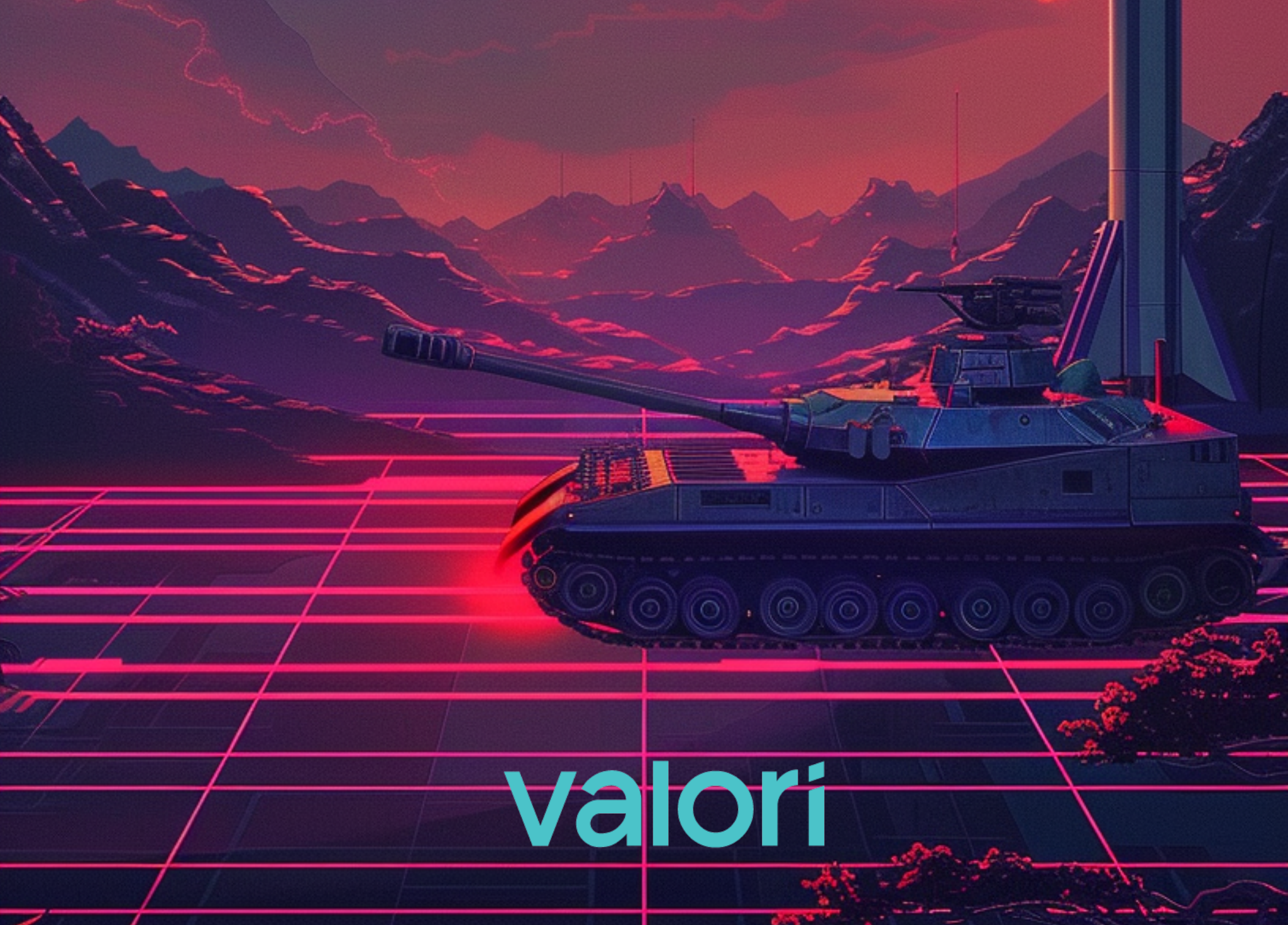
L’intelligenza artificiale va al fronte



valori

L’intelligenza artificiale va al fronte

Un dossier di Valori.it

L’intelligenza artificiale è ormai applicata in maniera intensiva nel settore militare. Negli Stati Uniti è stato già testato un caccia totalmente autonomo. Ucraina e Striscia di Gaza sono laboratori a cielo aperto.

Ecco come l’IA sta cambiando la guerra

INDICE

La corsa al riarmo passa anche dall'intelligenza artificiale

di Maurizio Bongioanni

In guerra, a decidere quando sparare finora erano gli esseri umani. L'avvento dell'intelligenza artificiale sta cambiando questo paradigma.

Fino a qualche tempo fa esisteva una linea rossa che i ricercatori impegnati nella ricerca e nello sviluppo dell'intelligenza artificiale (IA) si rifiutavano di oltrepassare: il suo utilizzo in guerra. Il fatto è che, oggi, nessun esercito può permettersi di farne a meno. Quando parliamo di cyberwarfare intendiamo attacchi informatici, droni, sistemi di intelligenza artificiale, disinformazione e deep fake. Viviamo in un'era in cui il nostro modo di pensare alla tecnologia e al suo sviluppo è determinato anche da interessi geostrategici.

Se le armi funzionano senza la presenza dell’uomo

L'idea di armi che “funzionino" indipendentemente dalla presenza dell'uomo o meno non è nuova. Prendiamo le mine antiuomo: il principio è lo stesso. Tant'è che in Cambogia, Angola e Bosnia, a molti anni dalla fine delle rispettive guerre interne, continuano a mietere vittime. Ecco perché la comunità internazionale ha deciso di vietarle: nel 1997, 164 Stati hanno adottato la Convenzione di Ottawa contro le mine antiuomo. Ciò, tuttavia, non impedisce a molti governi di continuare a utilizzarle senza alcuna regolamentazione. Ancora oggi Paesi come Stati Uniti, Cina, Russia, India e Pakistan – dove l'industria militare ha un ruolo decisivo nell'economia – si rifiutano di firmare questa convenzione.

Più di recente si è cominciato a parlare di killer robots o LAWS (Lethal autonomous weapon system) per definire tutte quelle armi in grado di selezionare e attaccare un obiettivo senza alcun supporto umano. Questo pone una serie di dubbi morali ed etici.

E non solo: le LAWS rendono più complicato anche stabilire di chi sia la responsabilità. Come riportato dal settimanale francese Courrier International, Ulrike Franke, del Consiglio europeo per le relazioni internazionali, ha evidenziato come un sistema guidato dall'intelligenza artificiale sappia imparare da sé stesso e prendere decisioni senza che gli umani ne comprendano la logica. «Ciò – ha spiegato – è particolarmente pericoloso in un contesto bellico perché, se non riusciamo a seguire le fasi del processo decisionale, diventa molto difficile individuare un atto di sabotaggio». Insomma, anche se pensiamo che gli esseri umani mantengano il controllo sull'intelligenza artificiale, quest'ultima ha già cambiato completamente il modo di fare una guerra.

Le possibili conseguenze dell'uso dell'intelligenza artificiale in guerra

Nella nostra società, ormai, ci sono sensori in grado di rilevare dati ovunque: sulla terraferma, nell'acqua, nell'aria, nello spazio e nel cyberspazio. La quantità dei dati raccolti da tutti questi strumenti è così grande che un essere umano non può comprenderli. Da qui si è sviluppata la necessità di un trattamento automatico. Nei luoghi dove si combatte, chi controlla questi dati si trova in una posizione di vantaggio. Di conseguenza, l'uso dell'intelligenza artificiale in guerra non è più teoria. La vediamo in Palestina, ma è stata l'Ucraina a impiegarla per prima.

Stati Uniti, Cina e altre superpotenze stanno lavorando per incorporare l'intelligenza artificiale nei loro eserciti. «Il vantaggio sarà di coloro che non vedono più il mondo come gli esseri umani», scrivevano nel 2022 gli ufficiali di ricerca dell'esercito statunitense Thom Hawkins e Alexander Kott.

La distanza tra operatore umano e IA si sta dunque assottigliando. Un timore che viene alimentato da più parti, anche sulla base del fatto che già in passato l'intelligenza artificiale sarebbe stata impiegata durante i conflitti, come segnalato da un rapporto del Consiglio di Sicurezza dell'Onu riguardo alla seconda guerra civile in Libia. Era il 2014 e in quel caso si trattava di sistemi d'arma letali e completamente autonomi, ma ancora lontani dall'utilizzo di "robot con licenza di uccidere", come li chiama Carola Frediani nell'ebook "Generazione AI". O di interi sciami di robot autonomi d'assalto dotati di forza letale sia via terra che in volo. Gli STM Kargu-2 utilizzati in Libano erano

droni capaci di individuare e attaccare fino a distruggere bersagli di natura non predefinita, operando senza alcuna connessione con operatori remoti.

La prima risoluzione Onu sulle armi autonome

Da allora – e con maggior forza oggi – queste armi autonome sollevano molte questioni etiche, legali e di sicurezza. Alcuni sostengono che la loro implementazione possa provocare gravi conseguenze, come errori nel targeting e un'escalation non controllata dei conflitti. Quest'ultima comprende il rischio di una corsa agli armamenti, l'abbassamento della soglia di conflitto e la proliferazione anche verso attori non statali. «L'intelligenza artificiale come fattore di potenza militare, oltre che come fattore di ricchezza economica, è al centro degli obiettivi delle principali potenze planetarie», scrive Carola Frediani. «I tentativi di comprensione e regolamentazione del fenomeno sono però ancora frammentati e divisi in ambiti diversi».

Ma qualcosa si sta muovendo. Il 1 novembre 2023, la Prima commissione dell'Assemblea generale delle Nazioni Unite, quella dedicata al "disarmo", ha adottato la prima Risoluzione in assoluto mai discussa sulle armi autonome. Dopo dieci anni di discussioni internazionali, bloccate da una minoranza di Stati militarizzati, quel voto può rappresentare un passo avanti fondamentale e aprire la negoziazione di un nuovo trattato sull'autonomia delle armi in questo contesto di rapidi sviluppi tecnologici.

La Risoluzione L56 è stata presentata dall'Austria e sostenuta da un gruppo eterogeneo di Stati. 164 hanno votato a favore, tra cui l'Italia, mentre i voti contrari sono stati cinque e le astensioni otto. La risoluzione pone in evidenza il problema e le implicazioni delle armi autonome e stabilisce che l'ordine del giorno provvisorio dell'Assemblea generale delle Nazioni Unite del prossimo anno includa anche un punto sui LAWS. Aprendo un processo che consentirà a tutti gli Stati di presentare le proprie opinioni e stabilendo una chiara tabella di marcia per l'adozione di un trattato.

La prima risoluzione Onu sulle armi autonome

«La disumanizzazione e l'uccisione di persone da parte delle tecnologie con intelligenza artificiale in contesti militari è inaccettabile e avrà conseguenze terribili nelle attività di polizia, nel controllo delle frontiere e nella società in generale», scrivono gli autori della campagna Stop Killer Robots. Di cui fanno parte Rete Italiana Pace e

Disarmo, Amnesty International, Human Rights Watch, il Comitato internazionale della Croce Rossa. E anche 26 premi Nobel ed esperti della società civile. «I 164 voti a favore della risoluzione contro le armi autonome all'Assemblea generale Onu sono un risultato clamoroso», ha sottolineato Francesco Vignarca, coordinatore delle campagne della Rete Pace Disarmo.

«Lo slancio politico è chiaro. Ed esortiamo ora gli Stati a fare un passo in più per impedire la delega di decisioni di vita e di morte alle macchine», prosegue Vignarca. «Siamo poi particolarmente soddisfatti della posizione assunta dall'Italia, sia nel voto finale sia con la decisione di sostenere la Risoluzione L56 presentata dall'Austria. È tempo di un nuovo trattato internazionale vincolante che garantisca un significativo controllo umano sull'uso della forza. Questo voto è un chiaro passo nella giusta direzione».

L’Ucraina, il laboratorio dell’intelligenza artificiale nei conflitti

di Luca Pisapia

L'invasione dell'Ucraina ha rappresentato un terreno di test per le nuove tecnologie basate sull'intelligenza artificiale

La guerra in Ucraina è stata definita un laboratorio per lo sviluppo dell'intelligenza artificiale nei conflitti. Per questo e per quelli a venire. È stato chiaro fin da subito, fin dai primi giorni dell'invasione russa, che questa guerra fosse contrassegnata dall'uso massiccio dell'IA, dispiegata da entrambe le parti. Soprattutto nelle armi letali. Ma non solo.

C'è un'altra dimensione del conflitto, forse meno evidente ma altrettanto decisiva, che ha a che fare con l'intelligenza artificiale e con le piattaforme tecnologiche che la sviluppano e/o utilizzano. È la propaganda. Lo raccontava già Sun Tzu un paio di millenni fa che la miglior guerra vinta è quella che non si combatte con le armi. E oggi l'Ucraina ci racconta che sia le armi letali sia quelle retoriche sono gestite attraverso l'accumulazione di big data.

Il Ministero della trasformazione digitale

Ma andiamo con ordine. E partiamo da un personaggio. Il suo nome è Mychajlo Fedorov, ha appena compiuto 33 anni, ed è il ministro della Trasformazione digitale e vice primo ministro del governo di Denys Šmyhal. Parafrasando Jean Baudrillard, e con tutto il rispetto dell'oltre mezzo milione di persone morte in questo conflitto, se leggiamo questa guerra come una grande battaglia postmoderna Mychajlo Fedorov è sicuramente una delle stelle di questo spettacolo.

Esperto di marketing digitale, dapprima ha costruito la candidatura presidenziale di Volodymyr Zelensky e avviato la transizione tecnologica del Paese. Poi, una volta

scoppiato il conflitto, si è preso la scena nella gestione dei due aspetti che da sempre configurano le sorti della guerra: le armi e la propaganda.

In entrambi i casi lo ha fatto utilizzando al meglio i big data, il cuore pulsante dell'intelligenza artificiale. E in entrambi i casi si è avvalso della potenza commerciale e tecnologica delle Big Tech della Silicon Valley: il terzo attore in campo in questo conflitto.

I droni: verso l'automazione delle armi letali

Il 29 marzo 2022, appena un mese dopo l'invasione, già la rivista Fortune pubblicava un articolo sull'utilizzo dell'IA nel conflitto. «Il mercato globale delle armi letali controllate dall'intelligenza artificiale vale ora circa 12 miliardi di dollari, ma si stima che il suo valore possa superare i 30 miliardi entro la fine del decennio», scriveva con preoccupazione Jeremy Kahn.

«Purtroppo non abbiamo idea se a questo sviluppo ci sarà un limite, e soprattutto quale sarà il limite», gli faceva eco Verity Coyle, senior advisor di Amnesty International. Sul campo intanto si affrontavano dalla parte ucraina i droni Bayraktar TB2, sviluppati dalla multinazionale turca Baykar Technologies. E dalla parte russa i droni "suicidi" Shahed-136 costruiti dalla Iran Aircraft Manufacturing Industries Corporation.

In realtà nessuno dei due droni era completamente automatizzato e guidato "solo" dall'IA. E anzi i Bayraktar TB2 avevano quasi più una funzione propagandistica nel raccogliere immagini e girare video che non una forza letale di distruzione dei carri armati russi. Ma era già evidente fin dall'inizio che sarebbe stato un conflitto segnato dallo sviluppo tecnologico. Dai big data e dall'intelligenza artificiale. Mancava poco alla completa automazione.

Il 10 gennaio 2023, a nemmeno un anno dall'invasione, Mychajlo Fedorov in un tweet annunciava che tutti gli sforzi del comparto industriale bellico sarebbero stati tesi alla costruzione di armi e droni che dovevano funzionare «senza l'umano».Il dado era tratto. Le sorti del campo di battaglia non sarebbero più state decise dai tradizionali mercanti di armi, ma dalle Big Tech della Silicon Valley che si occupano della raccolta dei dati e dello sviluppo dell'intelligenza artificiale.

E poche settimane dopo era sempre Mychajlo Fedorov ad annunciare l'invio da parte degli Stati Uniti dei Fortem DroneHunter F700 Interceptor. Droni completamente automatizzati e guidati dall'intelligenza artificiale in grado di localizzare, riconoscere, identificare e poi annientare i droni nemici. Il tutto senza il minimo intervento umano.

Il deus ex machina della guerra: Palantir Technologies

Passano altre due settimane e nel febbraio 2023 al World Forum dell'Aia, in Olanda, si tengono le conferenze del Reiam. Una manifestazione che ha lo scopo di collegare i mondi dell'intelligenza artificiale e del comparto strategico militare. Alla conferenza interviene Alex Karp, amministratore delegato di Palantir Technologies, che annuncia trionfante: «Siamo responsabili della maggior parte degli attacchi che avvengono sul suolo ucraino».

La Silicon Valley annuncia che il conflitto sul territorio ucraino è cosa sua. Nel giro di un anno, il grande protagonista della guerra in Ucraina diventa proprio la Palantir Technologies. Multinazionale di raccolta, utilizzo e sviluppo dei big data nata a Palo Alto nel 2003 per volontà di Peter Thiel, multimiliardario trumpiano fondatore di PayPal.

Quando nel 2016 scoppia lo scandalo Cambridge Analytica si scopre, o si torna a scoprire, che la raccolta dei dati è un'arma politica capace di decidere i destini delle nazioni. SCL Group, proprietaria di Cambridge Analytica e chiusa nel 2018 dopo lo scandalo della sua sussidiaria, è stata contractor tra gli altri del Pentagono, della Nato e dell'intelligence militare britannica. E si è sempre vantata di avere influenzato elezioni, colpi di Stato e guerre attraverso i suoi sistemi di analisi comportamentale e raccolta dati.

Dalla polizia predittiva all’individuazione dei droni dei nemici

Palantir Technologies dall'inizio degli anni Zero ha gli stessi clienti del comparto militare e di intelligence di SCL Group. La Cia, il Pentagono, vari servizi di intelligence, la Difesa degli Stati Uniti, del Regno Unito e di Israele. Forse non ha deciso le elezioni in Nigeria o nelle Filippine come SLC. O almeno non se ne vanta.

Di sicuro però partecipa al fianco dell'esercito degli Stati Uniti alle invasioni dell'Iraq e dell'Afghanistan. E all'interno del Paese conduce guerre a bassa intensità come le

operazioni di polizia predittiva per le forze dell'ordine di New Orleans. O per le polizie di frontiera durante l'amministrazione Trump.

Il tutto sempre raccogliendo, catalogando e sviluppando i big data: il cuore nero dell'intelligenza artificiale. Fra i servizi che Palantir offre all'esercito ucraino, spesso anche gratuitamente, spicca il sistema di IA Skykit che offre la possibilità di analizzare i movimenti satellitari dei droni nemici e i feed dei social media. Sempre il doppio livello: armi letali e informazione.

Tutto quello che può fare l'IA in guerra

In un approfondito reportage su Time uscito a febbraio 2024, si racconta come Alex Karp, l'amministratore delegato di Palantir Technologies che si era vantato di essere il protagonista della guerra, avesse già incontrato il ministro della Trasformazione digitale Fedorov pochi mesi dopo l'invasione. Facendo risalire la strettissima collaborazione tra la multinazionale della Silicon Valley e il governo ucraino agli albori del conflitto.

Da allora i colloqui tra i due sono praticamente quotidiani. L'articolo del Time spiega con dovizia di particolari il ruolo di Palantir Technologies e di altre start-up tecnologiche nel conflitto. E approfondisce tutti i possibili utilizzi dell'intelligenza artificiale sul campo di guerra: monitoraggio, analisi satellitari, decrittazione dei codici, interferenze radio, riconoscimento facciale, analisi predittive, cyber attacchi, propaganda sui social media, armi letali di distruzione.

E anche raccolta delle prove dei crimini di guerra avversari, pulizia dei territori minati, organizzazione logistica degli sfollati, analisi e ottimizzazione della burocrazia e delle decisioni interne – politiche e militari. Ma soprattutto, raccontano diversi fonti a Time, i software di IA di Palantir Technologies presentano ai comandi militari le migliori opzioni per condurre la guerra. Quando non sono i software stessi a prendere le decisioni.

La nuova industria degli armamenti: le Big Tech

Ma non c'è solo Palantir Technologies. A fianco dell'Ucraina nel conflitto ci sono tutti i giganti della Silicon Valley che forniscono aiuto tecnologico al governo di Volodymyr Zelensky sotto forma di software, cloud, programmi informatici di protezione e di

attacco, di difesa e di offesa. Nel conflitto ucraino gli Stati Uniti oltre a fornire le armi schierano i pezzi da novanta Microsoft, Amazon, Google e Starlink.

Per non parlare della discussa Clearview AI – sempre finanziata da Peter Thiel – ovvero la più ambigua applicazione dell'intelligenza artificiale per il riconoscimento facciale. Ecco la nuova industria degli armamenti del futuro: le Big Tech della Silicon Valley. «Possiamo definire le multinazionali che si occupano dello sviluppo dell'IA come i nuovi commercianti di armi», dice senza giri di parole l'esperto di sicurezza Jacob Helberg al Time.

Ecco come il laboratorio di guerra ucraino diventa fondamentale per raccontare il doppio binario delle applicazioni dell'intelligenza artificiale alla guerra. E come diventa decisivo per raccontare la guerra a venire. Le guerre del futuro. Guerre esplicite, dove moriranno come sempre decine o centinaia di migliaia di innocenti, uomini, donne e bambini. E guerre sotterranee, combattute a colpi di analisi comportamentali, previsioni e condizionamenti. Sempre attraverso la raccolta e l'utilizzo dei big data: il cuore nero dell'IA.

I sistemi di intelligenza artificiale che dirigono i raid di Israele a Gaza

di Maurizio Bongioanni

Secondo un'inchiesta, Israele userebbe l'intelligenza artificiale per colpire le vittime nella Striscia di Gaza senza supervisione umana

Se c'è una guerra in cui l'intelligenza artificiale sta dimostrando tutta la sua asettica brutalità, è quella in corso nella Striscia di Gaza. Difficile stabilire quando Israele ha impiegato l'AI per la prima volta contro i palestinesi. Quel che si sa è che già nel 2021 l'esercito di Tel Aviv ha utilizzato i primi sciami di droni in risposta agli attacchi di Hamas. Non si conoscono i dettagli di quell'operazione, se non che si trattava di droni da nove chili (il modello Thor prodotto da Elbit Systems) e che hanno effettuato tutte le fasi della missione, dal riconoscimento alla tipizzazione vera e propria. Probabilmente sotto sorveglianza del comando militare.

Cos'è cambiato con il programma Lavender dell'esercito israeliano

Ma se fino ad adesso il controllo umano è sempre stato presente, dal 7 ottobre 2023, giorno dell'assalto di Hamas, le cose sono cambiate. Un'inchiesta di Yuval Abraham per +972 Magazine e Local Call ha rivelato che l'esercito israeliano ha sviluppato un programma basato sull'intelligenza artificiale noto come Lavender. Secondo sei ufficiali dell'intelligence israeliana, che hanno tutti prestato servizio nell'esercito durante l'attuale guerra contro la Striscia di Gaza e sono stati coinvolti in prima persona nell'uso dell'intelligenza artificiale per generare obiettivi da assassinare, Lavender ha svolto un ruolo centrale e senza precedenti nei bombardamenti. Infatti, secondo le fonti, la sua influenza nelle operazioni militari è stata tale da indurre i militari a trattare i risultati dell'IA «come se si trattasse di una decisione umana».

Le fonti hanno riferito a +972 e Local Call che, durante le prime settimane di guerra, l'esercito si è affidato quasi completamente a Lavender, che ha registrato ben 37mila palestinesi come sospetti militanti. E le loro case obiettivi per possibili attacchi aerei. Una fonte ha dichiarato che il personale umano spesso serviva solo come «timbro di approvazione» per le decisioni della macchina. Aggiungendo che, di solito, dedicava personalmente solo «20 secondi» a ciascun obiettivo prima di autorizzare un bombardamento. Il tempo di assicurarsi solo che l'obiettivo contrassegnato da Lavender fosse di sesso maschile.

Questo nonostante si sappia che il sistema commette errori in circa il 10% dei casi. Inoltre, è noto per bollare occasionalmente individui che hanno solo un legame debole con i gruppi militanti, o addirittura nessun legame diretto. Gli attacchi venivano condotti con munizioni non guidate note come dumb bomb (“bomba stupida") che distruggono intere abitazioni insieme a tutti i suoi abitanti. «Non conviene sprecare bombe costose per persone poco importanti», è stato il commento di un ufficiale dell'intelligence.

Migliaia di palestinesi attaccati mentre sono in casa con le loro famiglie

Inoltre, l'esercito israeliano ha sistematicamente attaccato le persone mentre si trovavano nelle loro case – di solito di notte, alla presenza dei loro familiari – piuttosto che durante le attività militari. Altri sistemi automatizzati, tra cui uno chiamato “Where is daddy?", erano usati specificamente per rintracciare gli individui presi di mira e per effettuare attentati quando erano entrati nelle loro residenze.

La prova di questa politica è evidente anche dai dati. Durante il primo mese di guerra, insieme a 6.120 persone uccise, sono morte 1.340 famiglie intere. Nell'attuale guerra, la percentuale di nuclei bombardati nelle loro case è molto più alta rispetto all'operazione israeliana del 2014 a Gaza (che in precedenza era stata la guerra più letale di Israele nella Striscia). Il che suggerisce ulteriormente l'importanza dei mezzi automatici impiegati in questo frangente.

Il ruolo umano nella selezione degli obiettivi è sempre meno rilevante

Prima del 7 ottobre, la decisione di "incriminare" un individuo veniva discussa e poi approvata con i consulenti legali. Ma ora le cose sono drasticamente cambiate: i comandanti ora vogliono un flusso costante di obiettivi. Un'altra fonte riportata da +972 e Local Call ha rivelato che, ogni volta che il ritmo degli omicidi diminuiva, venivano caricati altri obiettivi in sistemi come "Where's Daddy?" per individuare nuovi bersagli da bombardare nelle loro case. Inoltre, a decidere chi inserire nei sistemi di localizzazione erano ufficiali di grado relativamente basso nella gerarchia militare. «Un giorno, di mia spontanea volontà, ho aggiunto qualcosa come 1.200 nuovi obiettivi al sistema [di tracciamento], perché il numero di attacchi [che stavamo conducendo] era diminuito», ha detto la fonte. «Ci dicevano: ora dobbiamo disintegrare Hamas, a qualunque costo. Bombardate tutto quello che si può».

Il ruolo umano nel processo di selezione dei bersagli sarebbe stato insomma poco rilevante: anche alcuni minorenni sono stati contrassegnati da Lavender come obiettivi per i bombardamenti. Di solito le persone scelte dal sistema hanno più di 17 anni, ma questa non è una conditio sine qua non. Secondo l'inchiesta, l'esercito avrebbe anche deciso che per ogni agente di Hamas di basso livello targettizzato da Lavender si poteva accettare l'uccisione di 15 o 20 civili. In passato, l'esercito non autorizzava alcun "danno collaterale" durante l'assassinio di militanti di basso rango. Nel caso di un alto funzionario, il numero di civili che si possono sacrificare sale a 100.

The Gospel, l'altro sistema di intelligenza artificiale usato a Gaza

Lavender si unisce a un altro sistema di intelligenza artificiale, The Gospel. La differenza fondamentale tra i due sistemi sta nella definizione dell'obiettivo. Mentre il primo contrassegna le persone e le inserisce in una lista di target da uccidere, una vera e propria kill list, The Gospel si limita a contrassegnare gli edifici e le strutture da distruggere.

«Attraverso l'utilizzo di questi potenti sistemi di intelligenza artificiale, Israele è entrato nel territorio inesplorato delle guerre d'avanguardia. Sollevando una serie di questioni legali e morali e trasformando il rapporto tra personale militare e macchine», scrivono i

giornalisti Bethan McKernan e Harry Davies sul Guardian, che ha co-pubblicato in anteprima l'inchiesta di +972 e Local Call. I reporter fanno riferimento al fatto che, come confermato dalle fonti, gli ufficiali hanno più fiducia in un «meccanismo informato» che in un soldato in lutto che magari ha perso qualche persona cara nell'attentato del 7 ottobre. La macchina agisce freddamente e questo, per le forze militari israeliane, è un vantaggio.

Da parte sua, il corpo militare isrealiano nega qualsiasi accusa. Attraverso una nota, dice che non esiste una policy che ammetta l'uccisione di decine di migliaia di persone nelle loro case. Lavender, poi, sarebbe solamente un database utilizzato «per incrociare le fonti di intelligence» e non «un elenco di operativi militari confermati».

La diffusa preoccupazione per l'uso dell'intelligenza artificiale nei conflitti, a Gaza e non solo

«Questa inchiesta, se confermata nei dettagli, apre interrogativi enormi e inquietanti sul ruolo che i sistemi di intelligenza artificiale stanno assumendo o potranno assumere in guerra. Sistemi che tendono già a essere delle scatole nere per come sono progettati e funzionano. E che, specie in scenari di conflitto, diventano ancora più opachi, privi di controlli o audit esterni», spiega Carola Frediani, esperta di cybersicurezza e autrice di "Guerre di Rete".

La coalizione Stop Killer Robots (la stessa che chiede una legge internazionale sul tema) ha pubblicato un commento in cui dice di «trovare profondamente preoccupanti, da un punto di vista legale, morale e umanitario, le notizie sull'uso da parte di Israele di sistemi di raccomandazione dei bersagli nella Striscia di Gaza. Sebbene il sistema Lavender, come il sistema Habsora/Gospel, non sia un'arma autonoma, entrambi sollevano serie preoccupazioni sull'uso crescente dell'intelligenza artificiale nei conflitti, sui pregiudizi dell'automazione (automation bias), sulla disumanizzazione digitale e sulla perdita del controllo umano nell'uso della forza».

L’intelligenza artificiale prepara la guerra fredda del nuovo millennio

di Andrea Di Turi

Lo sviluppo dell'intelligenza artificiale per scopi militari è il cuore del nuovo scontro tra Stati Uniti e Cina

Sull'utilizzo dell'intelligenza artificiale (IA) in ambito bellico si sta assistendo a una sorta di riedizione della guerra fredda. Dove da una parte c'è il cosiddetto blocco occidentale, Stati Uniti e Nato, dall'altro la Cina. E dove tutti sanno che l'ascesa dell'IA è irreversibile, per cui corrono per arrivare prima degli altri.

La guerra algoritmica dell’IA

Maven è il nome del progetto alla base della crescente diffusione dell'IA nelle forze armate Usa. Un documento del 2017 del dipartimento della Difesa (DoD) sottolineava la necessità, per mantenere il vantaggio sui concorrenti, di integrare nelle attività del DoD l'utilizzo dell'IA, la gestione dei big data e il machine learning. Da qui l'attivazione del progetto Maven tramite la costituzione di un team interfunzionale di guerra algoritmica: AWCFT (algorithmic warfare cross-functional team).

Tre anni dopo, nell'estate del 2020, accadeva un episodio fondamentale di questo percorso. In un'esercitazione condotta a Fort Liberty, importante base militare americana nella Carolina del Nord, un carro armato ormai dismesso veniva identificato attraverso l'IA. E dopo approvazione umana, le coordinate della sua posizione venivano inviate a un lanciarazzi che facendo fuoco lo distruggeva.

Si materializzava così uno degli obiettivi principali del progetto Maven: applicare tecnologie di visione artificiale, ad esempio attraverso l'utilizzo di droni, per identificare automaticamente e classificare gli obiettivi da colpire.

Il ruolo delle Big Tech

Inizialmente pensato per l'impiego durante le esercitazioni, il progetto è stato progressivamente affinato e migliorato. Anche grazie al supporto di società Big Tech private. E le soluzioni sviluppate sono state poi utilizzate su scenari di guerra reali, ad esempio in Yemen, Siria, Iraq. Di recente si è anche avuto, sempre in una base militare su suolo americano, il primo combattimento tra un caccia controllato da IA e uno guidato da un essere umano.

Questi sistemi vanno ormai molto al di là dell'identificazione degli obiettivi. Identificano movimenti di truppe, ottimizzano lo schieramento sul campo, aumentano la consapevolezza dello spazio in cui si svolgono le battaglie, supportano la logistica.

Per farlo, utilizzano diverse fonti di dati, dalle immagini satellitari ai dati di geolocalizzazione, alle intercettazioni di comunicazioni. Le aggregano, le analizzano e poi le rendono utilizzabili operativamente. In modo infinitamente più preciso e soprattutto più veloce di quanto gli essere umani potrebbero mai fare.

Gli investimenti in area Nato

I programmi di sviluppo di questi sistemi, inoltre, da sperimentali sono diventati strutturali e i loro finanziamenti sono aumentati: tre miliardi di dollari sono stati richiesti dal Pentagono al Congresso Usa solo nel bilancio 2024 per attività militari legate all'IA.

Veniamo alla Nato, che annovera l'IA fra quelle che chiama «tecnologie emergenti e dirompenti» (emerging and disruptive technologies, EDTs). Insieme a tecnologie quantistiche, biotecnologie, sistemi ipersonici. L'investimento in queste tecnologie, secondo la Nato, può rendere le forze armate più efficienti, resilienti, efficaci. E addirittura sostenibili (da capire come, francamente). Per giunta a costi inferiori.

Per sviluppare le EDTs è stato ad esempio varato il Fondo per l'innovazione della Nato, primo fondo di venture capital multi-sovrano, con 24 Paesi aderenti e una dotazione iniziale di un miliardo di euro per investire in start-up del settore. Il Defense Innovation Accelerator per il Nord Atlantico (DIANA) promuove inoltre la cooperazione transatlantica in quest'ambito. C'è poi anche un Comitato di supervisione sui dati e l'IA, che si occupa dell'uso responsabile dell'IA, con tanto di standard di certificazione.

E la risposta della Cina

Sul versante opposto della trincea della nuova guerra fredda, la Cina non sta certo a guardare. La Strategic Support Force dell'esercito cinese ha il compito di preparare le forze armate alla «guerra intelligente». E ha di recente pubblicato un annuncio per 500 dipendenti provenienti da università specializzate in IA.

L'esercito cinese ha anche affermato, e mostrato in un video ufficiale, che i suoi droni aerei sono capaci di raggrupparsi in sciami, auto-guidarsi, auto-ripararsi. E così completare le proprie missioni senza ulteriore aiuto umano. Allo sviluppo di sciami di droni, aerei e marittimi, si guarda in particolare nella prospettiva di un possibile futuro scontro con gli Stati Uniti per Taiwan. Dove pare potrebbero risultare decisivi.

L'esercito cinese ha anche affermato, e mostrato in un video ufficiale, che i suoi droni aerei sono capaci di raggrupparsi in sciami, auto-guidarsi, auto-ripararsi. E così completare le proprie missioni senza ulteriore aiuto umano. Allo sviluppo di sciami di droni, aerei e marittimi, si guarda in particolare nella prospettiva di un possibile futuro scontro con gli Stati Uniti per Taiwan. Dove pare potrebbero risultare decisivi.

L’accordo sull’IA bellica tra Xi e Biden

Forse questo spiega perché ci si è seduti attorno a un tavolo per parlarne. Ad esempio per decidere se debba essere solo facoltativo o invece obbligatorio che il controllo finale sulle cosiddette «armi autonome» resti in capo all'essere umano. Questione chiave a detta degli esperti per determinare il vantaggio effettivamente ottenibile con il loro utilizzo.

Xi Jinping e Joe Biden pare abbiano raggiunto un accordo almeno a parole per avviare gruppi di lavoro sulla sicurezza dell'IA. Del resto ad auspicare la collaborazione tra Cina e Stati Uniti, per porre un freno alla proliferazione delle armi basate su IA, era stato prima di morire lo stesso Henry Kissinger. Uno che a ragionare di guerra, e di guerre, ha passato la vita.

Armi e intelligenza artificiale, i grandi fondi d’investimento in prima linea

di Alessandro Volpi

Le armi generate dall'intelligenza artificiale sono una delle destinazioni privilegiate degli impieghi finanziari, attirando i grandi fondi

Le armi generate dall'intelligenza artificiale sono rapidamente diventate una delle destinazioni privilegiate degli impieghi finanziari, attirando in primis, come del resto era naturale attendersi, i grandi fondi.

Semplificando una ricostruzione ben più complessa, è possibile individuare due tipologie di produttori di armi tragicamente “intelligenti”. La prima tipologia è costituita dai grandi produttori di armi che si occupano anche di intelligenza artificiale: in particolare Northrop Grumman, Raytheon, Lockheed Martin, Charles River Analytics, L3 Harris Technologies. La seconda tipologia è rappresentata dalle società che lavorano in materia di intelligenza artificiale e la applicano anche alle armi: C3.ai., UiPath, Palo Alto Networks, KLA Corporation, Synopsys, Cadence Design Systems.

L’onnipresenza di Vanguard, BlackRock e State Street

Cosa hanno in comune queste due tipologie di società? È molto chiaro: hanno come principali azionisti i tre più grandi fondi mondiali. Vanguard, BlackRock e State Street, complessivamente, ne possiedono circa il 25%. In Northrop Grumman, State Street possiede il 9,3%, Vanguard l'8,1 e Black Rock quasi il 7%. Percentuali simili sono presenti in Raytheon (Vanguard 9,3, State Street 9,1, BlackRock 7,9) e in L3 Harris Technologies (Vanguard 10,6, BlackRock 9,1, State Street, 4,8). Ancora maggiore è la partecipazione di Vanguard e BlackRock in Lockheed Martin 15,5 e 9,1, mentre State Street ha il 7,6%) e in Charles River Analytics (11,6 e 10,02, con State Street al 4%).

Nelle società che si occupano di intelligenza artificiale, le percentuali sono simili. In C3.ai Vanguard ha l'8,7%, BlackRock il 5,7 e State Street poco meno del 2%, mentre in UiPath Vanguard si attesta all'8%, BlackRock supera il 5,6 e State Street registra l'1,7%. In Palo Alto Networks, Vanguard risulta il primo azionista con l'8,5%, seguita da BlackRock con il 5,8 e, più distanziata, compare State Street con il 3,8%. Kla Corporation è quella che ha partecipazioni ancora più consistenti da parte dei fondi, con Vanguard al 9,6%, BlackRock all'8,5% e State Street al 4,2. In Synopsys Vanguard possiede l'8,8, BlackRock il 5,9 e State Street il 4,4. In Cadence Design Systems, infine, la quota di BlackRock è pari all'11,2, quella di Vanguard al 9 e quella di State Street al 4,29.

Come nasce l’interesse dei grandi fondi verso armi e intelligenza artificiale

Questo rapido quadro di sintesi ha bisogno ancora di qualche precisazione. In primo luogo la partecipazione delle “Big Three" alle società che producono armi risale ormai a qualche anno fa, in particolare alla fase successiva alla crisi del 2008, quando tali realtà hanno iniziato una vera e propria campagna di acquisizioni, utilizzando la mole di risparmio gestito messo a loro disposizione da risparmiatori e da altri fondi spaventati dallo scoppio della bolla immobiliare, da cui Vanguard, BlackRock e State Street si erano tenuti, in buona parte, fuori.

La presenza nelle società che trattano di intelligenza artificiale è invece, inevitabilmente, più recente, ma sta procedendo a ritmo serrato con acquisizioni azionarie sempre più cospicue. Di fatto, ancora nel 2018, la presenza dei tre grandi fondi in questo settore era assai ridotta. Occorre rilevare poi che, se alla partecipazione delle Big Three nei due ambiti delle armi e dell'intelligenza artificiale si aggiunge quella degli altri fondi con forti attivi, si registra un controllo dell'azionariato non lontano dal 50%. In tale ottica vale la pena ricordare che gli stessi fondi figurano, sia pur in percentuali decisamente minori, anche in società come Thales e Bae Systems e persino in Rafael Advanced Defense Systems, che è posseduta quasi per intero dallo Stato di Israele.

Ci sono poi le start-up e le società più “piccole”, come Anduril, Databucks, Shield AI, Hawkage 360 e Epirus, che sono finanziate da venture capital, a partire da Andreessen & Horowitz. E che cercano di partecipare, in realtà senza troppo successo, alle

commesse del governo degli Stati Uniti. Alcune di loro, peraltro, godono di finanziamenti diretti – esemplare il caso di Databuck – da colossi come Amazon e Microsoft. In estrema sintesi, pochissimi soggetti guadagnano una montagna di soldi dalle nuove frontiere della tecnologia militare.

IA militare: le Big Tech e start-up che si alleano con l'industria bellica

di Andrea Barolini

Si moltiplicano i progetti di intelligenza artificiale nel settore militare. I principali attori di questo business sono i soliti noti

Nel febbraio del 2022, soltanto due settimane dopo l'inizio dell'invasione russa in Ucraina, un uomo d'affari statunitense scriveva una lettera aperta ai dirigenti europei. Nel testo, sottolineava come la guerra fosse ormai alle loro porte. E spiegava che, per questa ragione, le nazioni del Vecchio Continente avrebbero dovuto affrettarsi a modernizzare i loro arsenali. Ma per farlo, oggi, non è necessario rivolgersi alle industrie tradizionali. O almeno non soltanto. Occorre piuttosto puntare sulla Silicon Valley americana. Perché, secondo la lettera, il futuro del settore militare dipenderà strettamente dall'intelligenza artificiale.

Dal boom della tedesca Palantir al programma americano NGAD

Quell'uomo d'affari si chiama Alexander Karp, e non è un manager del settore della Difesa: è il fondatore e amministratore delegato di Palantir Technologies. Una società nata nel 2003, specializzata nell'analisi di grandi moli di dati (Big data) e diventata vent'anni dopo un colosso con una capitalizzazione da oltre 22 miliardi di dollari (dato del 2020), ricavi da 2,23 miliardi (2023) e più di 3.700 dipendenti. L'azienda e il suo numero uno hanno fiutato da tempo l'affare legato allo sviluppo di tecnologie ad uso militare.

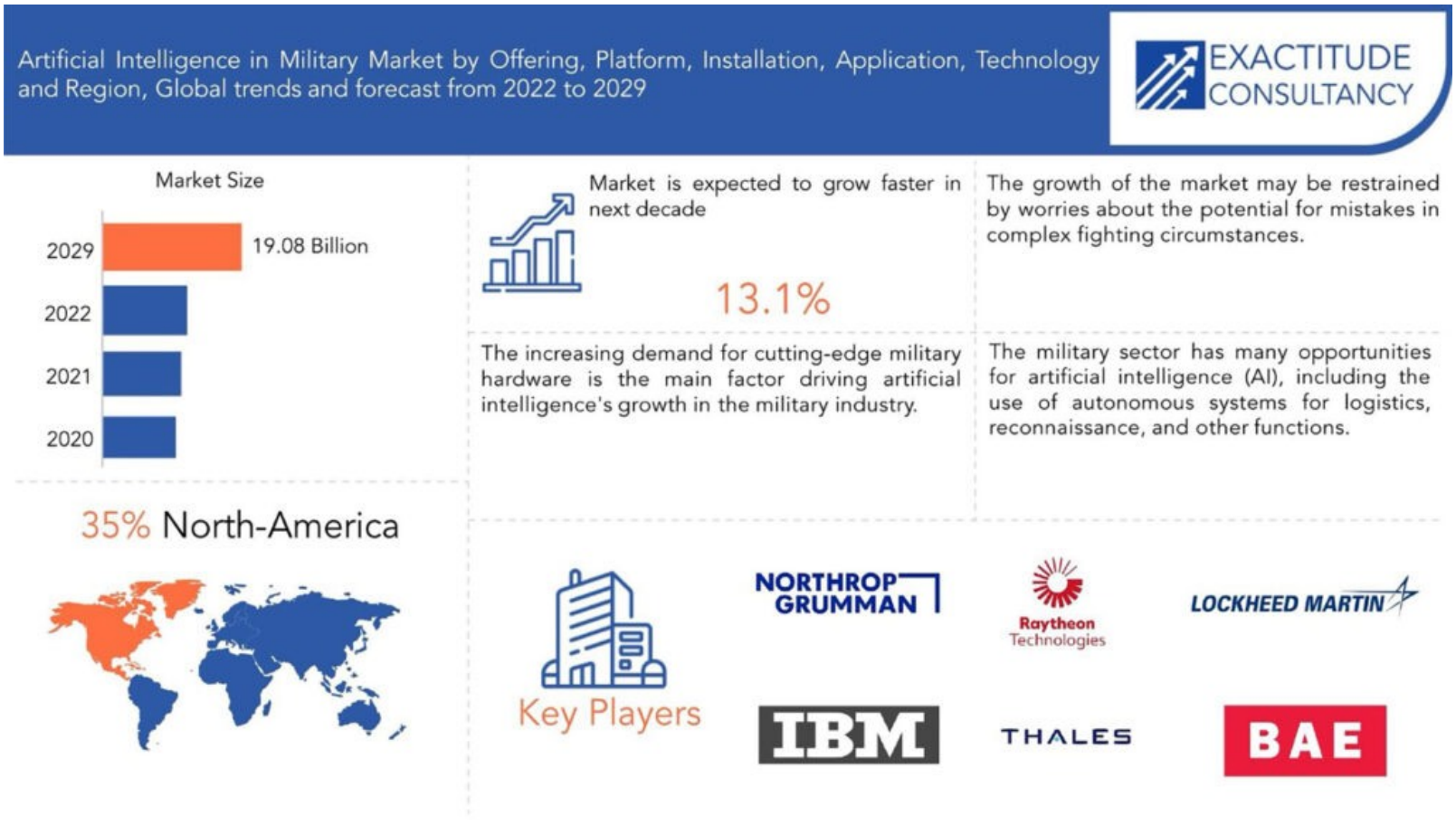
La risposta della Nato, in quel 2022, fu d'altra parte pronta. Il 30 giugno, l'Alleanza atlantica annunciava la creazione di un fondo per l'innovazione nel settore militare. Dotato di ben un miliardo di dollari. Investimenti che sarebbero andati a vantaggio di start-up e fondi di venture capital mirati allo sviluppo di tecnologie considerate "strategiche". Ovvero, appunto, intelligenza artificiale, big data e automazione.

D'altra parte, dall'inizio della guerra in Ucraina, il Regno Unito ha sviluppato una nuova strategia d'IA specificatamente dedicata alla Difesa. E la Germania ha stanziato mezzo miliardo di dollari per la ricerca in tale settore. Mentre gli Stati Uniti hanno già da tempo avviato numerosi programmi, come nel caso del "Replicator", che punta a sviluppare uno stormo di duemila caccia pilotati da macchine. Un misto di droni, algoritmi, materiali innovativi che dovranno dare corpo al programma Next Generation Air Dominance (NGAD). Quest'ultimo punta a sviluppare velivoli che dovranno rimpiazzare nel 2030 gli F-22 Raptor.

BAE System, Lockheed Martin, Boeing, Thales: nel business dell'intelligenza artificiale militare i soliti noti

Di fronte a tale "effervescenza" (e allettati dagli ingenti fondi stanziati) sono numerose le imprese che si stanno lanciando nello sviluppo di intelligenza artificiale militare. Secondo un rapporto della società di consulenza Exactitude Consultancy, pubblicato nel mese di maggio del 2023, i principali attori del crescente mercato dell'intelligenza artificiale militare sono in gran parte nomi noti. Come BAE Systems, Northrop Grumman, Raytheon Technologies, Lockheed Martin, Thales. E ancora L3Harris Technologies, Rafael Advanced Defense Systems, IBM, Charles River Analytics e Boeing.

Exactitude Consultancy sottolinea come molti di loro stiano stringendo accordi con aziende specializzate. EDGE, uno dei principali attori del mercato dell'IA, ad esempio, ha firmato un protocollo con BAE Systems nel febbraio del 2023. Lockheed Martin e Sintavia (primo produttore mondiale di componenti interamente digitali per l'aerospace) hanno annunciato una collaborazione tre mesi prima.



Le previsioni sul mercato dell’intelligenza artificiale militare © Exactitude Consultancy

Il caso della tedesca Helsing, tra accordi con i governi e promesse “democratiche”

Allo stesso modo, l'impresa specializzata in intelligenza artificiale applicata alla Difesa Helsing AI, secondo quanto riportato da Wired, ha proposto una nuova tecnologia di punta a diversi eserciti di tutto il mondo. Un sistema capace di assorbire in breve tempo quantità enormi di dati provenienti da sensori e armi utilizzati in guerra. Grazie a un algoritmo, le informazioni in questione vengono trasformate in una visualizzazione simile a un videogioco, che fornisce dati dati in tempo reale e una visione d'insieme del campo di battaglia.

Si tratta anche in questo caso di una start-up, nata a Berlino nel 2021 grazie a un investimento di 100 milioni di euro del fondo Prima Materia, di proprietà del fondatore di Spotify, lo svedese Daniel Ek. Successivamente, l'azienda ha aperto divisioni anche nel Regno Unito e in Francia. Il tutto sulla base dello slogan «L'IA al servizio delle democrazie». Helsing, infatti, promette che mai farà affari con governi autoritari. Già, ma in che modo si può qualificare veramente una democrazia come tale? È lo stesso Wired a porsi la domanda: «Quando abbiamo chiesto ai dirigenti se venderebbero le

loro tecnologie a Paesi come la Polonia e l'Ungheria, nei quali i giudici sono stati privati della loro indipendenza e i diritti LGBT sono stati negati, non abbiamo ottenuto risposta».

L'Ucraina, una «miniera d'oro» per chi sviluppa intelligenza artificiale militare

Tuttavia, i fondatori di Helsing assicurano, ad esempio, di avere «particolarmente a cuore la vita privata era libertà. Mai ci lanceremo in strumenti come il riconoscimento facciale», ha affermato il co-amministratore delegato Gundberg Scherf. Secondo il quale l'obiettivo è aiutare i militari a riconoscere degli oggetti, non delle persone. L'altro co-Ad, Torsten Reil, si è affrettato a precisare che la sua società non fabbrica armi autonome: «Al contrario, creiamo sistemi di intelligenza artificiale che aiutano gli esseri umani a comprendere meglio la situazione».

Ciò nonostante, l'applicazione dell'intelligenza artificiale al settore militare, e in particolare l'interazione tra soldati e macchine, lascia molti interrogativi aperti. L'industria militare francese Nexter, ad esempio, si è appoggiata a Helsing per migliorare la precisione dei colpi del suo cannone automatizzato Caesar. Al giornale transalpino Usine Digitale, la ricercatrice dell'Istituto francese per le relazioni internazionali, Laure de Roucy-Rochegonde, ha osservato come l'avvio di così tante collaborazioni dopo l'inizio della guerra tra Mosca e Kiev non può essere un caso: «Tutte le imprese specializzati nell'intelligenza artificiale militare si stanno gettando in Ucraina. Per loro è l'occasione per testare i prodotti sul campo. E per raccogliere enormi moli di dati operativi. Una miniera d'oro».

Dalla Germania agli Stati Uniti, si moltiplicano i progetti di IA applicata alla Difesa

Una miniera d'oro sulla quale si stanno lanciando anche altri grandi gruppi, come nei casi di Thales e Airbus. Ma anche le grandi aziende informatiche mondiali hanno un ruolo. Da un lato, non è un caso se il gruppo Helsing ha assunto Antoine de Braquilanges, ex di Palantir e di Amazon Web Services, e Antoine Bordes, ex dirigente dei laboratori di intelligenza artificiale di Facebook. Dall'altro, l'arrivo in azienda del generale Denis Mercier, ex capo di Stato maggiore delle forze aeree francesi, fa

comprendere quanto la start-up tedesca sia ormai diventata strategica agli occhi dei poteri pubblici europei.

Di qui nascono partenariati come quello con Saab Germany per la fornitura di sensori concepiti specificatamente per integrare i radar di quindici Eurofighter di Luftwaffe, destinati a sostituire i Tornado nelle missioni di attacco di difese aeree avversarie. Si tratterà di sistemi capaci di «generare in qualche millesimo di secondo misure di auto-protezione precise contri i moderni radar nemici», spiegano dall'azienda.

La guerra commerciale tra Big Tech americane e cinesi

Negli Stati Uniti, un'azienda in piena espansione è Anduril Industris, che ha sviluppato un sistema di trattamento dei dati battezzato Lattice, impiegato su una piattaforma di telecomunicazioni chiamata Spacetime e concepita da Aalyria, spin-off di Google. Similmente, Shield AI fornirà a Boeing Defence, Space & Security il "pilota digitale" Hivemind, che sfrutta dati GPS per spostarsi sui teatri di guerra (ed è già stato impiegato su degli F-16 e su dei droni a decollo verticale). Sempre gli Stati Uniti, da alcuni anni hanno lanciato in contesti di ricerca militare il progetto KAIROS (Knowledge-directed Artificial Intelligence Reasoning Over Schemas), destinato a concepire un'intelligenza artificiale capace di esplicitare dei ragionamenti.

Inevitabile la presenza, in questo quadro, dei grandi attori della Big Tech come Google, Apple, Facebook, Amazon, Microsoft. Un'analisi di Nicolas Mazzucchi di alcuni anni fa già indicava come tali aziende fossero particolarmente attive. Esattamente come le loro omologhe cinesi Baidu, Alibaba, Tencent, Xiaomi. Il tutto non senza tensioni interne. Come nel 2018, quando alcuni impiegati di Google protestarono in riferimento all'uso militare di alcune applicazioni della libreria open source per l'apprendimento automatico TensorFlow.

Com’è andata la prima battaglia aerea tra un essere umano e l’IA

di Valentina Neri

L’intelligenza artificiale sa anche pilotare un aereo da combattimento. Lo dimostra il primo test condotto dalle forze armate statunitensi

È il mese di settembre 2023 quando un X-62A VISTA e un F-16 decollano dalla base aerea di Edwards, in California, per affrontarsi in un combattimento aereo di prova. Di per sé si potrebbe pensare che non ci sia niente di strano, se non per un dettaglio: l'F-16 è controllato da un pilota umano, l'X-62A dall'intelligenza artificiale.

Un sistema di intelligenza artificiale che sa pilotare un jet da combattimento

La DARPA (Defense Advanced Research Projects Agency, Agenzia per i progetti di ricerca avanzata di difesa) ha iniziato a dicembre 2022 a sperimentare le possibili applicazioni dell'IA all'interno del suo programma Air Combat Evolution (ACE), collaborando anche con la scuola di addestramento al volo avanzato dell'Air Force. L'obiettivo? Sviluppare un sistema di intelligenza artificiale che fosse in grado di pilotare in autonomia un jet da combattimento, rispettando i protocolli di sicurezza stabiliti dall'Aeronautica.

I team coinvolti hanno cominciato con le simulazioni, per poi installare l'IA nei sistemi dell'X-62A e condurre 21 voli di prova che hanno permesso di apportare oltre 100mila modifiche critiche al software. Nell'arco di meno di un anno, i tempi erano già maturi per il primo test di combattimento aereo ravvicinato (dogfight) contro un F-16 pilotato da un essere umano. Un esperimento riuscito.

Com’è andato il primo combattimento aereo di prova tra umani e IA

«Il combattimento aereo è uno scenario altamente complesso che l'X-62A ha utilizzato per dimostrare con successo che l'utilizzo sicuro di intelligenza artificiale non deterministica è possibile nel settore aerospaziale», si legge nel comunicato della DARPA. Il test ha preso il via con manovre difensive, per poi passare agli scontri offensivi. I due velivoli si sono avvicinati fino a 600 metri, a una velocità di quasi 2mila chilometri orari.

A bordo dell'F-16 c'era un pilota umano. Anche a bordo dell'X-62A in realtà c'era un team che aveva la possibilità di disattivare il sistema di intelligenza artificiale e prendere il comando. Ma non ne ha mai avuto bisogno. La DARPA non ha fatto sapere quale dei due aerei abbia prevalso ma, d'altra parte, non era questo il fulcro dell'operazione. «Il combattimento aereo era il problema da risolvere per poter iniziare a testare in aria i sistemi di intelligenza artificiale autonomi», sottolinea Bill Gray, capo pilota di prova della scuola di addestramento dell'Air Force. «Ogni lezione che stiamo imparando si applica a qualsiasi compito si possa assegnare a un sistema autonomo».