SoftWar

Alla digitalizzazione della guerra corrisponde la militarizzazione del digitale. L'utilizzo dell'AI nella guerra di Gaza è solo la parte visibile di una più vasta e intensa torsione bellica della produzione digitale.

Giulio De Petra

Lavender

Da quando l'inchiesta di Yuval Abrahm sulla rivista israeliana +972 Magazine ha raccontato come l'esercito israeliano stia intensamente utilizzando sistemi basati su intelligenza artificiale nella guerra di Gaza, grande è stata l'attenzione che la stampa ha dedicato al funzionamento e all'uso di 'Lavender', che è il nome del sistema di AI appositamente realizzato.

In particolare opinionisti ed esperti sono rimasti colpiti dal fatto che l'individuazione dei bersagli da uccidere fosse di fatto delegata al sistema digitale senza alcuna revisione o intervento da parte di militari 'umani'.

Poiché i bersagli da uccidere sono i militanti di Hamas ci si è interrogati su quali fossero i criteri con cui il sistema individua chi sia un militante di Hamas, attribuendo anche un rango al bersaglio (capo, ufficiale, soldato semplice, fiancheggiatore), rango che, come vedremo, genera effetti significativi nelle procedure di 'eliminazione' del bersaglio.

E poi quali fossero gli indizi, sempre valutati dal sistema automatico, che associavano il bersaglio così individuato a un punto effettivo sulla mappa di Gaza da colpire.

E, in presenza di percentuali di errore stimate del 10% dei casi, si è criticata l'assenza di ogni controllo umano, che forse avrebbe diminuito di qualche punto percentuale la possibilità di un falso positivo, cioè di far diventare un bersaglio chi non era un militante di Hamas.

Si sono cioè utilizzati, nell'analisi e nel commento, gli stessi argomenti di valutazione di un sistema digitale automatico di predizione che si sarebbero utilizzati per una campagna di marketing progettata per vendere aspirapolvere.

Allo stesso modo in cui le armi autonome, da tempo presenti su molti teatri di guerra, aumentano ancora di più la separazione tra chi uccide e chi è ucciso, facendo diventare il bombardamento di una città un videogioco, anche il racconto e il commento sull'uso dell'intelligenza artificiale in guerra sembra aver perso completamente di vista il contesto, il significato, le conseguenze, le responsabilità.

Che non riguardano in questo caso la percentuale di falsi positivi del sistema di predizione automatico, ma la scelta consapevole e pianificata dell'esercito israeliano di uccidere centinaia di civili, donne, bambini ogni volta che si cerca di 'eliminare' il bersaglio individuato.

Da colpire quando rientra nella sua abitazione, o si muove in luoghi affollati. Così suggerisce Lavender. E se il rango determinato dal sistema automatico di classificazione lo individua come capo, la quantità esseri umani che vengono uccisi può essere pari alle centinaia di abitanti di un intero caseggiato.

Spiegare con l'uso di un sistema di AI le bombe da 1000 kg lanciate su centri abitati e su campi profughi densamente popolati sembra più la grottesca giustificazione di una mattanza che l'uso di un sofisticato armamento.

Digitalizzazione della guerra e militarizzazione del digitale

Tuttavia avere acceso i fari dell'attenzione di esperti e opinionisti sull'uso dell'intelligenza artificiale nei teatri di guerra ha avuto il merito di portare in superficie ciò che già da molti anni sta accadendo nelle strategie di sviluppo dei grandi monopolisti digitali: una crescente e reciproca dipendenza tra industria digitale e apparato statale militare. L'apparato militare sempre più dipendente dai prodotti e dai servizi delle imprese digitali in tutti i teatri di guerra, le big tech sempre più alla ricerca di nuovi mercati, di lucrose commesse pubbliche, o di investimenti in ricerca e sviluppo orientati all'utilizzo in ambito militare.

Per dimostrare l'uso crescente del digitale in ambito militare non c'è solo l'inchiesta di +972 su Lavender, basta ricordare il ruolo che ha giocato e sta

giocando Starlink, la rete di proprietà di Elon Musk, nella guerra in Ucraina, o la crescita esponenziale nella produzione dei droni militari e dei loro componenti digitali, dall'Ucraina alla Russia, dall'Iran alla Turchia per finire all'italiana Leonardo.

E, reciprocamente, per mostrare la dipendenza delle grandi imprese dalle commesse pubbliche di natura militare basta fare riferimento a quanto descritto dalla recente ricerca "Blurring boundaries: an analysis of the digital paltforms-military nexus" che descrive i numerosi e grandi contratti pubblici delle big tech USA.

Questa torsione dell'industria digitale verso la produzione militare sta avendo nelle due guerre in corso una accelerazione così forte da costituire essa stessa uno dei motivi che determina la prosecuzione dei conflitti e anche la loro traiettoria futura.

Succede a Gaza

L'agenzia di informazione giapponese Nikkei racconta ad esempio di come diverse startup israeliane esportino tecnologia militare avanzata alimentata dall'intelligenza artificiale la cui precisione è migliorata proprio grazie all'uso che se ne fa nella guerra di Gaza.

Axon Vision, ad esempio, rivendica che il suo sistema Edge 360, installato nei veicoli blindati attualmente schierati a Gaza, identifica le minacce provenienti da tutte le direzioni e avvisa il soldato alla guida del veicolo. il CEO Roy Riftin in un'intervista descrive i vantaggi degli stretti rapporti con l'esercito israeliano: "Riceviamo feedback in continuazione".

Asio Technologies sta collaudando a Gaza per la prima volta il suo sistema Orion, che determina la portata e la posizione di un bersaglio utilizzando dati geografici e riprese aeree. I risultati forniscono ai soldati percorsi per avvicinarsi a un bersaglio che riducono al minimo le linee di fuoco del nemico.

SmartShooter è a sua volta un'azienda tecnologica emergente che fornisce apparecchiature intelligenti di controllo del fuoco dei fucili per garantire un colpo più preciso. Dopo i test a Gaza la BBC riferisce che anche i soldati britannici sono stati addestrati utilizzando l'attrezzatura prodotta da SmartShooter.

Succede in Ucraina

Ciò che ha avviato il governo Ucraino non è da meno, ed è raccontato in un articolo di Flavio Pintarelli apparso sul sito di "Guerre di rete".

Il 26 aprile del 2023 grazie alla cooperazione di sei importanti attori istituzionali ucraini attivi nella sfera della sicurezza e della difesa – i ministeri della Trasformazione digitale, delle Industrie strategiche, dell'Economia e della Difesa, lo Stato Maggiore delle Forze Armate ucraine e il Consiglio nazionale di sicurezza e difesa – è stato costituita BRAVE1, una piattaforma per velocizzare la crescita dell'ecosistema tecnologico nel settore della difesa e accelerare lo sviluppo di sistemi pronti per essere utilizzati in prima linea.

"La nostra missione – scrive Nataliia Kushnerska nel documento di presentazione di BRAVE1 – è favorire la cooperazione tra i diversi attori coinvolti nel processo: aziende, forze di sicurezza e difesa, governo, industria, investitori, fondazioni, partner internazionali, media e ogni altro soggetto coinvolto nel rafforzamento delle capacità delle forze armate ucraine. Per farlo BRAVE1 attrae e sostiene sviluppatori e innovatori nel campo delle tecnologie per la difesa, accelera l'implementazione dei prodotti fornendo accesso alle competenze militari, alle capacità di dimostrazione e collaudo, all'utilizzo in ambiente operativo".

Quella sulle tecnologie di difesa e sicurezza per il governo ucraino non è una visione limitata esclusivamente alla difesa, ma si inserisce in un progetto strategico, teso a fare dell'Ucraina un hub globale nel settore *defence tech.*

A confermare questa visione è lo stesso presidente Zelensky che, in un'intervista rilasciata alla giornalista Natalia Moseychuk, sottolinea come l'Ucraina abbia, nell'agricoltura come nella tecnologia, grandi opportunità, tra cui quella di diventare un Paese guida nel settore della difesa e della sicurezza.

In questa visione, quelle che oggi sono solo piccole startup impegnate a ideare, sviluppare, verificare e ottimizzare nuove tecnologie belliche, ambiscono a diventare, nei prossimi anni, potenti aziende tecnologiche nel settore della difesa, dal valore di miliardi di dollari, in grado di proporre sul mercato soluzioni già messe alla prova nel campo di battaglia.

Dual use

Da questi esempi, che dimostrano come un teatro effettivo di guerra possa essere il migliore ambiente di collaudo possibile per le aziende digitali che producono tecnologie militari, vengono anche svelate le implicazioni della locuzione 'dual use', che nelle intenzioni di chi la utilizza descrive il fatto che una tecnologia, o un settore di ricerca tecnologica, possa avere un doppio uso possibile, in ambito militare, ma anche in ambito civile, e che questo doppio utilizzo possibile giustifichi ed autorizzi la ricerca, anche universitaria, in settori applicativi che possono essere sfruttati in ambito militare.

Se ci riferiamo a Lavender, e cioè all'utilizzo di sistemi di intelligenza artificiale basati su apprendimento automatico per individuare bersagli da colpire, ne deriva la conseguenza efficacemente descritta da Daniela Tafani in un contributo apparso su "Orizzonti", sezione online della rivista Italiani Europei.

> "Lo sviluppo dei sistemi di apprendimento automatico ha luogo entro una relazione, originaria e costitutiva, con l'apparato militare e i sistemi statali di sorveglianza: i primi sistemi di *computer vision* sono stati realizzati per automatizzare la fotointerpretazione delle immagini aeree, alla ricerca di oggetti di interesse militare, e alla filiera della sorveglianza... Esprimere tale relazione con l'espressione "*dual use*" è fuorviante: i sistemi concepiti per fini militari conservano l'impostazione, la concettualizzazione degli oggetti di interesse, gli assunti normativi e la logica originari. Con la polizia predittiva, ad esempio, si trasforma la totalità dei cittadini in persone oggetto di sorveglianza, estendendo all'ambito civile la logica militare dell'*intelligence* e sopprimendo il diritto individuale a non essere oggetto di sorveglianza senza fondate ragioni".

Il diritto di opporsi

Chi può opporsi a questa crescente militarizzazione della produzione digitale, e alla crescente torsione bellica dei sistemi basati su intelligenza artificiale?

Sicuramente provano a farlo gli studenti che nelle università italiane stanno lottando per sospendere la collaborazione dei loro atenei con le aziende

militari israeliane. Torino, Pisa, Roma sono alcune delle tappe di questa mobilitazione generosa che resiste intelligentemente ai tentativi del governo di farne un problema di ordine pubblico. Studenti, ricercatori e docenti utilizzano l'obiettivo di interrompere la collaborazione con i centri di ricerca israeliana direttamente o indirettamente coinvolti nella guerra di Gaza per proporre un tema politico di portata più ampia: quello della incompatibilità tra l'autonomia della ricerca, ed in particolare di quella che si occupa di tecnologie digitali di punta, e l'uso del digitale in guerra, in tutte le guerre. Come si è cercato di fare per le tecnologie nucleari, con i trattati di non proliferazione nucleare oggi rimessi in discussione dai due attuali principali attori della produzione militare, USA e Russia, così è necessario fare per le tecnologie dell'intelligenza artificiale, proponendo finché si è in tempo, di "disarmare l'AI".

Ma oltre agli studenti, che andrebbero maggiormente sostenuti nelle loro lotte per l'autonomia della scienza e delle tecnologie, gli altri soggetti che possono opporsi alla sussunzione del digitale nel militare sono i lavoratori delle big tech, che iniziano ad organizzare esplicite manifestazioni di contestazione.

Racconta il Time che nel centro di Manhattan il 4 marzo, mentre in un convegno l'amministratore delegato di Google per Israele stava promuovendo l'industria tecnologica israeliana, un giovane si è alzato in segno di protesta. "Sono un ingegnere del software di Google Cloud e mi rifiuto di costruire una tecnologia che alimenta il genocidio, l'apartheid o la sorveglianza", ha gridato, indossando una maglietta arancione con un logo Google completamente bianco. Il lavoratore di Google, un ingegnere del software di 23 anni di nome Eddie Hatfield, fa parte di un gruppo di protesta chiamato No Tech for Apartheid che chiede all'azienda di abbandonare il progetto Nimbus, un contratto da 1,2 miliardi di dollari con Israele, detenuto congiuntamente con Amazon. Hatfield è stato rapidamente portato fuori dalla sala della conferenza. Dopo una pausa, l'amministratore di Google ha così commentato questo atto di protesta. "Uno dei privilegi di lavorare in un'azienda che rappresenta i valori democratici è dare spazio a opinioni diverse", ha detto ai presenti. Tre giorni dopo Google ha licenziato Hatfield.