Guerra e Intellgenza Artificiale

Chi è appassionato di cinema conoscerà un film degli anni ’80 intitolato “War Games”, giochi di guerra. Si racconta la storia di un ragazzo, genio dell’informatica, che si ritrova alle prese con un supercomputer intelligente della Difesa Usa che ne gestisce l’arsenale nucleare: Wopr, acronimo di War Operation Plan Response. L’intelligenza artificiale dello Wopr è collegata direttamente ai silos di lancio dei missili intercontinentali statunitensi, e per una serie di disavventure, e imperfezioni del sistema, il mondo corre il rischio di andare incontro all’olocausto nucleare. Non sveliamo la fine, per coloro i quali ancora non avessero visto il film, ma la pellicola offre una perfetta introduzione per una problematica che, negli ambiti militari, è più che mai attuale e, financo, che necessita di risoluzione impellente.
L’intelligenza artificiale, ed in particolare quella con capacità Machine Learning (traducibile come “apprendimento automatico”), è ormai una realtà nello strumento militare dei Paesi più tecnologicamente avanzati. Questa piccola rivoluzione, che, come vedremo, non è affatto una novità storicamente parlando, comincia ad attirare le attenzioni anche di quei ricercatori, analisti e personale militare, che si occupano e gestiscono i sistemi d’arma nucleari.

Il Csis (Center for Strategic & International Studies) ha recentemente pubblicato un piccolo dossier che pone l’attenzione proprio su questo aspetto: come si può integrare l’intelligenza artificiale, anche con capacità Ml, nella gestione degli arsenali nucleari.
Il rapporto esclude immediatamente la possibilità, espressa nel film già citato, che un sistema di questo tipo possa gestire autonomamente il lancio di missili atomici: un futuro che “dovremmo evitare”, viene detto. Però esistono altri campi di impiego per l’Ia nel settore nucleare che andremo ad analizzare cercando di spiegarne i possibili rischi ed implicazioni di carattere strategico.
Cominciamo col dire che l’Ia, nelle sue forme più basiche, è qualcosa che esiste da decenni: è emersa, a livello di studi accademici, sin dagli anni ’50 ed ha avuto una storia caratterizzata da alterne vicende a seconda delle “infatuazioni” o meno di progettisti e ricercatori. Da allora, però, l’intelligenza artificiale è cresciuta e ora comprende una vasta gamma di campi come le Ml, il ragionamento automatico, la robotica, l’elaborazione del linguaggio naturale, la computer vision e molti altri. Per quanto ci riguarda risulta interessante proprio l’aspetto del Machine Learning, inteso come quel processo che utilizza modelli, o algoritmi, per fare previsioni utili o prendere decisioni usando una serie di dati rilevanti per risolvere un determinato problema o compito.
Oggi sistemi informatici Ml sono ovunque. Banalmente basti pensare ad un filtro antispam: il sistema, in base alle nostre scelte (ma anche in modo automatico preimpostato), riconosce quelle mail considerate spazzatura e autonomamente le elimina dalla nostra casella di posta in arrivo. Un sistema Ml eccelle nella risoluzione di un particolare tipo di problemi: individuazione delle anomalie, classificazione, raggruppamento e generazione di dati, ottimizzazione, classificazione ecc. L’applicazione della Ml in un mondo reale, o in un ambiente incontrollato,

resta però solo sperimentale. I ricercatori sono consci, infatti, che ambienti incontrollati o particolarmente ricchi di dati "stressano" e "mettono sotto tensione" i sistemi Ml.
I sistemi a intelligenza artificiale, infatti, sono ben lontani dall'essere a prova di errore, e l'introduzione della Ml introduce nuove vulnerabilità. Uno studio Microsoft del 2019 individuava due tipologie di "errori" per le Ml: quelli intenzionali, che risultano da sforzi "attivi" di soggetti avversari, e quelli non intenzionali, che sono tecnicamente corretti dal punto di vista della logica del sistema ma sono sbagliati da quello dell'applicazione dello stesso. Per quanto riguarda le interferenze esterne, una sistema Ml può essere facilmente messo "fuori strada" attraverso l'immissione di input "maligni" nel sistema di basi di dati, che la macchina non è in grado di riconoscere come tali. In particolare, si legge, le reti neurali sono quelle a più alto rischio per quanto riguarda questa tipologia di attacco, pertanto è necessario ripensare alla protezione e messa in sicurezza delle fonti dei dati per evitare questo "inquinamento" volontario: un aspetto di non facile risoluzione in quanto viviamo in un mondo in cui la maggior parte di esse sono fonti aperte (open source), consultabili e modificabili da chiunque.
Per quanto riguarda l'argomento della nostra trattazione è risaputo che la tecnologia degli armamenti atomici è quella più "conservatrice" in assoluto e caratterizzata da un approccio "lento" riguardante l'integrazione di nuovi sistemi, a fronte della velocità a cui corre il resto del mondo, non solo militare. Proprio questa velocità di espansione delle tecnologie Ai/Ml nel settore della Difesa al di fuori dell'ambito nucleare impone, per via dell'intrinseca correlazione tra i settori, che questo aspetto venga preso in carico dai decisori politici e dai gestori degli arsenali atomici.

Questo lungo cappello introduttivo è funzionale per arrivare all'analisi fatta dal Csis, i cui ricercatori hanno individuato quattro ambiti nel campo della Nc3 (Nuclear Command, Control and Communications) in cui l'Ia può essere introdotta, escludendo quindi a priori quello dell'autorizzazione all'utilizzo, come già detto.

Il primo riguarda la sicurezza e la difesa delle installazioni. La difesa delle basi, dei sistemi, e delle testate stesse sia dagli attacchi informatici sia da quelli fisici, è vitale per la sopravvivenza di un arsenale atomico al pari delle porte corazzate dei silos di lancio. L'intelligenza artificiale, in questo senso, potrebbe intervenire nella sorveglianza dei siti, attraverso sensori elettro-ottici o video, e provvedere al monitoraggio, identificazione e inseguimento dei bersagli, fino all'intervento dell'uomo. L'Ia può anche svolgere il ruolo di pattugliamento automatico dei sistemi rilevando i tentativi di intrusione cibernetica, individuando i malware monitorando l'attività in rete, fornendo la mappatura delle sorgenti degli attacchi e rispondendovi automaticamente. Esistono però delle vulnerabilità: un sistema video ad Ia, ad esempio, può essere ingannato semplicemente indossando abiti particolari, oppure un sistema che si basa su un database di foto può essere messo fuori strada semplicemente inserendovi immagini ad hoc.

Il secondo ambito riguarda l'attività di intelligence e di allarme precoce. In un mondo dove le immagini satellitari di tipo commerciale sono sempre più precise e accessibili, mettendo in atto una vera e propria rivoluzione dell'intelligence geospaziale (Geoint) in quanto fotografie in tempo reale (o quasi) sono immediatamente disponibili sul mercato, l'Ia può diventare uno strumento efficace per la raccolta delle informazioni sui bersagli proprio per la sua capacità di vagliare un'enorme mole di dati in poco tempo. Un utilizzo di Ai/Ml, infatti, può essere la determinazione dei bersagli per i missili nucleari, che diventa particolarmente efficace se

pensiamo agli assetti terresti mobili degli avversari: Russia, Cina e Corea del Nord, ad esempio, posseggono un buon numero di Icbm (Intercontinental Ballistic Missile) su mezzi ruotati o su ferrovia in grado di essere dispersi lungo il territorio. Un sistema Ml, sfruttando la ricognizione satellitare, potrebbe prevedere i probabili siti di lancio di questi veicoli, addirittura individuando le possibili strade percorse, i periodi di manutenzione e lo stato di allerta, facilitando quindi l'assegnazione dei bersagli per le testate. Questa capacità, però, potrebbe alterare l'equilibrio strategico: la capacità di colpire con una maggiore sicurezza i sistemi nucleari avversari potrebbe aumentare la fiducia nell'efficacia di un "primo colpo" (first strike) e soprattutto potrebbe indurre l'avversario a intraprendere azioni volte a salvaguardare la propria capacità di deterrenza atomica, magari anche colpendo per primo. In ogni caso sembra che la necessaria completezza di informazioni (geografiche e temporali) per una simile eventualità non sia realisticamente ottenibile.

Il terzo ambito è rappresentato dalla modellizzazione, simulazione, ottimizzazione e analisi di dati. L'Ia può affrontare con successo le miriadi di ottimizzazioni e problemi analitici riguardanti l'impiego degli arsenali nucleari e la deterrenza strategica. Simulazioni e modellizzazioni permettono all'uomo di affrontare meglio un fenomeno, e in questo senso i il "wargaming", i giochi di guerra, sono preziosi ambiti in cui l'Ia può intervenire per esplorare il comportamento avversario sul campo di battaglia. Non solo. L'Ia può subentrare anche nei processi di valutazione di un sistema d'arma (banalmente effettuando dei test virtuali) affiancando le prove effettuate nel mondo reale. Una Ml, poi, può perfino adoperarsi nella progettazione stessa di una nuova arma: potrebbe infatti sviluppare autonomamente, in base ai dati che utilizza, nuovi missili, determinare il peso o la grandezza ottimale di un veicolo di rientro, definire la potenza della testata e anche ottimizzare tutta la filiera produttiva. Ancora in questo ambito, dato che le nazioni utilizzano i dati raccolti sugli armamenti avversari per stilare i propri piani operativi, l'Ia diventerebbe parte fondamentale per ottimizzare l'utilizzo delle testate nucleari ed effettuare un'accurata selezione dei bersagli. Anche in questo caso il rischio è che si incappi in uno sbilanciamento dell'equilibrio strategico minando la capacità dell'avversario di effettuare un secondo colpo.

Il quarto e ultimo ambito riguarda la logistica. Questo, potenzialmente, è quello più impattante e che dovrebbe avere la priorità stante l'attuale situazione dell'arsenale atomico statunitense. Nel 2014, infatti, un rapporto del Dipartimento della Difesa aveva evidenziato come le operazioni di manutenzione e logistiche per mantenere le armi atomiche in efficienza avevano raggiunto il "punto di rottura" richiedendo sempre più personale che veniva impiegato in turni sempre più lunghi. Da allora, si legge, sono stati fatti dei progressi, ma dato che l'arsenale atomico occupa solo una piccola frazione della catena logistica statunitense, spesso cade in fondo alla scala delle priorità della Difesa. L'Ia potrebbe intervenire in modo efficace andando a snellire i tempi di approvvigionamento della logistica e soprattutto prevedendo con una ragionevole certezza la fine della "vita operativa" delle varie componenti, in modo da velocizzare la loro sostituzione che avverrebbe prima della loro rottura. Quanto già avviene per gli elicotteri Blackhawk grazie al programma Joint Artificial Intelligence Center (Jaic).

Gli Stati Uniti, quando si tratta di Ia/Ml, hanno scelto di mantenere l'uomo al termine ultimo della catena decisionale: quello che in gergo si chiama Human-in-the-loop, ma il rapporto ricorda che altre nazioni non sembrano essere orientate nella stessa direzione: viene citato, infatti, come la

Russia sia prossima a mettere in servizio un sistema sottomarino automatico nucleare, il famoso supersiluro Poseidon, già noto come Status-6 o Kanyon. Viene anche sottolineato come, attualmente, il ricorso ad Ia/Ml nel campo nucleare ponga più incertezze che altro, essendo sostanzialmente un sistema ancora “immaturo” per adattarsi a tale settore in modo pervasivo come avvenuto in altri. La ricerca pertanto deve concentrarsi nell’eliminare gli “errori”, che siano nei dati o nel modo di “pensare” che hanno le macchine, affinché l’incertezza venga totalmente eliminata o ridotta ai minimi termini. La “comunità nucleare”, quindi, deve dare priorità allo studio e all’analisi dell’Ai/Ml nei campi qui individuati per meglio comprendere i rischi tecnici e quelli connessi alla possibile escalation che ne deriverebbe, senza dimenticare quindi le interconnessioni che esistono tra il dominio tecnico e quello strategico.