il Giornale

diffusione:45227
tiratura:95398

IL SAGGIO

La guerra diventa la nuova battaglia della Ia (come in Ucraina)

Taddeo illumina lo scenario, anche etico, dei conflitti moderni

Andrea Venanzoni

Il primo giugno 2022, le luci dell'alba illuminano un piccolo corteo di Toyota Land Cruiser. Dal confine polacco, i veicoli si spostano in territorio ucraino. Incontrano profughi spaventati e sentono, lontana ma reale, l'eco delle esplosioni. Volute nere di fumo accompagnano il loro viaggio.

A bordo di una delle auto, l'amministratore delegato di Palantir Technologies, Alexander Karp, primo alto dirigente di una società del Tech a incontrare il Presidente ucraino Zelensky nel bunker allestito a Kyiv.

Da questo incontro nascerà una sinergia che renderà il sistema MetaConstellation, una piattaforma software integrata da intelligenza artificiale, la vera infrastruttura digitale dell'amministrazione e dell'esercito ucraini. Processa dati, di ogni genere e provenienti da qualunque fonte, predice spostamenti di truppe nemiche, suggerisce pattern decisionali, coadiuva gli attacchi.

Al centro c'è la vicenda de «tech» che da Kiev contrib spostamenti di truppe nen

Diventerà una presenza talmente forte da finire effigiata sulla copertina del *Time* nel febbraio 2024; una bandiera ucraina, snodi digitali e il nome di Palantir bene impresso.

E ancora. I droni a guida autonoma con intelligenza artificiale, capaci di scardinare il paradigma human-centered, di Anduril Industries.

È davvero la prima guerra dell'intelligenza artificiale, per usare le parole di *Time*.

La relazione sempre più stringente, e problematica, tra difesa, conflitto e intelligenza artificiale, è al centro del prezioso libro *Codice di guerra. Etica dell'intelligenza artificiale nella difesa* (Raffaello Cortina Editore) di Mariarosaria Taddeo, docente di Digital Ethics and Defence Technologies all'Oxford Internet Institute dell'Università di Oxford.

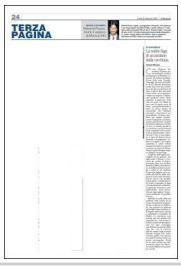
In apertura del volume, la Taddeo ricorda la ormai assoluta centralità dell'intelligenza artificiale negli scenari di guerra e nei dispositivi di difesa; da Lavender, utilizzato dall'Idf a Gaza, alle strategie di difesa elaborate da Usa, Regno Unito, Francia, Australia e al cui interno l'Ia occupa un posto di rilievo, senza dimenticare i monumentali sforzi cinesi.

I temi e i problemi posti dalla connessione tra Ia e guerra, nella duplice declinazione della difesa e dell'attacco, sono enor-

lla Palantir, la società uisce a prevedere iche e pianifica attacchi

IL TESTO

Il volume «Codice di guerra. Etica dell'intelligenza artificiale nella difesa» è stato scritto da Mariarosaria Taddeo per Raffaello Cortina Editore (pagg. 320, euro 25) ruota intorno alla digitalizzazione della difesa nazionale che ha trovato nella guerra in Ucraina il suo punto di non ritorno. Ogni giorno i dati che produciamo uniti all'intelligenza artificiale influiscono nella difesa e nella sicurezza



il Giornale

diffusione:45227
tiratura:95398

mi: la fiducia nei confronti del fattore tecnico determina spesso dis-percezioni nei team umani-macchine, facendo insorgere necessità di addestramenti specifici per calibrare razionalmente le aspettative.

Senza dimenticare poi l'affidabilità dei sistemi di machine learning quando calati nel reale, la cura estrema e la pulizia dei dati che divengono un elemento cardine nella accuratezza degli scenari e dell'impiego materiale dell'Ia.

L'autrice passa in rassegna gli usi materiali, cinetici e non cinetici, dell'Ia: sostegno, supporto, predizione, elaborazione di scenari, con l'insorgere di enormi sfide di natura etica, posto che la sostituzione dell'agente umano nei processi spesso anche decisionali autonomizza scelte di natura letale.

D'altronde a questa autonomizzazione, corrispondono anche non banali rischi di hacking di armi autonome; per questo la stessa Ia è sempre più utilizzata nella sicurezza digitale e la cybersecurity ha perso la sua valenza di mera sicurezza dei circuiti aziendali o amministrativi per divenire un tassello del complessivo dispositivo di sicurezza nazionale e di difesa.

Lo ricorda la Nato, che ha siglato con Palantir un maxi-contratto per il Maven Smart System, lo ricordano la Commissione europea e l'agenzia per la cybersicurezza in Europa, Enisa, che al binomio hanno destinato ampia normazione e altrettanto ampie linee guida.

In un quadro come questo, sovente caotico, non può stupire il ritorno sulla scena dell'etica. Si segnalano gli studi di Luciano Floridi sull'etica dell'intelligenza artificiale, le ricerche di Paolo Benanti, e della stessa Taddeo che, riprendendo la letteratura sul punto, delinea principi etici per l'impiego dell'Ia nel settore della guerra.

La parola «guerra» spaventa ma è quella più idonea, in una fase storica sempre più simile alla grande stagione della teologia bellica e nella quale non per caso, proprio facendo leva sull'etica, si rievocano Grozio, come fa Paul Saffo parlando di *Momento Grozio* sulle pagine di *Grand Continent*, o Francisco de Vitoria, citato da Johannes Thumfart a proposito del cyberspazio. È il nomos algoritmico, la lezione di Carl Schmitt nell'era digitale.

Tra i principi che l'autrice passa in rassegna, gli usi equi dell'Ia, ossia un utilizzo razionale e ponderato che eviti bias non voluti nello sviluppo e nell'uso di sistemi Ia, la trasparenza sotto condizione di tracciabilità, declinata come formazione specifica del personale che impiega questi strumenti al fine di evitare il fenomeno delle «black box». Infine, reliability e governabilità, affinché la robustezza e la sicurezza degli strumenti Ia siano opportunamente testate e garantite. Del pari essenziale, la presenza di una supervisione umana che possa bloccare una potenziale e non voluta escalation dell'agente non-umano.

La supervisione umana resta comunque decisiva per bloccare potenziali escalation determinate dal cosiddetto «agente non umano»