Intelligenza artificiale e sicurezza nazionale 2025

Come si relazionano intelligenza artificiale e sicurezza nazionale nel panorama in rapida evoluzione della sicurezza informatica globale? L'intelligenza artificiale rappresenta una rivoluzione con profonde implicazioni per la sovranità degli Stati e la protezione dei sistemi democratici, in un recente inserto "INTELLIGENCE FOOD FOR THOUGHT – L'altra intelligenza: tra opportunità e minacce" pubblicato dalla Presidenza del Consiglio dei Ministri – Sistema di Informazione per la Sicurezza della Repubblica italiana, analizza dettagliatamente questa "altra intelligenza", tracciando un quadro complesso di sfide e opportunità.

L'IA come tecnologia di rottura

L'intelligenza artificiale è ormai considerata una tecnologia "*general purpose*" che, come la macchina a vapore o l'elettricità in passato, non si limita a svolgere una specifica attività, ma trasforma radicalmente il modo di operare in molteplici settori. Questo carattere rivoluzionario spiega l'interesse delle agenzie di *intelligence* verso il fenomeno.

La rapidità con cui si è imposta è impressionante: mentre il telefono ha impiegato 75 anni per raggiungere 100 milioni di utenti, ChatGPT ha raggiunto lo stesso traguardo in appena 0,16 anni. Si stima che **entro il 2027 il mercato mondiale dell'IA raggiungerà i 407 miliardi di dollari**, con un potenziale incremento del PIL mondiale del 7% entro il 2033.

Minacce alla sicurezza informativa

Una delle principali preoccupazioni nell'ambito della cybersecurity riguarda l'uso distorto dei sistemi IA. Il

documento evidenzia come l'intelligenza artificiale possa potenziare minacce già esistenti, come gli attacchi informatici e la disinformazione, creando scenari inediti di rischio.

"*L'IA generativa ha creato le condizioni per generare notizie fasulle, immagini finte, audio e video falsi (deepfake)*", si legge nel rapporto. "*Non si tratta di un gioco: si altera la correttezza dell'informazione e della comunicazione*". Questa capacità di manipolare l'informazione rappresenta una minaccia concreta per i processi democratici, come dimostrato dal fatto che nel 2024 metà della popolazione mondiale è stata chiamata a votare.

Disinformazione e democrazia

Un aspetto particolarmente preoccupante emerso dall'analisi è l'uso dell'intelligenza artificiale come strumento di amplificazione della disinformazione nelle campagne elettorali. Il documento cita l'adozione del "*Collective Response Framework*", un meccanismo adottato dai Paesi G7 nel dicembre 2024 per fornire una risposta coordinata agli attacchi di disinformazione contro gli apparati democratici.

Significativa anche la precisazione che:

> *"l'intelligenza artificiale non è solo un potenziale strumento di amplificazione della disinformazione. Essa stessa è intossicabile: dipende dalla natura dei dati sui quali svolge il suo processo di apprendimento".*

Applicazioni militari

Il rapporto dedica un'ampia sezione alle applicazioni militari dell'IA, mappando 18 aree di potenziale utilizzo, dalla logistica al comando e controllo, dall'addestramento all'analisi dell'ambiente operativo. Particolarmente sensibili risultano gli ambiti dell'analisi degli obiettivi, la valutazione dell'impatto delle missioni e la stima dei danni

collaterali.

Emerge chiaramente come l’integrazione dei sistemi IA nelle operazioni militari stia ridefinendo le dinamiche di sicurezza globale, con implicazioni significative per gli equilibri geopolitici.

Divario digitale e geopolitica dell’IA

Un altro elemento critico evidenziato nel documento è il cosiddetto “*AI divide*“, ovvero la disparità nella capacità di accedere all’intelligenza artificiale tra le diverse aree del mondo. L’Oxford Insights Government AI Readiness Index mostra come Nord America, Europa e Asia Orientale occupino le prime posizioni, mentre i Paesi dell’Africa Subsahariana registrino i punteggi più bassi.

Sul piano geopolitico, gli Stati Uniti mantengono la leadership mondiale negli investimenti e nell’innovazione IA (punteggio 100 nel Global AI Index), seguiti dalla Cina (53,88) ancora notevolmente distanziata. Il primo Paese europeo è il Regno Unito (quarto nel mondo), mentre la Francia guida gli Stati membri UE.

Regolamentazione e governance

Di fronte a questi scenari complessi, il documento sottolinea l’importanza di una governance internazionale basata su due parole chiave: etica e inclusione. Il G7, in particolare, ha ribadito la centralità dell’uomo nell’approccio all’intelligenza artificiale, promuovendo il rispetto dei valori democratici anche in questo settore.

In questo contesto, l’Unione Europea ha approvato l’AI Act, che identifica quattro livelli di rischio per i sistemi IA (basso, limitato, alto, inaccettabile), con i conseguenti

adempimenti, obblighi o divieti. Il regolamento definisce un sistema di IA come un “sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione”.

L’intelligenza artificiale come frontiera della sicurezza nazionale

Un’analisi più dettagliata del documento del Sistema di Informazione per la Sicurezza della Repubblica italiana rivela ulteriori sfaccettature di questa complessa relazione.

La struttura economica dell’IA e le implicazioni per la sicurezza

L’economia dell’intelligenza artificiale si articola attorno a tre fattori principali: i dati (le “materie prime”), gli algoritmi (il “lavoro”) e le infrastrutture computazionali (il “capitale”). Questa tripartizione evidenzia vulnerabilità specifiche per la sicurezza nazionale:

1. **La questione dei dati**: La dipendenza dai dati solleva interrogativi sulla proprietà intellettuale e sulla sovranità digitale. Il documento sottolinea come i contenziosi sulla proprietà dei dati utilizzati per addestrare i sistemi IA siano di “fondamentale importanza ai fini della tutela dei diritti d’autore”. Questo aspetto ha implicazioni dirette per la sicurezza informativa e l’autonomia tecnologica degli Stati.
2. **La concentrazione del capitale**: Le dinamiche di mercato mostrano una crescente concentrazione in grandi gruppi industriali privati, principalmente americani e cinesi. Il documento evidenzia come “le future dinamiche del mercato potranno confermare se il panorama del ‘capitalismo dell’IA’ corra il rischio dell’oligopolio o esso sia già una certezza”. Questa tendenza solleva preoccupazioni sulla resilienza delle catene di

approvvigionamento tecnologico e sulla dipendenza strategica.

Protezione del know-how tecnologico: una priorità nazionale

Il rapporto dedica particolare attenzione alla tutela del patrimonio di conoscenze scientifiche e tecnologiche. I dati sui brevetti mostrano un quadro allarmante: dal 2017, la Cina supera ogni anno gli Stati Uniti nel numero di brevetti concessi nel campo dell'IA, mentre l'Europa risulta sempre più marginale.

Particolarmente significativo è il divario nei "*Foundation Models*", i modelli avanzati che consentono lo sviluppo di sistemi IA multimodali: nel 2023, il **70% circa dei modelli rilasciati proveniva dagli USA, contro il 12% della Cina e solo il 9% dell'Europa**. Questa disparità configura una vulnerabilità strategica per chi non dispone di autonomia in questo settore, con ripercussioni dirette sulla sicurezza cibernetica nazionale.

Manipolazione dell'informazione: la nuova frontiera delle minacce ibride

Il documento approfondisce le modalità attraverso cui l'IA può alterare l'ecosistema informativo, evidenziando come le tecnologie digitali di ultima generazione stiano ampliando le capacità offensive di attori ostili. La creazione di contenuti a scopi propagandistici diventa più sofisticata e difficile da rilevare, incidendo sull'equilibrio tra sicurezza nazionale e libertà fondamentali.

"*In un'ottica di bilanciamento*", si legge nel rapporto, "deve essere chiaro il discrimine esistente tra ciò che merita un effettivo intervento da parte degli apparati di sicurezza e quello che, al contrario, deve essere rimesso al giudizio dei fruitori dei contenuti". Questa distinzione è cruciale per evitare derive autoritarie nel contrasto alla disinformazione.

Il documento sottolinea inoltre la necessità di maggiore trasparenza sui "*criteri con cui vengono allenati gli algoritmi per il controllo dei contenuti pubblicati sul web*", evidenziando l'importanza della "*garanzia del contraddittorio per gli utenti 'sanzionati'*". Un approccio equilibrato che riflette la complessità della minaccia.

Contromisure tecniche e normative per la protezione cibernetica

L'analisi identifica diverse linee d'azione per rafforzare la resilienza dei sistemi nazionali di fronte alle minacce potenziate dall'IA:

- **Meccanismi di autenticazione e provenienza dei contenuti**: Il Codice di Condotta adottato dal G7 a Hiroshima nel 2023 prevede esplicitamente lo "*sviluppo e implementazione di meccanismi affidabili di autenticazione e provenienza dei contenuti, come la filigrana o altre tecniche per consentire agli utenti di identificare i contenuti generati dall'IA*".
- **Controlli di sicurezza rigorosi**: Il documento raccomanda "*investimenti e implementazione di controlli rigorosi di sicurezza, tra cui la sicurezza fisica, la sicurezza informatica e le misure di salvaguardia verso le minacce interne in tutto il ciclo di vita dell'IA*".
- **Sistema di monitoraggio dell'aderenza ai principi etici**: Si sottolinea l'importanza di implementare "*un sistema di monitoraggio che consenta di 'misurare' l'effettiva aderenza dei sistemi IA ai Principi guida*" stabiliti a livello internazionale.

Il futuro dell'IA e le frontiere della ricerca sulla sicurezza

Il documento identifica tre ambiti di frontiera che potrebbero ridefinire radicalmente il panorama della sicurezza:

1. **L'intelligenza artificiale generale (AGI)**: Lo sviluppo

di sistemi IA con funzioni cognitive di ordine superiore, capaci di svolgere attività per le quali non sono stati specificamente addestrati, rappresenta una discontinuità potenzialmente rivoluzionaria.
2. **L'interazione tra sistemi IA e sistemi biologici**: Lo sviluppo di architetture informatiche neuromorfiche basate non solo sulle tecnologie del silicio ma anche su sostanze organiche apre scenari inediti di convergenza tra intelligenza artificiale e biologia.
3. **I computer quantistici e l'IA quantistica:** L'avvento dei computer quantistici rappresenta una minaccia diretta per gli attuali standard crittografici, ma offre anche nuove prospettive di calcolo e apprendimento che potrebbero rivoluzionare la sicurezza informatica.

Il rapporto con il mondo dell'informazione e la sicurezza cognitiva

Un aspetto particolarmente rilevante per la sicurezza nazionale è l'impatto dell'IA sull'ecosistema dell'informazione. Il documento evidenzia come il web e i *social network* siano diventati la principale fonte di reperimento delle informazioni, con i motori di ricerca (basati su algoritmi IA) che fungono da intermediari primari.

In questo contesto, "*l'accesso all'informazione rischia di essere in futuro regolato più dalle piattaforme tecnologiche che dagli editori o dagli autori*", con conseguenze potenzialmente destabilizzanti per i principi di indipendenza e interesse pubblico che fondano il sistema informativo nelle società democratiche.

Particolarmente allarmante è la constatazione che "*non c'è più bisogno di un giornalista (vero) per costruire e diffondere una notizia falsa. Un buon informatico, una rete neurale e un 'suggeritore' dell'obiettivo da colpire sono sufficienti per costruire campagne stampa artificiali*". Questa evoluzione configura una vulnerabilità sistemica per la "sicurezza

cognitiva” delle democrazie, richiedendo contromisure che vadano oltre gli approcci tradizionali alla cybersecurity.

Verso un approccio integrato alla sicurezza nell’era dell’IA

L’analisi approfondita del documento evidenzia come l’intelligenza artificiale stia ridefinendo il concetto stesso di sicurezza nazionale, richiedendo un approccio più integrato che comprenda dimensioni tecniche, economiche, normative e cognitive.

Come suggerito dalla citazione di Francisco Goya nell’illustrazione che accompagna il documento (“Il sonno della ragione genera mostri”), la sfida principale consiste nel mantenere un controllo razionale e democratico su uno sviluppo tecnologico di portata epocale. Solo attraverso una governance multilivello, che bilanci innovazione e protezione, sarà possibile navigare le acque turbolente dell’era dell’intelligenza artificiale preservando al contempo i valori fondamentali delle società libere.

La sicurezza nazionale nell’era digitale non può più essere concepita come mera difesa perimetrale, ma deve evolvere verso una protezione olistica degli interessi vitali dello Stato, inclusa la salvaguardia dell’integrità del tessuto informativo e cognitivo che sostiene il funzionamento delle istituzioni democratiche.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/intelligenza-artificiale-e-sicurezza-nazionale/