Intelligenza artificiale e irresponsabilità umana: l'IA sul campo di battaglia

di *Francesca Farruggia* e *Maurizio Simoncelli*

L'Intelligenza Artificiale (IA) sta trasformando, se non rivoluzionando, sempre più la nostra società offrendo molteplici e rilevanti opportunità in tutti i settori. L'IA è in via di larga e crescente applicazione anche nel settore militare. I mass media li chiamano con un termine ad effetto i "killer robot", facendo venire in mente i film hollywoodiani tipo "Robocop" o "Terminator". Non siamo ancora a quel livello, ma almeno sperimentalmente sono già una realtà in ambito industriale e militare presso numerosi stati, dagli USA alla Russia, dalla Francia alla Gran Bretagna, dalla Corea del Sud ad Israele. L'utilizzo di armi autonome appartiene dunque a un non lontano futuro. Gli Stati Uniti impiegano ad oggi sistemi d'arma semi-autonomi come i missili antinave a lunga gittata che hanno sì bisogno dell'intervento umano per identificare il bersaglio, ma agiscono in piena autonomia nello scegliere come distruggerlo, o come la nave anti-sottomarino Sea Hunter che può navigare per mesi senza equipaggio. Israele invece utilizza un drone, Harpy, che senza l'intervento umano è in grado di individuare ed annientare sistemi radar.

Da alcuni anni ingenti risorse vengono destinate dai governi interessati in questo settore, che appare destinato ad una crescita esponenziale, tanto che le previsioni per l'impatto economico dell'IA (civile e militare) si aggirano intorno ai $ 13 trilioni entro il 2030.

Quali sono i vantaggi legati all'utilizzo di queste armi? L'interesse destato dai *Lethal Autonomous Weapons Systems* (LAWS) presso vari governi e stati maggiori è giustificato con molteplici motivi (maggiore precisione negli attacchi rispetto a quella umana, elevata rapidità reattiva ad un attacco subito, assenza di stress emotivo umano, riduzione dei danni collaterali nel rispetto del diritto umanitario internazionale, regole d'ingaggio più stringenti ecc.). D'altro canto, si può opporre che le minori perdite di vite dei propri militari potrebbero incentivare sia l'acquiescenza dell'opinione pubblica, sia quella dei decisori politici verso nuovi conflitti armati, fondandosi sulla convinzione di una guerra combattuta solo dalle macchine.

Allo stato attuale l'IA presenta tuttavia ancora forti limiti. Diverse sperimentazioni, utilizzando la metodologia di *adversarial testing*, hanno messo in rilievo come la rete neurale possa essere indotta in errore, scambiando uno scuolabus e un cane per un'ostrica o una tartaruga per un fucile. Analogamente l'analisi del processo di machine learning (ML) ha fatto emergere alcuni punti critici che non possono essere trascurati, tanto che risulta assai rischioso affidarsi a tali tecniche come unico strumento decisionale, stando almeno ai livelli tecnologici attuali. Emergono elevati rischi connessi sia ad un'azione offensiva avversaria che con varie modalità può indurre in errore il sistema, sia a malfunzionamenti interni e difficilmente prevedibili dell'IA dovuti ai propri processi di autoapprendimento e al complesso funzionamento degli algoritmi. Inoltre, dati i costi relativamente ridotti della robotica e dell'IA, potrebbero svilupparsi non solo una nuova corsa al riarmo coinvolgente un numero elevato di stati, ma anche una diffusione di tali sistemi d'arma presso milizie irregolari e formazioni terroristiche, con conseguenze imprevedibili sulla sicurezza interna ed esterna. Se poi consideriamo anche i progressi nel settore delle stampanti 3D e i pericoli connessi all'evoluzione tecnologica e dei materiali, i rischi appaiono ancora più incombenti.

Certamente l'uso di sistemi d'arma autonomi comporterebbe una trasformazione radicale nella gestione dei conflitti, con l'ineludibile sovvertimento del quadro in ambito etico, giuridico, comportamentale e operativo.

Dal punto di vista giuridico, i LAWS devono comunque fare riferimento sia all'ottemperanza delle norme del diritto internazionale umanitario, sia al mantenimento della catena delle responsabilità nelle azioni belliche, sia alla questione etica rappresentata dal rispetto della dignità degli esseri umani coinvolti nel conflitto. Da un lato, infatti, risulta difficile immaginare come la robotica e l'intelligenza artificiale potranno sviluppare sistemi capaci di distinguere tra combattenti e popolazione civile, fra bersagli leciti e illeciti, fra prigionieri di guerra, internati civili e detenuti comuni. Dall'altro lato, presupponendo l'uso di capacità cognitive ed emotive, nonché di competenze sociali ed esperienziali, è difficile pensare che l'IA sarà in grado di valutare

se, quale e quanto una determinata azione configuri un vantaggio militare, in relazione alle perdite umane e ai danni alla popolazione civile, ai beni patrimoniali e a quelli culturali, così come ai beni civili, incidentalmente causati. L'utilizzo dei killer robots non garantirebbe inoltre il rispetto della dignità umana: le decisioni sulla vita o la morte in un conflitto armato richiedono intuizione e compassione, virtù che le macchine non potranno mai possedere.

Quale vaccino potrà debellare questo virus che incombe sulla nostra società? Ad oggi solo forti pressioni da parte della società civile, come il lancio nel 2013 della Campagna *Stop Killer Robots* da parte di un gruppo di Organizzazioni non governative (Ong) guidate dalla Human Rights Watch (HRW), hanno fatto sì che il tema delle armi autonome sia stato incluso, a partire dal 2016, all'interno dell'agenda della Conferenza di riesame della *Convention on Certain Conventional Weapons* (CCW). La Quinta Conferenza di riesame della CCW tenutasi a Ginevra nel 2016 ha infatti deciso di creare un gruppo di "esperti governativi" con il compito di valutare le tecnologie emergenti nel campo delle armi autonome letali (LAWS). La posizione dei governi sulla materia è però ambivalente, mentre è più netta, seppur non unanime, la posizione della comunità scientifica sull'applicazione dell'intelligenza artificiale all'industria della difesa. La previsione di drammatiche conseguenze derivanti dallo sviluppo di "robot killer" ha portato circa 4.500 ricercatori di varie discipline (in particolare quelle collegate a informatica, robotica, intelligenza artificiale) a redigere un appello per la messa al bando delle armi completamente autonome, ritenute "moralmente inaccettabili". Nel maggio del 2018 forte è stata anche la posizione presa dai dipendenti di Google che hanno manifestato in massa contro il supporto che l'azienda stava offrendo al Pentagono nello sviluppo di droni dotati di intelligenza artificiale, tanto da indurla a non rinnovare il contratto con il Dipartimento della Difesa americano.

Ad oggi 30 Paesi hanno chiesto la messa al bando delle LAWS, ma il dibattito è in corso e un eventuale accordo globale è ancora lontano. C'è da auspicare e da mobilitarsi affinché a livello mondiale i governi prendano atto dell'opposizione pubblica allo sviluppo di sistemi d'arma che sfidano tanto il buon senso quanto il senso comune, sottraendo sia ai politici, in quanto decisori, sia ai militari, in quanto esecutori, la più delicata e grave delle loro responsabilità.

Per approfondimenti vedi un recentissimo studio dell'Istituto di Ricerche Internazionali Archivio Disarmo intitolato *LAWS Lethal Autonomous Weapons Systems. La questione delle armi letali autonome e le possibili azioni italiane ed europeeper un accordo internazionale in materia*, che mette in evidenza non solo il quadro della R&S del settore e le questioni giuridiche, ma anche l'attuale inaffidabilità di tali tecnologie, rilevando come i sistemi di IA siano vulnerabili a tutti gli attacchi cibernetici che sfruttano vulnerabilità dei normali sistemi informatici. https://www.archiviodisarmo.it/view/K0Y2nX8-UWjKHNM9OQ83o96Kv0-oDTrYQW5IYIxM1dE/iriad-review-luglio-agosto.pdf