CIRCOLO DI STUDI DIPLOMATICI
Piazzale della Farnesina, 1
00135 Roma

LETTERA DIPLOMATICA
n. 1360 – Anno MMXXIII
Roma,20 settembre 2023

1. L'INTELLIGENZA ARTIFICIALE E IL SUO IMPIEGO NEL QUADRO DELLA SICUREZZA E DIFESA

Dagli scacchi ai droni passando per Alexa

Nel 1997, Garry Kasparov il più grande scacchista al mondo, venne battuto in 19 mosse da Deep Blue, il super computer dell'IBM. Solo pochi anni prima era impensabile che una macchina potesse prevalere sull'intelligenza umana da cui era stata creata.

Deep Blue basava la sua "bravura" su programmi incentrati su mosse concepite da esperti giocatori. In altre parole, il software del computer si fondava su strategie e mosse elaborate da esseri umani. Il vantaggio competitivo della macchina risiedeva nella sua strabiliante velocità di calcolo che gli permetteva di analizzare 200 milioni di mosse al secondo.

Ma nel 2017 il programma di scacchi allora più potente al mondo è stato clamorosamente battuto da AlphaZero, un algoritmo sviluppato da Google. Si trattava di vera rivoluzione perché AlphaZero non operava sulla base di strategie programmate da esseri umani. La sua abilità era frutto di un addestramento dell'Intelligenza Artificiale alla quale i creatori avevano" insegnato ad imparare" per ottenere il massimo numero di vittorie. Alpha Zero eseguiva mosse che nessun giocatore aveva mai previsto. Sacrificava pezzi all'inizio della partita che i giocatori umani ritenevano essenziali come la regina. Ma che succederebbe, si chiede H. Kissinger, nel suo ultimo libro "l'Era dell'intelligenza Artificiale", se per ragioni di sicurezza nazionale l'IA decidesse che vanno sacrificati un gran numero di cittadini per garantirsi la vittoria sul nemico?

La rivoluzionaria intelligenza artificiale, per quanto si tratti di una tecnologia complessa, si può sintetizzare in un'idea di fondo semplice: sviluppare sistemi hardware e software dotati di capacità di imparare autonomamente dai dati che gli vengono forniti e capace di costruire un modello autonomo ed originale per ogni specifico problema che gli si presenta.

Il salto concettuale e culturale introdotto dall'intelligenza artificiale nella tecnologia informatica va molto oltre la comune innovazione a cui siamo abituati: ora le macchine possono apprendere e agire con processi simili a quelli del cervello umano e lo fanno più rapidamente e con meno errori.

Nell'ultimo ventennio l'IA si è inserita in ogni aspetto della vita dell'uomo. Sicurezza e difesa non sono rimaste al margine. Si è ormai convinti negli ambienti della sicurezza che il mondo si trovi sull'orlo di una rivoluzione pari, e forse superiore, a quella che determinarono le armi da fuoco nel 1300 e quelle nucleari nel secolo scorso. E la competizione fra Stati per guadagnare posizioni di vantaggio nel campo dell'intelligenza artificiale applicata alla difesa è crescente.

L'IA è stata in grado di produrre una drammatica evoluzione capace di mutare la natura delle guerre attraverso l'accelerazione dei processi decisionali, dell'intelligence, della potenza e delle tipologie delle armi (per esempio l'applicazione dell'IA alla guerra cibernetica). L'IA ha infatti la capacità di mutare in modo radicale la metodologia dei conflitti. L'IA non è solo una tecnologia. È una classe di tecnologie che possono venire integrate in un ampio spettro di applicazioni anche militari.

Secondo Ian Bremmer, presidente di Eurasia Group, oggi i più avanzati modelli di IA dispongono di un potere di elaborazione 5 miliardi di volte superiore a quelli di dieci anni fa. Ed entro cinque anni saranno disponibili modelli di IA in grado di gestire cento miliardi di miliardi (100 trillion) di parametri che è circa il numero delle sinapsi del cervello umano. Nel 2018, GPT1, modello

linguistico già in grado di creare testi e rispondere a domande, lavorava con 117 milioni di parametri. Oggi GPT4 lavora con oltre 1000 miliardi di parametri.

"L'intelligenza artificiale", ha detto nel suo discorso al Parlamento Europeo sullo Stato dell'Unione il Presidente della Commissione von der Leyen il 13 settembre 2023 "procede con incrementi che i suoi creatori non avevano previsto". "Accessibile, potente, adattabile essa verrà impiegata per usi civili e militari. L'IA migliorerà l'assistenza sanitaria, incrementerà la produttività e permetterà di gestire i cambiamenti climatici. Ma oggi, affermano gli esperti, è una priorità ridurre i rischi di estinzione a causa di una pandemia o di una guerra nucleare che l'IA potrebbe provocare. L'IA ha, pertanto, bisogno di una struttura che poggi su tre pilastri: limiti, governance e innovazione guidata".

Lo stesso giorno del discorso al Parlamento europeo, il Senato americano ascoltava Altman, Gates, Zuckemberg, Musk e altri venti personaggi chiave del settore per acquisire elementi utili per regolamentare l'IA foriera di straordinari progressi e serissimi rischi. Anche la NATO, come vedremo più avanti, ha fornito linee guida per l'impiego dell'IA e sta lavorando ad una sua regolamentazione.

La "weaponisation" dell'intelligenza artificiale

Il campo della geopolitica, della guerra e della deterrenza, è probabilmente quello che subirà a causa dell'AI le maggiori trasformazioni, secondo Michael Hirsh in "How AI Will Revolutionize Warfare". Gli Stati Uniti hanno investito molte risorse soprattutto nell'IA applicata alle forze aeree sviluppando la capacità di pilotaggio autonomo di aerei F16 in operazione. I cinesi non sono da meno in ogni settore delle forze armate. I russi stanno lavorando sull'IA applicata all'operatività dei carri. Nuovi sistemi d'arma come sciami di aerei senza pilota che affiancano e assistono in varie funzioni aerei pilotati da esseri umani sono l'ultimo grido dell'aeronautica americana. Volendo essere ottimisti potrebbe risultarne una guerra meno letale e la deterrenza potrebbe essere rinforzata dallo sviluppo dell'IA. L'aumento esponenziale dei droni in campo terrestre, navale ed aeronautico potrebbe ridurre perdite umane in guerra. Tuttavia, prevale al momento la preoccupazione per i rischi che incontrollate applicazioni dell'IA in campo militare potrebbero comportare per l'umanità. Uno dei problemi che si pongono negli attuali conflitti, che è molto evidente in quello russo-ucraino, è la riduzione dei tempi necessari per identificare il bersaglio, comunicare la sua posizione alle proprie artiglierie, colpirlo e spostarsi rapidamente per non subire il fuoco avversario avendo rivelato con l'attacco la propria posizione. L'IA sta riducendo enormemente i tempi di questo processo che implica conoscenza di dati, elaborazione ed azione. La compressione dei tempi per l'azione è gravida di conseguenze nei processi decisionali sul campo di battaglia. Uno dei principali rischi è che questa accelerazione induca progressivamente l'affermazione di sistemi di IA che si sostituiscano all'intervento umano. Se tale evoluzione presenta già dei rischi nelle guerre convenzionali in un potenziale conflitto nucleare il pericolo per l'umanità aumenterebbe in modo esponenziale. Nel gennaio scorso il dipartimento della difesa americana ha pertanto aggiornato la direttiva sui sistemi d'arma che implicano l'impiego dell'IA inserendo nelle direttive ai comandi l'obbligo di una valutazione umana che preceda il loro impiego. Cionondimeno il Pentagono non ha accennato a diminuire i programmi di sviluppo per l'integrazione dell'IA nei processi decisionali anche se il direttore del centro di intelligence della Difesa, Gen. Shavahan, ha affermato che "tale integrazione non riguarderà il comando e controllo delle forze nucleari". Una riluttanza a livello politico, forse ancora maggiore di quella americana nei confronti delle armi autonome, è presente anche in Russia e in Cina. Una caratteristica comune tanto alla Cina come alla Russia riguarda infatti la centralizzazione dei processi decisionali. La dirigenza politica cinese ha sempre affermato finora il controllo politico su quello militare. Sarebbe sorprendente che esso voglia delegare a dei computer ciò che non è

disposto a delegare neppure alla classe militare per timore di perdere il controllo assoluto del comando. È dunque probabile che la tendenza sia quella di conservare, per quanto possibile, il controllo umano dei sistemi di difesa. Per affermazione diretta di Xi Jiping ciò è scontato per quanto riguarda le armi nucleari che sarebbero escluse da qualsiasi meccanismo di attivazione autonoma così come avviene negli Stati Uniti. Queste le intenzioni. Ma le contingenze e gli interessi, come sappiamo dalla storia, possono mutare i buoni propositi.

La competizione fra Potenze

Le due maggiori potenze che già si affrontano nella competizione per il dominio nel campo dell'IA sono Stati Uniti e Cina. Secondo Paul Sharre, noto autore negli ambienti dell'IA per la difesa, nel suo ultimo libro del 2023 "Four Battlegrounds", i quattro campi di battaglia sui quali avrà luogo la contesa sono i talenti, gli attori (pubblici e privati) che operano in campo tecnologico, i computer e i dati. "Il Paese che prevarrà nella competizione per queste quattro risorse acquisirà vantaggi significativi in campo politico, economico e militare. Disporrà di maggiori informazioni dell'avversario e sarà più efficace nell'uso della forza militare. Dominerà l'informazione ed il cyberspace. Sarà più letale nei conflitti".

Gli Stati Uniti possiedono numerosi talenti e sono più avanti nella ricerca e nella tecnologia. In questo campo gli USA sono il paese che presenta maggiori attrattive a livello globale per simili talenti anche se la Cina ha prodotto il quadruplo dei laureati in IA degli USA ed in Cina vi sono 400 università che offrono lauree in questa materia. L'orientamento della ricerca è diverso nei due paesi. In Cina gli studi sono diretti verso il riconoscimento di immagini ed in particolare il riconoscimento facciale, l'azione e la traduzione linguistica. Negli USA l'attenzione è più rivolta verso la comprensione e l'elaborazione dei testi, il riconoscimento vocale. Paradossalmente, comunque, l'interazione tra le due comunità scientifiche è ancora elevata e nel 2021 sono stati pubblicati 10mila studi congiunti sino-americani. Un fatto questo che potrebbe in prospettiva favorire un certo dialogo.

La Cina è indietro nella produzione dei chip ma con 900 milioni di utenti ha una superiore disponibilità di dati senza vincoli sul piano della privacy. Varie App cinesi dispongono di enormi bacini di utenza ai quali il Partito Comunista accede senza restrizioni.

Fra gli attori un ruolo essenziale viene svolto dalle società private. Il confine fra impiego civile e militare dell'IA è indefinito e l'osmosi di conoscenze fra l'uno e l'altro, così come il dual use dei sistemi civili e militari è intrinseco a queste tecnologie. Google, Microsoft, TikTok, e Alibaba sono imprescindibili protagonisti nello sviluppo dell'IA e come tali andranno inevitabilmente coinvolti nella pianificazione e sviluppo dei sistemi di IA nella difesa. A questo proposito va notato che le società private cinesi sono massicciamente finanziate dallo Stato e la sinergia tra pubblico e privato è molto più stretta che negli Stati Uniti o in Europa.

Disporre di computer di grande potenza per elaborare efficaci modelli di intelligenza artificiale è un requisito indispensabile per prevalere in questo campo. Ciò significa hardware, chips ed energia. I nuovi potenti computer con grande capacità di calcolo sono via via più complessi e costosi. I chips necessari per l'IA rappresenteranno nel 2025 il 20% del mercato dei semi-conduttori. Questo è il settore nel quale gli USA esercitano il maggior controllo nelle esportazioni verso la Cina anche attraverso pressioni su altri Paesi produttori.

L'IA sostenuta da grandi quantità di dati sarà fondamentale nelle guerre del futuro. Tuttavia, secondo alcuni autori essa non trasformerà in modo radicale il combattimento. L'intelligenza umana rimarrà in controllo dei sistemi d'arma letali, inclusi quelli che operano da remoto (droni). La situazione in area di combattimento è quasi sempre confusa e complessa e per operare efficacemente un sistema d'arma saranno sempre necessarie l'abilità, l'astuzia e la presenza del giudizio umano. Ma un paese che intenda prevalere in un conflitto armato avrà sempre più bisogno di "big-data" e della capacità di analizzare, attraverso l'IA

l'informazione proveniente dal campo di battaglia. Necessiterà di computer efficienti, di algoritmi e software per gestire l'informazione nonché di scienziati, ingegneri e programmatori nei posti di comando per utilizzarli al meglio. La guerra russo-ucraina già fornisce una percezione chiara del vantaggio di chi può condurre operazioni militari basate sull'elaborazione di dati attraverso l'IA.

L'energia necessaria per la creazione di modelli di IA è molto superiore a quella già enorme necessaria al "mining" dei bitcoin. Ciò significa che le società interessate allo sviluppo dell'IA si dirigeranno sempre più anche verso l'acquisizione di fonti di energia. La disponibilità di fonti energetiche e di acqua per raffreddare i computer sarà dunque un vantaggio per lo sviluppo dell'IA.

Un dettagliato studio della RAND "Military Application of AI" commissionato dal Pentagono esamina in profondità molteplici temi attinenti all'uso dell'IA in ambito militare negli USA, Cina e Russia.

Secondo tale studio, gli Stati Uniti hanno finora sviluppato un assortimento di tecnologie militari con vari gradi di autonomia. La leadership politica è stata prudente nel valutare la decisione di dispiegare armi autonome e anche coloro che ritengono sia necessario incoraggiarne lo sviluppo, ma non il dispiegamento, restano di questa opinione. Alcuni sistemi "difensivi" (missili Aegis e Phalanx) sono giunti ad uno stadio operativo per i vantaggi che essi offrono sia in velocità che in manovrabilità in caso di attacchi simultanei di grande portata. Contrariamente nel caso di applicazioni "offensive" l'atteggiamento di leader politici è più conservatore. Questo perché il vantaggio della velocità è meno pressante nel caso di operazioni offensive. Avendo gli attaccanti l'opzione dell'iniziativa possono scegliere tempi e modi dell'attacco obbligando i difensori a reagire. Inoltre, le operazioni offensive implicano delle resistenze etiche maggiori. Gli attaccanti possono decidere di non attaccare se ciò pone in pericolo dei civili. I difensori invece non dispongono di tale scelta e viene loro riconosciuta una maggior libertà di azione sul piano etico essendo costretti a salvare la loro vita. Il risultato di queste considerazioni è che la leadership americana non ha voluto dispiegare armi offensive autonome malgrado esse siano state già sviluppate ed utilizzate in esercitazione.

Il progetto "Maven" costituisce un interessante esempio in materia di resistenze etiche e politiche. Esso consiste in un modello atto ad analizzare filmati e fotografie raccolti da droni e satelliti con lo scopo di accelerare l'integrazione dei big data e "machine learning". Il progetto nato nel 2017 ad opera di Google è gestito dallo scorso anno direttamente dall'Agenzia Geospaziale di Intelligence poiché i dipendenti di Google hanno rifiutato di continuare a svilupparlo malgrado il progetto fosse limitato alla raccolta ed all'elaborazione di dati e non alla gestione di armamenti. La "resistenza etica" dei componenti civili coinvolti nel progetto potrebbe metterne ancora in forse l'ulteriore sviluppo. Si tratta di un chiaro esempio di come gli aspetti etici riguardanti l'IA applicata alla difesa siano politicamente rilevanti nelle democrazie occidentali.

La Cina secondo la RAND sta attivamente sviluppando l'IA e la robotica applicata alla difesa. Attualmente non si conoscono sistemi d'arma cinesi completamente autonomi. Tuttavia, alcuni di essi lo sono già in alto grado e potrebbero facilmente operare senza il controllo umano se il loro software venisse modificato. Abbiamo già accennato alla riluttanza del Partito a cedere qualsiasi tipo di controllo significativo ad altri attori siano essi comandanti militari o modelli di software. Pechino sta conducendo ricerche nell'identificazione di bersagli tramite l'IA che potrebbe rendere i sistemi d'arma più indipendenti dagli operatori umani. Altri studi riguardano sistemi autonomi atti a fornire informazioni volte a facilitare ed accelerare i processi decisionali. Sarebbe opportuno, secondo lo studio della Rand, che gli Stati Uniti ingaggiassero Pechino in un negoziato per il bando di armi autonome letali. Purtroppo, malgrado le richieste dell'amministrazione americana di avviare discussioni "military to military" durante la visita del Segretario di Stato Blinken a

Pechino nel giugno 2023, nelle quali l'IA avrebbe certamente costituito un punto centrale dell'agenda, la Cina ha rifiutato l'incontro. L'Occidente probabilmente avrebbe tutto da guadagnare da un trattato che introducesse l'obbligo del controllo umano delle armi autonome poiché gli standard etici nelle democrazie sono certamente più severi.

La Cina è molto avanti anche nello sviluppo del "concetto operativo" nell'impiego dell'IA in campo militare e nella "cognitive warfare". Xi ha lanciato l'idea, che in italiano viene tradotta con il neologismo "intellicizzazione dello strumento militare" per descrivere la chiave della riforma militare cinese tuttora in atto. La Cina dipende per l'85% da importazioni nel settore dei microchip che sono indispensabili per lo sviluppo dell'IA e che vengono fortemente ostacolate dagli USA. Tuttavia, nel campo strategico, sostiene Mr. Takaci, responsabile del Ministero della Difesa giapponese per la sicurezza in Asia orientale, i cinesi sanno che l'abilità nello sviluppare un concetto innovativo di impego tattico di un sistema può far prevalere chi lo mette in atto su un avversario che dispone di forze superiori. Un esempio storico è la rapida vittoria della Germania sulla Francia all'inizio della Seconda guerra mondiale grazie ad un impiego innovativo dei carri armati (Blitzkrieg) malgrado la Francia disponesse di carri più numerosi e performanti dei tedeschi. E nella guerra franco-prussiana, malgrado la Francia disponesse di una tecnologia superiore a quella prussiana in campo ferroviario, Moltke riuscì a prevalere sui francesi usando le ferrovie per disperdere e poi concentrare, manovrandole simultaneamente, le truppe prussiane sull'obiettivo (idea che richiama quella dello sciame di droni). La Cina sta investendo molte risorse nella "cognitive warfare" che può essere definita come una dottrina volta a valutare e sfruttare a proprio vantaggio, con l'ausilio dell'IA ed il suo straordinario effetto moltiplicatore di analisi, aspetti psicologici, culturali ed emotivi che guidano le decisioni umane in sincronia con altri strumenti di potere. Essa mira ad influenzare l'avversario e ad ottenere il sopravvento su quest'ultimo e non implica necessariamente lo scontro. Il suo ambito di azione si situa piuttosto al di sotto della soglia del conflitto militare.

La Russia si trova in una fase molto meno avanzata della Cina, per non parlare degli USA, nel campo dell'IA. Le prospettive di sviluppo russe sono limitate da fattori strutturali, demografici e culturali. Il bilancio russo è inferiore a quello degli USA e della Cina e la Russia soffre da tempo di un continuo esodo di talenti dal Paese. Inoltre, come la Cina, la Russia è caratterizzata da una forte centralizzazione decisionale. La leadership politica e gli alti comandi russi non consentirebbero l'uso di armi autonome o anche semi-autonome in scenari dove errori tecnici possano generare situazioni escalatorie. Tuttavia, una minor riluttanza verso l'impiego di armi autonome, potrebbe derivare dalla percezione, nell'attuale guerra in Ucraina, di una reale minaccia alla sicurezza del proprio territorio. La preoccupazione strategica potrebbe rappresentare per la Russia una priorità. In tal caso Mosca potrebbe essere indotta ad usare le proprie, anche se limitate capacità, nel campo della tecnologia militare nell'IA impiegandole in modo più aggressivo dell'avversario. La Russia inoltre sta imparando molto rapidamente dal confronto con le forze ucraine nel campo della IA applicata alla guerra.

L'IA in campo militare in Gran Bretagna, Francia e Italia

Gran Bretagna: ambizioso, articolato, pragmatico ed informativo appare il sito del Department of Defence britannico sul tema dell'IA nella difesa. In 72 pagine è indicata con dettaglio non solo la catena di comando della governance in materia ma in modo chiaro la policy dell'impiego dell'IA nella difesa sostenuta da esempi pratici "…i comandi britannici possono esercitare un controllo rigoroso ed adeguato su sistemi d'arma IA anche senza una vigilanza permanente e diretta della supervisione umana. È il caso di una piattaforma navale in grado di proteggersi da missili ipersonico con sistemi autonomi che reagiscono più rapidamente di come potrebbero fare degli esseri umani". In quest'ultimo caso il DoD

introduce i limiti del mare aperto e quello di una specifica minaccia di un missile supersonico entro i quali il sistema può operare in modo completamente autonomo. Per quanto riguarda il bilancio sono stati accantonati per gli anni 2024-2025 6.6miliardi di sterline per ricerca e sviluppo e viene specificato che "ciò fornisce un'idea delle necessità per far fronte a future minacce incluse quelle derivanti dall'IA e dalle armi ad energia diretta" (armi laser).

Francia: il Ministero della Difesa pubblica sul sito l'entità dello stanziamento relativo alla ricerca e sviluppo dell'IA in ambito militare che ammonta a 700 milioni di € stanziati per il periodo 2019-2025; il reclutamento di 200 specialisti entro l'anno in corso (2023); il coinvolgimento di 5 Direzioni Generali del Ministero della Difesa; ribadisce lo stretto coordinamento con i principali attori nel campo dell'innovazione, della ricerca e nell'industria della difesa; conferma la volontà di mantenere nelle mani dei comandi militari l'impiego delle armi escludendo a priori, come fanno almeno a parole tutti gli altri, l'opzione "out of the loop" dell'operatore umano senza limiti.

Italia: nel percorrere i siti del Ministero della Difesa, degli Stati Maggiori, del CASD e del Cemiss si riscontra un'intensa attività di brainstorming sull'intelligenza artificiale, le "emerging diruptive technologies", le operazioni multidomino, la "cognitive warfare". Gli uffici di riferimento, al Ministero della Difesa per l'intelligenza artificiale sono l'UGID (Ufficio Generale Innovazione Difesa) e, al Segretariato della Difesa il V Reparto.

Nel bilancio Difesa per il 2023, su un totale di 27.748,5 milioni di euro, il Capitolo di Spesa 7420 prevede 120,3 milioni per "Interventi per l'attuazione di programmi ad alta valenza tecnologica" e il Capitolo 7421 877,9 milioni per "Interventi per lo sviluppo delle attività industriali ad alta tecnologia nei settori aeronautico ed aerospazio" che includono ricerca e sviluppo sul tema dell'AI in misura non specificata. Il parere espresso dal Ministero della Difesa in Commissione Difesa della Camera sul PNRR sottolinea "l'esigenza di valorizzare il contributo a favore della Difesa sviluppando le applicazioni dell'intelligenza artificiale".

Secondo le informazioni raccolte, le Forze Armate italiane non dispongono di sistemi d'arma con capacità totalmente autonome. Nel settore privato, Leonardo, l'azienda italiana considerata la prima società nel settore della Difesa nella UE, sta sviluppando da anni tecnologie direttamente o indirettamente collegate all'AI precisando "di aderire agli standard che assicurano che l'utilizzo dei sistemi d'arma autonomi garantiscano sempre un controllo umano on the loop o in the loop".

Accanto alle aziende private è da sottolineare il contributo delle Istituzioni accademiche quali il Politecnico di Milano e la Sapienza di Roma che hanno sviluppato negli ultimi anni diversi progetti, tra cui i velivoli UAV, in sciame o singoli, dotati di apprendimento statistico, identificazione automatica di bersagli, capacità di sorveglianza di aree prestabilite, in missioni operative e innovativi sistemi di guida autonoma di veicoli terrestri.

Lezioni dall'Ucraina

Malgrado la crescente pervasività dell'IA e della guerra cibernetica il conflitto in Ucraina ci dice che la guerra non è tutta IA e cyber. L'importanza della preparazione e del numero dei soldati, l'artiglieria, la quantità di munizioni disponibili giocano ancora un grande ruolo. Ciò che la guerra sta provando è che la "massa" in termini di forza d'urto (soldati, armi, munizioni, logistica) e la "tecnologia IA" associata a satelliti, droni, intelligence elettronica, vadano interconnesse per prevalere sul nemico. Il fattore tempo è divenuto in questa equazione un elemento centrale.

Gli ucraini hanno raggiunto risultati incredibili inventando un combattimento nel quale una varietà di sensori (video, intercettazioni di comunicazioni telefoniche, immagini termiche, radar, radio-antenne) sono in grado di scoprire bersagli nemici e comunicare la loro posizione con rapidità alla migliore arma in quel momento disponibile. Essi hanno creato ciò che viene definita una "kill-chain o kill-web" di efficacia e rapidità senza precedenti. Una app privata creata dagli

ucraini chiamata “l’Uber delle artiglierie” permette di condividere in tempo reale con tutte le batterie della zona le posizioni del nemico ed intervenire con efficienza e rapidità impensabili con sistemi di comunicazione tradizionali. Ma anche i russi stanno rapidamente imparando dalle innovazioni degli avversari ucraini.

I droni che identificano autonomamente i carri armati attraverso sistemi di IA forniscono al software un elevatissimo numero di immagini di carri nelle più diverse configurazioni: mimetizzati, immersi nel fango, semi nascosti dagli alberi. Inoltre, devono essere in grado di distinguerli da veicoli civili, agricoli e per il trasporto merci. Capire se il carro è amico o nemico. In questo momento l’Ucraina è l’unico posto al mondo dove sia possibile raccogliere un’enormità di dati che le forze ucraine ed i Paesi e le società di software che le assistono stanno accumulando da 18 mesi. Alla fine della guerra gli enti e le aziende che dispongono di queste informazioni saranno in grado di offrire prodotti assolutamente originali in campo militare. È ovvio che tale messe di informazioni sia davvero attraente per gli Stati maggiori, l’intelligence e l’industria di molti Paesi.

La tecnologia coinvolge sempre più anche civili come forze combattenti. Nella guerra in Ucraina la popolazione civile opera al cuore della resistenza contro la Russia. Con la maggioranza dei civili in possesso di smartphone, l’Ucraina dispone di fatto di un esercito di 200 mila persone che agiscono come altrettanti attori nell’intelligence per la localizzazione del nemico, come hakers che operano attacchi su obiettivi russi in Ucraina, o in Russia, e attraverso piattaforme satellitari commerciali, nel mondo. Ciò comporta conseguenze legali rilevanti. Infatti, uno dei principi cardine del diritto internazionale è la discriminazione fra combattenti e non combattenti. Se i civili identificano bersagli nemici, guidano su di essi droni, minacciano strutture civili del nemico ovunque esse si trovino sono ancora protetti dal diritto internazionale come soggetti civili o diventano piuttosto potenziali legittimi bersagli militari? Secondo la Convenzione di Ginevra, infatti, i civili che prendono parte diretta nelle ostilità perdono tale protezione.

Anche in mare come a terra ed in aria il ruolo dei droni è in forte espansione. Se la marina russa possiede unità di superficie in Mar Nero in misura molto superiore all’Ucraina quest’ultima può limitarne notevolmente i movimenti vicino alla costa grazie a modelli di IA connessi con droni ed artiglieria. I droni navali (molto simili ai “barchini esplosivi” italiani della Prima e Seconda guerra mondiale) dotati di sistemi di guida moderni, di IA e comunicazioni satellitare sono la maggior minaccia per la flotta russa.

La guerra del futuro sarà una guerra di IA e droni anche in mare. Dopo l’attacco al North Stream Pipeline, la minaccia alle infrastrutture subacquee è percepita come un rischio prioritario. Nel Mare del Nord, 600 droni subacquei, alcuni dei quali completamente autonomi, sorvegliano per conto di Gran Bretagna, Norvegia, Danimarca e Germania una area di 9mila km2. La NATO ha creato quest’anno una nuova cellula di coordinamento interalleato per la difesa sottomarina.

Conclusioni

L’introduzione dell’intelligenza artificiale nel settore della difesa condizionerà molti aspetti dei prossimi conflitti, specialmente se applicata a tecnologie distruttive emergenti, nelle quali l’IA giocherà un ruolo chiave. Esse comprendono, oltre ai sistemi autonomi applicati a numerose tipologie di armamenti, le biotecnologie (in particolare la creazione di DNA), le tecnologie spaziali (missili ipersonici e sistemi laser in orbita), i computer quantici. L’IA è una materia ancora volatile dove non esistono definizioni o interpretazioni condivise né una comune percezione dei vantaggi e dei pericoli che tali tecnologie comportano. Alcune recenti riflessioni di alleati europei sottolineano la necessità di creare una metodologia volta alla definizione di un linguaggio e di strategie comuni da adottare a livello internazionale. Concrete proposte di sistematizzazione miranti a creare un inventario di tali tecnologie ed un’analisi dei rischi e delle opportunità che esse comportano stanno

attualmente circolando per iniziativa di alcuni Paesi. Fra i rischi, ad esempio, quello dell'abbassamento della soglia dell'uso della forza generato da tecnologie distruttive non tradizionali come quelle cyber. Fra le opportunità quella di accrescere l'efficacia dei meccanismi di controllo degli armamenti. Si tratta di uno sforzo finalizzato alla ricerca dei più adatti strumenti internazionali volti alla regolamentazione di questa complessa materia che tenga conto delle sensibilità e degli interessi dei numerosi attori coinvolti: governi, istituzioni pubbliche, industria e società civile.

Stefano Ronca

BIBLIOGRAFIA

Libri:

- "Four Battlegrounds: Power in the Age of Artificial Intelligence", Paul Sharre, February 2023
- "L'era dell'intelligenza artificiale", Henry A. Kissinger, Eric Schmidt, Daniel Huttenlocher, Giugno 2023
- "Scary Smart: The Future of Artificial Intelligence and How You Can Save Our World", Mo Gawdat, September 2021
- "Artificial Intelligence and Warfare", Clay Wilson, June 2020

Documenti ufficiali:

- REAIM, Responsible AI in the Military domain – Summit The Hague, The Netherlands co-hosted by the Republic of Korea February 15-16, 2023
- Artificial Intelligence in Military Domain – Conference on Disarmament – Delegation of the EU to the UN in Geneva, 3 August 2023
- Remarks to the Security Council of the Secretary-General on Artificial Intelligence - New York, 18 July 2023
- Law of Armed Forces (LOAC), Schriever AFB Legal Office, March 2020
- Cognitive Warfare. La competizione nella dimensione cognitiva, Stato Maggiore della Difesa, Edizione 2023
- Artificial Intelligence Act. EU Research Service, June 2023
- Nato Artificial Intelligence Strategy, 22 October 2021

Siti web:

- L'intelligence artificielle et le monde de la défense | entreprises.gouv.fr – Ministère de l'économie, des finances et de la souveraineté industrielle et numérique, 1/3/2023
- BANKRUPTCY (spaceforce.mil) – Law of Armed Forces LOAC, March 2020
- Defence Artificial Intelligence Strategy - GOV.UK (www.gov.uk), 2023
- Nato Website, 7 february 2023

Blog:

- Intelligenza Artificiale (AI): cos'è, come funziona e come applicarla (osservatori.net)

Articoli, pubblicazioni e riviste:

- « How AI Will Revolutionize Warfare – The new arms race in technology has no rules and few guardrails", Michael Hirsh, 11/4/2023
- "The war in Ukraine shows how technology is changing the battlefield", Special report, The Economist, July 2023
- "How oceans became new technological battlefields", Special report, The Economist, July 2023
- "How Ukraine's enemy is also learning lessons, albeit slowly", Special report, The Economist, July 2023
- "Technology is deepening civilian involvement in war", Special report, The economist, July 2023
- "Can China Build a World-Class Military Using Artificial Intelligence?", Koichiro Tagaki, Hudson, 7/2/2023
- "The weaponization of artificial intelligence: What the public needs to be aware of", Brigitta Dresp-Langley, Frontier in Artificial Intelligence, 8/March/2023
- "Ukraine A Living Lab for AI Warfare!, Robin Frontes and Dr Jorrit Kamminga, RealClear Defense, 3/24/2023
- "AI weapons. In China's Military Innovation", Elsa B. Kania, Global China in partnership with Center for Security and Emerging Technology, 27/4/2020
- "Lethal Autonomous Weapon System (LAWS)", United Nations Office for Disarmament Affairs, 2023
- "The Continued Evolution of U.S. Law of Armed Conflict Implementation", Bryan Frederick and David E. Johnson, RAND Corporation, 2020
- "The commanding heights of ai", Eurasia Group politics first, Top risks 2023
- Ian Bremmer: the AI power paradoxe, Foreign Affairs, May 2023
- "Why the EU must now tackle the risks posed by military AI", Rosanna Fanni, CEPS, 08 June 2023
- "Altreconomia: Sistemi d'arma autonomi in Italia", Luca Rondi, 28 giugno 2023
- "Analisi Difesa: Il bilancio della Difesa italiana", G. Martinelli, 2023
- "Responsible military use of artificial intelligence", Vincent Boulanin, Netta Goussac, Laura Bruun and Luke Richards, Sipri, November 2020

Si ricorda che il Circolo di Studi Diplomatici è nell'elenco degli Enti di ricerca che possono essere destinatari del cinque per mille. Il beneficio può esserci attribuito indicando il codice fiscale del Circolo (80055250585) nel relativo riquadro del modello per l'attribuzione del cinque per mille per la ricerca.

L'Archivio del Circolo di Studi Diplomatici è consultabile al link https://circolostudidiplomatici.unilink.it

CIRCOLO DI STUDI DIPLOMATICI «Lettera Diplomatica»
Direttore Resp.: Paolo Casardi
Autorizzazione Trib. Roma N. 249/82 del 30-6-82

Direzione, Redazione: Piazzale della Farnesina, 1 – 00135 Roma
Per gli abbonamenti: Tel: 340.86.57.044 - e-mail: **studidiplomatici@libero.it**
https://www.esteri.it/it/ministero/sindacati-e-associazioni/circolostudidiplomatici/
Conto corrente bancario: UniCredit S.p.A. - Distretto ROMA Via del Corso "A"
Via del Corso, 307 - 00186 Roma
c/c n° 000401005051 - IT 84 P 02008 05181 000401005051