Dichiarazione congiunta sull'intelligenza artificiale nella guerra

Noi, organizzazioni e individui firmatari, siamo profondamente allarmati dalla rapida militarizzazione delle tecnologie di intelligenza artificiale (IA). I sistemi di IA integrati nelle "catene di uccisione" (kill chain) militari stanno accelerando la velocità e la portata degli attacchi militari in un modo che crea nuovi e rilevanti rischi per la responsabilità nei conflitti e che rischia di agevolare violazioni del diritto penale internazionale, dei diritti umani e del diritto umanitario.

Chiediamo pertanto alle aziende tecnologiche e agli Stati di interrompere la fornitura di sistemi di IA destinati all'uso nella kill chain militare e di adottare ogni misura per garantire che gli altri sistemi di IA che forniscono non causino né contribuiscano a violazioni del diritto internazionale umanitario (DIU) e del diritto internazionale dei diritti umani (DIDU). Questo include l'uso di sistemi di IA di supporto alle decisioni, compresi i sistemi di generazione degli obiettivi, la sorveglianza biometrica da remoto e i modelli di IA multimodali, inclusi i grandi modelli linguistici (LLM). La guerra accelerata dall'IA sta rapidamente diventando un mezzo per "timbrare" l'uccisione di massa a grande velocità e su larga scala, e attualmente nessuna correzione tecnica o procedurale può prevenire efficacemente le conseguenze letali e devastanti che derivano dalle sfide fondamentali che essa pone al diritto internazionale.

Tutte le aziende, comprese quelle che stipulano contratti con agenzie militari governative lungo l'intera catena di fornitura dell'IA — dalla concessione in licenza e dall'addestramento dei modelli "di frontiera" fino alla fornitura di funzioni di elaborazione e archiviazione dei dati — devono adottare ogni misura possibile per garantire che i loro prodotti e servizi non causino, contribuiscano o siano direttamente collegati ad abusi dei diritti umani e a crimini internazionali. Nei conflitti armati, questa responsabilità si estende al rispetto del diritto internazionale umanitario e penale, dato l'accresciuto rischio di agevolare gravi abusi dei diritti umani in tali contesti. Laddove le aziende non siano in grado di prevenire o mitigare in modo concreto tali rischi, non devono stipulare né dare esecuzione a contratti di questo tipo.

I sistemi di archiviazione e analisi dei dati abilitati dall'IA usati nella kill chain — tra cui il grande modello linguistico Claude di Anthropic e il Maven Smart System — secondo un'inchiesta della NBC starebbero giocando un ruolo nel supportare gli attacchi statunitensi e israeliani contro l'Iran. OpenAI ha recentemente accettato di fornire servizi di IA al Dipartimento della Difesa statunitense; Google ha stipulato contratti con il Dipartimento, come Anthropic, per "sviluppare prototipi di capacità di IA di frontiera per affrontare sfide critiche di sicurezza nazionale negli ambiti bellico e operativo"; Microsoft, Google e Amazon forniscono da anni servizi di archiviazione, elaborazione dati e altre infrastrutture ai programmi bellici del Dipartimento.

Secondo notizie di stampa e dichiarazioni ufficiali del Dipartimento della Difesa, la rapida generazione di obiettivi tramite strumenti di IA ha consentito un aumento della velocità,

della portata, dell'intensità e della forza distruttiva degli attacchi statunitensi contro l'Iran. Nelle prime 48 ore di attacchi, Israele e gli Stati Uniti avrebbero colpito quasi 2.000 obiettivi in Iran. Sebbene molto resti poco chiaro sul ruolo preciso svolto dai sistemi di IA in questi attacchi, le incursioni hanno avuto un impatto devastante sui civili e sulle infrastrutture civili.

L'adozione di sistemi di targeting basati sull'IA in questa campagna segue l'esempio dell'uso, da parte del governo israeliano, di strumenti di analisi dei dati e machine learning alimentati dalla sorveglianza di massa nei suoi attacchi genocidi contro Gaza. Diluendo la responsabilità umana nelle decisioni di vita e di morte, l'uso da parte di Israele di sistemi come Lavender, Gospel e Where's Daddy può contribuire a occultare crimini internazionali dietro un'apparenza di presunta oggettività algoritmica, offuscando al tempo stesso le responsabilità.

Non è la prima volta che vediamo la Palestina usata come laboratorio per metodi di guerra sperimentali e disumanizzanti, anche attraverso partnership tecnologiche aziendali con le agenzie militari israeliane. Microsoft, Google, Palantir e altre aziende tecnologiche potrebbero aver contribuito o consentito l'accesso del governo israeliano a sistemi di archiviazione, elaborazione e analisi di dati di massa che stanno favorendo la distruzione e il genocidio in corso a Gaza, che finora ha causato l'uccisione di almeno 72.000 palestinesi.

Studiosi e professionisti del diritto, esperti tecnici, lavoratori del settore tecnologico, relatori speciali dell'ONU e giornalisti investigativi mettono in guardia da tempo contro lo sviluppo e l'impiego dell'IA in guerra, dato l'accresciuto rischio di crimini internazionali. Nonostante le affermazioni dei suoi sostenitori secondo cui gli strumenti di IA renderebbero la guerra più efficace, precisa o "umana", gli impieghi reali indicano che l'IA sta in realtà agevolando metodi di guerra più violenti, disumanizzanti e distruttivi.

In particolare, siamo profondamente preoccupati dal fatto che l'uso degli LLM per la generazione e la definizione delle priorità degli obiettivi stia spingendo gli attori militari verso una forma di guerra in cui i principi fondamentali del diritto internazionale umanitario — tra cui i principi di distinzione, proporzionalità e precauzione — non sono, e probabilmente non possono essere, sufficientemente rispettati, data l'enorme velocità e portata di tali tecnologie, oltre alla natura inaffidabile, distorta e spesso illegalmente ottenuta dei dati di input. Affermiamo inoltre che queste dinamiche rischiano di agevolare abusi dei diritti umani, crimini contro l'umanità e crimini di guerra. Inoltre, l'opacità che accompagna l'uso di questi strumenti minaccia alla radice la possibilità di attribuire responsabilità morali o legali nei casi in cui vengano commessi errori. Come la stessa Anthropic ha dichiarato, "...oggi i sistemi di IA di frontiera semplicemente non sono abbastanza affidabili da alimentare armi pienamente autonome. Non forniremo consapevolmente un prodotto che metta a rischio i combattenti e i civili americani". Gli attori che scelgono di impiegare sistemi di IA usati per commettere crimini internazionali devono essere ritenuti penalmente responsabili.

Le nostre preoccupazioni non si limitano agli errori che possono derivare dal malfunzionamento di tali sistemi, ma riguardano il modo in cui questi sistemi trasformano alla radice le operazioni militari. Respingiamo pertanto la premessa secondo cui, allo stato attuale, correzioni tecniche o funzionali — che si tratti di un presunto "uomo nel circuito" (human in the loop) o di supposte barriere di sicurezza "cablate" nei modelli di IA — possano prevenire le conseguenze letali e devastanti delle kill chain accelerate dall'IA. Tali proposte permettono la normalizzazione e la proliferazione dell'integrazione dell'IA nel processo decisionale militare, a danno delle comunità e delle popolazioni vulnerabili. Allo stato attuale, un controllo umano significativo, una reale assunzione di responsabilità, la supervisione e la trasparenza di queste tecnologie non sono possibili nella loro forma odierna.

Anche quando i sistemi di IA usati per l'acquisizione degli obiettivi non prendono la decisione finale di uccidere, rischiano di diventare meccanismi di mera ratifica per l'uccisione su larga scala, perché fanno leva su false nozioni di oggettività e possono spostare altrove la responsabilità e la dovuta diligenza, finendo per accelerare e snellire l'uccisione di massa. Sovrapporre a questi sistemi tecniche ancora più "prive di attrito" di sorveglianza, acquisizione degli obiettivi e operazioni di comando — ad esempio sotto forma di grandi modelli di IA come gli LLM — automatizza la disumanizzazione, riducendo le questioni di vita e di morte a un semplice prompt di chat. La decisione di uccidere un altro essere umano porta con sé un grave peso morale e giuridico e non deve mai essere ridotta al puro accettare o rifiutare le raccomandazioni di sistemi di IA. Quando gli eserciti si affidano all'IA per accelerare l'identificazione degli obiettivi con una velocità e una routinizzazione tali che qualsiasi revisione umana rischia di diventare una mera ratifica priva di controllo umano significativo, l'uccisione di massa può seguirne e spesso ne seguirà, in diretta violazione del principio di precauzione del DIU.

Le aziende hanno la responsabilità di rispettare i diritti umani e di astenersi dal causare o contribuire ad abusi e ad altre violazioni del diritto internazionale, compreso il fornire sostegno materiale o finanziario a Stati coinvolti in crimini internazionali. Come stabilito dai Principi Guida delle Nazioni Unite su imprese e diritti umani, le aziende che adottano tali comportamenti devono cessare immediatamente il loro contributo al danno. Anche quando un'azienda non causa né contribuisce al danno, ma è semplicemente collegata a esso, ci si attende che usi la propria capacità di influenza per cercare di porre fine a tali violazioni.

Una volta stipulati contratti militari, le aziende possono avere un controllo limitato su come i loro prodotti e servizi vengano utilizzati, come dimostrato dal braccio di ferro tra Anthropic e il governo statunitense, oltre che dalle notizie di Google e Amazon che avrebbero sospeso l'applicabilità dei propri termini di servizio nei contratti con il governo israeliano. Ancora di recente, il 27 aprile 2026, più di 560 dipendenti di Google hanno firmato una lettera aperta all'amministratore delegato della società, sollecitandola a rifiutare l'uso della propria tecnologia di IA da parte del governo statunitense in operazioni militari classificate.

Le aziende tecnologiche e i loro dirigenti dovrebbero prendere sul serio la propria potenziale responsabilità nei casi in cui le loro tecnologie giochino un ruolo in violazioni del diritto internazionale, prima di stipulare questi lucrosi contratti di difesa, e astenersi dal farlo laddove non siano in grado di compiere tale valutazione. Oltre a ciò, devono anche comprendere il ruolo che hanno nel ridisegnare l'architettura normativa dell'uso dell'IA nei conflitti.

Noi, organizzazioni e individui firmatari, chiediamo:

Alle aziende tecnologiche di:

- astenersi dallo stipulare o dare esecuzione a contratti con agenzie militari o gruppi armati che commettono possibili violazioni del diritto internazionale, comprese violazioni dei diritti umani e crimini atroci;
- astenersi dal vendere, trasferire, fornire assistenza o esportare sistemi di IA di supporto alle decisioni destinati alle kill chain militari e al targeting di esseri umani, compresi i sistemi di generazione degli obiettivi e la sorveglianza biometrica da remoto;
- astenersi dal vendere o esportare sistemi di IA di supporto alle decisioni per scopi non letali, compresi i modelli di IA multimodali come gli LLM, destinati all'uso nei processi decisionali militari, finché non saranno possibili una reale assunzione di responsabilità, un controllo umano significativo, supervisione e trasparenza in linea con i principi del diritto internazionale umanitario e dei diritti umani.

Agli Stati di:

- interrompere l'uso di strumenti di IA, compresi i grandi modelli linguistici, nella conduzione del targeting militare, e garantire il rispetto dei principi del diritto internazionale umanitario e dei diritti umani;
- garantire trasparenza su come l'IA viene attualmente utilizzata nella condotta delle ostilità.