelligenza Artificiale, che **garantisca che l'intervento umano sia sempre presente nei processi decisionali guidati dagli algoritmi**, può (e deve) aiutare a mitigare i rischi e massimizzare i benefici per l'intera società, ma deve seguire determinati principi:

A. Una gestione etica dell'IA nelle relazioni internazionali deve ruotare innanzitutto attorno alla **trasparenza**: questo implica una chiara divulgazione delle **metodologie**, dei **criteri** e dei **dati utilizzati** dagli algoritmi, permettendo una comprensione e una verifica indipendente delle decisioni prese. Essere "aperti" su come gli algoritmi vengono utilizzati nelle decisioni che influenzano gli Stati può aiutare a costruire fiducia e comprensione tra i Paesi. Questo è particolarmente critico in scenari di diplomazia e negoziazione, in cui la percezione della parzialità o di informazioni riservate o soggette a limitazioni sulla circolazione dei dati può intensificare le tensioni esistenti. In questo senso, può diventare fondamentale **definire normative che obblighino la registrazione e la divulgazione dei sistemi di IA utilizzati a livello internazionale**.

B. In parallelo, la **garanzia di responsabilità, sicurezza e affidabilità delle decisioni *AI-oriented*** è cruciale. Nonostante i sistemi di Intelligenza Artificiale debbano operare in mondo affidabile e sicuro, garantendo i principi di *privacy* e sicurezza, i Paesi devono essere pronti a rispondere delle azioni intraprese sulla base delle raccomandazioni date all'IA, assicurando che esistano meccanismi robusti per la **revisione e il controllo delle decisioni automatizzate**. Questo principio garantisce che dietro ogni decisione assistita dall'IA vi sia una **"catena di responsabilità" chiara e tracciabile**. Ciò include l'identificazione degli operatori umani che supervisionano i sistemi di IA e la definizione delle procedure per il ricorso legale in caso di danni o errori. Per questo i governi dovrebbero implementare un quadro internazionale che regoli la responsabilità per gli errori di IA e fornisca linee guida su come gli individui e le nazioni possano adottare meccanismi correttivi. Un esempio può essere l'**istituzione di tribunali internazionali specializzati** o l'**integrazione di norme sulla responsabilità AI** nelle convenzioni esistenti.

C. Alla base di un uso responsabile dell'IA vi sono, infine, **equità e inclusività**. Le tecnologie basate sull'IA dovrebbero essere sviluppate e impiegate in modo da non discriminare tra Paesi o individui, né amplificare i *bias* esistenti. È quindi necessario un impegno costante per **rivalutare e ricalibrare gli algoritmi**, garantendo che le loro operazioni siano libere da pregiudizi. Da questo punto di vista, si dovrebbero definire politiche (ed eventualmente meccanismi di incentivazione) che promuovano la raccolta e l'uso di *dataset* di dati diversificati e più rappresentativi a livello internazionale.

Figura 26. I principi fondanti per un'applicazione responsabile e sostenibile dell'Intelligenza Artificiale nelle relazioni internazionali. *Fonte: elaborazione The European House – Ambrosetti, 2024*

Questi criteri devono essere contestualizzati all'interno di un *framework* per l'IA, anche Generativa, che non consenta la prevaricazione della "tecnica" sull'essere umano, ma possa valorizzarne le energie, la creatività e la capacità di esprimere valutazioni di carattere morale. Si tratta, quindi, di integrare l'**algoretica** nella rivoluzione dell'Intelligenza Artificiale, per fare convergere tra loro queste due dimensioni, **trasformando il valore morale in elementi computabili**.

La creazione di un quadro etico e legale che supporti l'uso responsabile dell'IA nelle relazioni internazionali, incoraggiando pratiche che rispettino i diritti umani e promuovano la cooperazione internazionale dovrebbe rientrare, anche a livello dei singoli Paesi, all'interno di **una strategia che coinvolga, oltre alle Istituzioni, il sistema imprenditoriale, il mondo accademico e della ricerca, i grandi *data center* e centri di calcolo**[44]. L'implementazione di queste politiche richiederà un coordinamento sostanziale tra i Paesi e le organizzazioni internazionali, ma è fondamentale per assicurare che l'Intelligenza Artificiale agisca come una forza propulsiva e positiva nelle dinamiche globali nella gestione e risoluzione di situazioni di crisi e nella definizione di soluzioni innovative a tutela della democrazia.

[44] Si pensi, nel caso italiano, al Centro Nazionale di Supercalcolo presso il Tecnopolo di Bologna, che accoglie dal 2022 il supercalcolatore "Leonardo" gestito da CINECA e dal Consiglio Nazionale della Ricerca.

Principali fonti bibliografiche di riferimento

- Agenda Digitale, "Crescono gli attacchi cyber in Italia, ma anche le difese: ecco il quadro", 2022
- American Enterprise Institute (AEI), "*The age of uncertainty - and opportunity: work in the age of AI*" (a cura di B. Orrell e D. Veldran), febbraio 2024
- Bitdefender, "*2024 Cybersecurity Outlook: navigating the geopolitical landscape*", 2024
- Brookings Institution, "*A cluster analysis of national AI strategies*" (a cura di J. Denford, G. Dawson e K. Desouza), dicembre 2023
- Brookings Institution, "*Twitter, the EU, and self-regulation of disinformation*", 2023
- Brookings Institution, "*The EU and U.S. diverge on AI regulation: a transatlantic comparison and steps to alignment*", 2023
- Brookings Institution, "*How can the U.S. can dominate in the race to national AI supremacy*" (a cura di G. Dawson e K. Desouza), febbraio 2022
- Brookings Institution, "*The geopolitics of AI and the rise of digital sovereignty*", 2022
- Brookings Institution, "*Police surveillance and facial recognition*", 2022
- Brookings Institution, "*How the NotPetya attack is reshaping cyber insurance*" (a cura di J. Wolff), dicembre 2021
- Brookings Institution, "*Artificial intelligence, geopolitics and information integrity*", 2020
- Built In, "*The future of AI: how Artificial Intelligence will change the world*", 2024
- CEPS, "*Germany's NetzDG: a key test for combatting online hate*", 2018
- CISA, "*Cybersecurity best practices*", 2024
- Clusit, "Rapporto Clusit sulla sicurezza ICT in Italia", edizioni 2016 – 2024
- Commissione Europea, "Una nuova strategia industriale europea per il settore della difesa: conseguire la prontezza dell'UE attraverso un'industria europea della difesa reattiva e resiliente", 5 marzo 2024
- Commissione Europea, "*Adequacy decisions*", 2024
- Commissione Europea, "*The 2022 code of practice on disinformation*", 2022
- Commissione Europea, "*Industry 5.0 - Towards a sustainable, human-centric and resilient European industry*", 2021
- CSIS, "*Digital dragnets: examining the government's access to your personal data*", 2022
- CubeCyber, "*Types of cyber threat actors and their motivations*", 2020
- Data Science Central, "*How Machine Learning is changing the world*", 2020
- Encyclopedia Britannica, "*Algorithms and complexity*", 2023
- European Audiovisual Observatory, "*Laws to combat manipulation of information finally adopted*", 2024
- Goldman Sachs, "*The generative world order: AI, geopolitics and power*", 2023
- Heimdal Security, "*Nation-state hacking – What you need to know*", 2022
- IBM, "*What is AI ethics?*", 2023

- IDSS, "*How algorithms impact society*", 2023
- Internet Encyclopedia of Philosophy (IEP), "*Ethics of Artificial Intelligence*", 2024
- ISC2, "*Enhancing cybersecurity through AI: a look into the future*", 2023
- Microsoft for Defense and Intelligence, "*Secure the digital defense ecosystem and improve interoperability*", 2023.
- Meta, "Disinformazione sottoposta a *fact-checking*", 2024
- Onfido, "*Identity Fraud Report 2024"*, 2024
- Pew Research Center, "*How Americans view data privacy*", 2023.
- Pew Research Center, "*Code-dependent: pros and cons of the algorithm age*", 2017
- Politico, "*Europe's new data protection rules export privacy standards worldwide*", 2018
- RAND, "*AI and Geopolitics*", 2023
- RAND, "*The motivations of cyber threat actors and their use and monetization of stolen data*", 2018
- Thales Group, "*Beyond GDPR: data protection around the world*", 2021
- The European House – Ambrosetti e Microsoft Italia, "AI 4 Italy: impatti e prospettive dell'intelligenza artificiale generativa per l'Italia e il *Made in Italy*", 2023
- The European House – Ambrosetti e Iren, "Materie prime critiche e produzioni industriali italiane. Le opportunità derivanti dall'economia circolare", 2023
- The Harvard Gazette, "*Great promise but potential for peril*", 2020
- U.S. Department of Defence, "*Digital transformation, AI important in keeping battlefield edge, leaders say*", 2022
- World Intellectual Property Organization (WIPO), "*Technology Trends 2019: Artificial Intelligence*", 2019
- VPNOverview, "*Big data and privacy: what is it and what are the risks?*", 2023

Questo Position Paper è stato curato dal Gruppo di Lavoro The European House - Ambrosetti formato da: Lorenzo Tavazzi (Senior Partner e Responsabile Area Scenari e Intelligence), Pio Parma (Senior Consultant Area Scenari e Intelligence e Project Leader), Claudio Conte (Analyst Area Scenari e Intelligence) e Leonardo Marconi (Analyst Area Scenari e Intelligence).

CAMERA DI COMMERCIO
VENEZIA GIULIA
TRIESTE GORIZIA

The European House
Ambrosetti

CON IL CONTRIBUTO DI

comune di trieste

Fondazione
FONDAZIONE CRTRIESTE

FONDAZIONE
Cassa di Risparmio di Gorizia

alpeadria
Global intermodal logistics

CON IL SOSTEGNO DI

INTESA SANPAOLO

CON IL PATROCINIO DI

REGIONE AUTONOMA
FRIULI VENEZIA GIULIA

UNIONCAMERE

COMUNE DI
GORIZIA

UNIVERSITÀ
DEGLI STUDI
DI TRIESTE

SISSA

MEDIA PARTNER

CORRIERE DELLA SERA
La libertà delle idee

WIRED