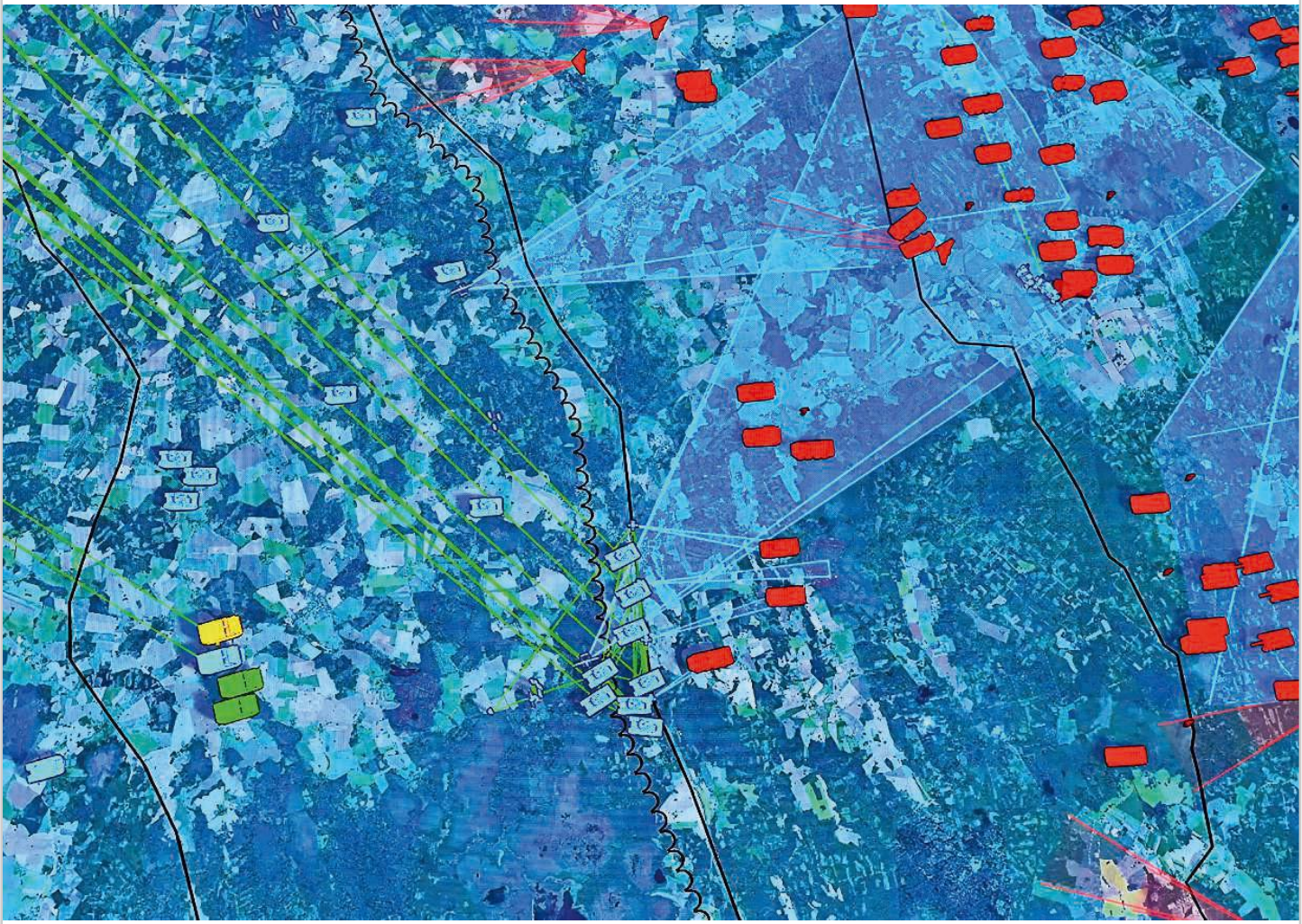
ELLE

diffusione:116015
tiratura:149118



1250 target raggiunti in 48 ore, droni sempre più sofisticati, le gerarchie di un intero Paese eliminate: l'IA sta cambiando volto ai conflitti in modo impressionante e le conseguenze potrebbero toccarci da vicino. Ne abbiamo parlato con *Mariarosaria Taddeo*, esperta di etica delle tecnologie digitali di difesa.

Algoritmi *di guerra*

Testo di
ADELAIDE BARIGOZZI

ELLE

diffusione:116015
tiratura:149118

Nelle prime 48 ore di attacco all'Iran, stando alle trionfanti comunicazioni ufficiali del Pentagono, gli Stati Uniti hanno colpito oltre 1.250 obiettivi, una capacità distruttiva impensabile solo pochi anni fa. A fare la differenza è stato l'utilizzo bellico dell'intelligenza artificiale come mai prima d'ora. Un'accelerazione che, anche al netto di eventuali considerazioni pacifiste, solleva non pochi dubbi che hanno a che fare con l'etica, il diritto internazionale, la gestione delle informazioni sui target e il concetto di responsabilità umana quando a uccidere sono le macchine. Proprio i temi di cui si occupa Mariarosaria Taddeo, docente di Digital Ethics and Defence Technologies all'Oxford Internet Institute dell'Università di Oxford, nonché autrice del saggio *Codice di guerra. Etica dell'intelligenza artificiale nella difesa* (Raffaello Cortina). «L'IA sta ridefinendo non solo il modo in cui vengono condotte le guerre, ma anche il funzionamento delle organizzazioni della difesa, i processi decisionali e operativi, le acquisizione di dati, le tattiche e le strategie», osserva l'esperta. Una rivoluzione che potrebbe non riguardare solo le popolazioni che hanno la sfortuna di vivere sul lato "sbagliato" di un confine. Se i film di fantascienza ci avevano preparati a eserciti di robot assassini, la realtà si presenta assai più inquietante e letale: una nuova generazione di armi intelligenti, ma non infallibili – vedi la scuola elementare iraniana colpita da un missile americano il 28 febbraio – droni, dispositivi d'arma autonomi (Aws), e sistemi di IA per l'intelligence (AIA) capaci di individuare centinaia di target in pochi minuti come Claude di Anthropic e Maven di Palantir, hanno già cambiato il modo di fare la guerra. Ne abbiamo parlato con Taddeo.

Il conflitto in Iran sta rivelando in modo plateale l'impatto dell'uso dell'IA in guerra, con un'accelerazione impressionante delle operazioni belliche. Quali sono le conseguenze di questa profonda trasformazione, che tutti noi cittadini dovremmo sapere?

Come cittadini dovremmo cercare di sapere tutto, perché purtroppo la guerra costituisce un elemento preponderante delle nostre società. Gli aspetti da considerare sono diversi. Il primo riguarda la mole di dati che produciamo. L'IA nella difesa arriva dopo anni di trasformazione digitale in ogni settore che ha generato enormi quantità di informazioni. Sono un po' come dei grandi pagliai, nei quali si nascondono gli aghi, ovvero le informazioni rilevanti, che in guerra sono fondamentali. Ebbene, l'IA ci permette di estrarre questi aghi da infiniti pagliai. A volte, si tratta di identificare un cittadino, altre capire quale sistema colpire con un attacco cibernetico, altre ancora, come abbiamo visto fare dagli Usa in Iran, individuare i target. E tra non molto, l'IA potrebbe anche guidare del tutto autonomamente un'arma letale, decidendo chi uccidere e cosa attaccare. I problemi etici, quindi, sono diversi e vanno dalla tutela della privacy e dell'anonimato dei cittadini all'attribuzione di responsabilità morale. Problemi resi più stringenti dal fatto che sull'IA abbiamo un limitato controllo.

In che senso la controlliamo poco?

È molto intelligente, apprende dalle interazioni con l'ambiente, ma può imparare anche qualcosa che non avremmo voluto e, a volte, arriva a conclusioni impreviste. In più, è una tecnologia poco robusta, sopporta male gli shock. Se, per esempio, sviluppiamo un sistema di IA su un set di dati e poi la usiamo in un diverso contesto, può comportarsi in modi inaspettati e questo è un problema, perché i comportamenti inattesi limitano il controllo, che in guerra è tutto. Per esempio, è essenziale per distinguere tra combattenti e civili o, meglio, non combattenti, i quali secondo l'etica e le leggi di guerra non vanno mai intenzionalmente esposti al pericolo, mentre i report della Croce Rossa e dell'Istituto per il Disarmo delle Nazioni Unite ci dicono che i civili colpiti in zone di guerra sono in aumento.

Dunque, "il Paese più potente del mondo", secondo le parole di Donald Trump, si sta affidando a una tecnologia letale imprevedibile?

Gli Stati Uniti non sono l'unico Paese a usare l'IA nella difesa. È un processo ormai inevitabile e non reversibile. L'intelligenza artificiale offre un vantaggio competitivo spesso irrinunciabile. Tutti i Paesi della Nato la stanno adottando. Nel farlo, però, ci si sta in effetti affidando a una tecnologia poco prevedibile. Questo livello d'incertezza può essere ridotto migliorando i processi in cui l'IA è integrata, creando le condizioni per un migliore controllo da parte degli ufficiali, scegliendo modelli più trasparenti e robusti di altri, decidendo a monte quali decisioni non delegare alle macchine. Insomma, dovremmo usarla senza fidarcene. Il problema è che noi esseri umani inciampiamo spesso nel cosiddetto tech bias: raramente mettiamo in discussione ciò che ci dice la macchina.

Come scrive nel suo saggio, emerge anche un problema di responsabilità.

È un problema etico molto serio. La guerra è una delle peggiori attività che gli esseri umani possono intraprendere, però a volte è necessaria o, quantomeno, giustificabile in caso di difesa, come nel caso dell'Ucraina. È però indispensabile stabilire dei limiti oltre i quali si sconfina nell'atrocità: qui ci aiuta l'etica della guerra. Al centro, oltre alla protezione dei civili, c'è la responsabilità morale, cioè la capacità di chi combatte di sentire il peso delle sue azioni quando uccide qualcuno, nella speranza che funga da freno. Negli atti del Processo di Norimberga i giudici dichiarano di condannare le persone, non lo Stato o l'esercito nazista, perché nei conflitti ci deve essere una presa di responsabilità individuale. L'IA ostacola questa consapevolezza, esponendoci a una guerra più atroce.

"Nei conflitti ci deve essere una presa di responsabilità individuale. L'intelligenza artificiale ostacola questa consapevolezza, esponendoci a una guerra più atroce"

Se un drone o un missile guidato da IA sbagliano il bersaglio e colpiscono, come è successo in Iran, una scuola elementare, di chi è quindi la colpa?

Non sappiamo se nel caso della scuola, di cui gli Usa non si sono presi ufficialmente la responsabilità, ci sia stato il coinvolgimento dell'IA, sebbene sia probabile, dato che Claude è stato utilizzato per identificare più di 1000 target nelle prime ore di guerra. Detto ciò, attribuire le responsabilità è complesso perché l'IA è una tecnologia distribuita in una lunga catena di competenze, dagli ingegneri che la progettano ai tecnici che la usano. Tutti fanno qualcosa che contribuisce all'esito finale, ma è difficile ricostruire i ruoli, il che porta a una deresponsabilizzazione sistematica. Il secondo problema è che siamo arrivati a utilizzare l'IA in Iran, così come prima in Ucraina e a Gaza, senza aver avviato in precedenza un dibattito

GETTY IMAGES

ELLE

diffusione:116015
tiratura:149118

pubblico sugli aspetti normativi, etici e legali, così ci ritroviamo a fare i conti in ritardo con questioni di fondamentale importanza per qualsiasi democrazia che voglia restare tale e qualsiasi società che intenda rimanere civile.

Nonostante tutto, ci viene spesso detto che le armi "intelligenti" fanno risparmiare vite. L'IA potrebbe rendere la guerra più giusta?

L'IA è uno strumento nelle mani di qualcuno: non rende la guerra più o meno giusta, ma più efficiente. Mille target in un giorno non sono gestibili senza l'aiuto di una macchina. Se poi questa efficienza sia orientata o meno ai principi della teoria etica della guerra giusta, dipende dalle decisioni politiche che stanno a monte, dalle soglie di rischio che si vogliono assumere.

Prima citava Claude: Dario Amodei, Ceo di Anthropic, prima dell'attacco all'Iran ne aveva negato l'utilizzo per dispositivi killer autonomi e la sorveglianza di massa provocando l'ira di Trump, c'è anche un processo legale in atto, eppure l'esercito Usa la sta usando. Come mai?

Immagino ci siano regole d'appalto da rispettare, ma in effetti è interessante notare che non c'è stato affatto lo stop immediato. Il fatto è che integrare un modello di IA su infrastrutture già esistenti richiede un lavoro complesso, e passare da uno all'altro non è banale. Possono volerci mesi. Questo ci dà la misura di quanto le forze armate siano oggi dipendenti dalle compagnie tecnologiche, i cui ingegneri lavorano fianco a fianco con gli ufficiali. Succede negli Usa, ma anche nella maggior parte dei Paesi Nato, con la differenza che questi ultimi si trovano doppiamente esposti, perché appoggiandosi a tecnologie militari IA, data center e cloud service di società americane, potrebbero da un momento all'altro non avere più garantito un certo servizio, per ordine del governo Usa.

IL LIBRO La copertina di *Codice di guerra* (Raffaello Cortina Editore) in cui Mariarosaria Taddeo, esperta di etica digitale e docente dell'Università di Oxford, analizza l'impatto dell'IA nella difesa e le sue conseguenze. Nella foto. Jessica Foster, la soldata generata dall'IA e seguita da un milione di followers su Instagram, con Donald Trump in un'immagine fake. A scoprire che si trattava di un falso è stato il *Washington Post*.

FACEBOOK

È già successo?

Sì, in Ucraina. La rete satellitare Starlink di Elon Musk è stata interrotta più volte durante operazioni militari ucraine per decisione di Musk stesso. Nel 2022, per esempio, la disattivò per impedire un attacco alla flotta russa in Crimea. Il controllo della tecnologia – oggi concentrato in pochissimi Paesi, e talvolta nelle mani di singoli privati – è una leva geopolitica di enorme peso. L'Europa ha avviato il piano ReArm Europe appunto per ridurre la sua dipendenza dotandosi di capacità industriali e tecnologiche proprie nel settore, in modo da non essere più esposta alle scelte di alleati, o miliardari, sui quali non ha alcuna influenza.

Quanto è reale il pericolo che l'IA per la difesa alimenti un sistema di sorveglianza di massa della popolazione civile anche in tempi di pace?

Il pericolo è reale e già in parte visibile. Dopo l'11 settembre, con l'Usa Patriot Act, gli Stati Uniti hanno iniziato a integrare grandi quantità di dati tra agenzie. Oggi, con l'IA, questa integrazione è diventata predittiva, permettendo di analizzare e utilizzare questi dati (anche sanitari o amministrativi) per il controllo del territorio. Esempi concreti, come la collaborazione tra Palantir (attraverso Immigration OS e Elite) e l'ICE, mostrano come questi strumenti possano essere usati per individuare e monitorare persone su larga scala. Il rischio non è teorico: senza forti limiti legali, l'IA può diventare uno strumento di sorveglianza di massa. Per questo la tutela della privacy è importante, non è una questione personale, è un limite al potere dello Stato. •