WINNING THE ARTIFICIAL INTELLIGENCE ERA.

QUANTUM DIPLOMACY AND THE POWER OF AUTOMATION

CAPITOLO I e II

È possibile quantizzare le relazioni internazionali?

Tecnologie quantistiche e relazioni internazionali

di Enrico Prati

La riscoperta della fisica quantistica e dell'intelligenza artificiale

Tra i fattori dell'accelerazione tecnologica a cui assistiamo in questi ultimi anni spiccano discipline come la meccanica quantistica e l'intelligenza artificiale. Nonostante siano state fondate rispettivamente circa cento e settanta anni fa, e sappiamo sfruttarle già da decenni – si pensi ai laser o a Deep Blue che battè Garry Kasparov, allora campione del mondo in carica nel gioco degli scacchi, è da pochi anni che assistiamo a un nuovo e moderno loro impiego: sono notizie di recente memoria il cosiddetto quantum advantage del computer quantistico di Google annunciato nel 2019 o al deep learning applicato al riconoscimento dei danni alla retina o dei tumori. Queste innovazioni sono generaliste, come lo è stato il computer, e aprono nuovi orizzonti applicativi potenzialmente in tutti gli ambiti della conoscenza.

Tuttavia i più recenti sviluppi ingegneristici e le scoperte in ambito matematico, combinati insieme, hanno permesso di aprire nuovi orizzonti tecnologi e sociali. Computer quantistici e intelligenza artificiale stanno fornendo nuova potenza computazionale – parafrasando Tom Conte dell'iniziativa IEEE Rebooting Computing, "nuovo hardware per nuovi tipi di software", che sosterranno la crescita economica di chi li controllerà e altereranno gli equilibri geopolitici per molti anni a venire.

La sfida economica

Dal punto di vista economico, tali tecnologie hanno un'importante ricaduta in termini di occupazione qualificata e di produttività. Si pensi per fare un esempio a Nvidia che dal 2006 al 2021 ha centuplicato il proprio valore in borsa, così come la creazione di nuove startup che non esistevano fino a 5 anni fa e ora sono quotate al NASDAQ come il produttore di computer quantistici IonQ il cui valore è ora a pochi mesi dall'IPO di 2.8B$ o la società di cybersecurity che impiega l'intelligenza artificiale Crowdstrike fondata nel 2011 e che valeva 1B$ nel 2017, fino al valore attuale di più di 50 B$. Sono necessarie politiche economiche su scala almeno decennale per generare un ecosistema in grado di portare a maturazione queste tecnologie, ben oltre i tempi di una singola legislatura di un Paese.

La sfida geopolitica

Dal punto di vista delle relazioni internazionali, vi sono due tipi di impatto. Il primo livello è l'impiego diretto delle tecnologie emergenti, come strumento di lettura delle dinamiche relazioni diplomatiche. Infatti, è possibile applicare le categorie di pensiero proprie della teoria quantistica alle scienze sociali, incluse le relazioni internazionali. La quantum social science è quella scienza che si pone come obiettivo di investigare i problemi delle scienze sociali, siano esse l'economia, la finanza, la psicologia, la sociologia, con l'ausilio dei metodi formali sviluppati nella teoria quantistica. I concetti di discontinuità (quantizzazione), di complementarietà, di indeterminazione, e così via, si adattano a descrivere qualitativamente i fenomeni sociali ed economici inclusi quelli inerenti le relazioni internazionali, come ad esempio lo scambio della moneta, un referendum verso una secessione, l'identità nazionale e lo stato dei rapporti tra Paesi. Tali analogie qualitative costituiscono una base per una modellizzazione anche quantitativa, che consente analisi predittive come avviene nel caso della quantum decision theory, in futuro anche grazie all'impiego dei futuri computer quantistici in via di sviluppo come dimostrano studi come quello sugli equilibri tra reti terroristiche in Siria e Iraq.

Il secondo livello invece consiste nell'impiego indiretto, come leva per vincere nella competizione economica in termini maggiore di competitività, ma anche, in termini pragmatici, come strumento di supremazia tecnologica per esercitare maggiore pressione in termini diplomatici. Lo tsunami tecnologico in corso sta alterando gli equilibri geopolitici, basti pensare alle implicazioni che ha avuto la concentrazione in oriente e in particolare con TSMC a Taiwan e Samsung in Corea del Sud che da sole producono il 70% dei semiconduttori al mondo, sulla crisi di disponibilità di processori e circuiti integrati, che ha spinto il presidente USA Joe Biden a stanziare 52 miliardi di dollari per potenziare la capacità produttiva domestica di chip, e l'Unione Europea a varare il Chips Act da 45 miliardi di euro nel Febbraio 2022.

La sfida etica

Se da un lato normativo sorgono già sfide in campo etico – si pensi ai droni militari pilotati dall'intelligenza artificiale sviluppate da alcuni Paesi come Cina e Turchia, si prefigurano anche nuovi scenari, dall'intelligenza artificiale generale in grado di emulare quella umana alle brain-machine interface come quelle di Neuralink di Elon Musk - che ha raccolto nel 2021 un nuovo round di finanziamenti da 205M$, di Amazon e di Google. Non è un caso se DARPA ha incluso le BMI nel finanziamento "AI Next" da 2B$ della terza generazione dell'intelligenza artificiale, quella che deve spingersi oltre l'attuale deep learning. Questa tecnologie non possono portare a nessun vantaggio per la società se non sarà accompagnata da una consapevole maturazione della sfera etica, della componente sociale, della trasparenza e del rispetto dei diritti e della privacy. Si tratta di una sfida interdisciplinare che richiede l'impegno di tutti gli stakeholder, e di una sintesi che solo la politica, l'arte della misura così come intesa da Platone, può restituire.

CAPITOLO III

Impiego dell'intelligenza artificiale nei sistemi d'arma: normativa internazionale

di Andrea Gilli

L'accelerazione tecnologica degli ultimi decenni nei processori, big data e machine learning hanno portato al progresso rivoluzionario dell'intelligenza artificiale. Questi sviluppi hanno attirato una rinnovata attenzione e diffusa preoccupazione riguardante i possibili rischi derivanti dal suo utilizzo soprattutto in campo militare. Per questo, studiosi ed esperti ne hanno chiesto più volte una maggior regolamentazione, controllo e persino interdizione. Tuttavia, è opportuno chiedersi se queste paure siano giustificate e se l'intelligenza artificiale possa offrire più rischi che opportunità. In questo Capitolo cerchiamo di rispondere a tale quesito, partendo dalle origini e sviluppi dell'intelligenza artificiale, la portata e le implicazioni di questa nuova tecnologia applicata al dominio militare e ai sistemi d'arma autonoma. Successivamente, sulla base di questa analisi valutiamo le critiche, di esperti e studiosi, sui rischi legati al suo uso. Infine, analizzeremo la struttura etico-legale che ne definiscono le regole di verifica e utilizzo a livello internazionale.

CAPITOLO IV

New warfare: potenziali rischi e mitigazioni

di Enrico Savio ed Enrico Comin

Le implicazioni dello sviluppo e dell'applicazione delle tecnologie disruptive nella difesa sono molteplici e stanno cambiando le "regole del gioco". I temi della velocità, dell'efficienza e della precisione; così come la necessità del controllo umano sulle capacità militari alimentate dall'IA, nonché le implicazioni etiche dell'utilizzo di tali strumenti rappresentano il cuore della questione nell'attuale dibattito sulle applicazioni dell'intelligenza artificiale e la sicurezza nazionale. […]

L'applicazione di queste tecnologie ai nuovi strumenti e metodi di guerra sta incentivando una dinamica internazionale di corsa agli armamenti sia nelle armi convenzionali che nelle disruptive technologies, mettendo in discussione gli attuali paradigmi strategici e degli equilibri di potere. […]

Nonostante non esista una definizione univoca e condivisa di intelligenza artificiale, generalmente il termine IA viene utilizzato per riferirsi a un sistema informatico con capacità cognitive al livello umano. L'IA è divisa in due categorie: IA ristretta e IA generale. I sistemi rientranti nella prima categoria possono eseguire solo il compito specifico per il quale sono stati addestrati, mentre i secondi, tramite apprendimento autonomo, potrebbero un giorno essere in grado di eseguire una vasta gamma di compiti, compresi quelli per i quali non sono stati specificamente addestrati. L'IA ristretta è attualmente integrata in numerose applicazioni militari, che includono ma non sono limitate - a intelligence, sorveglianza e ricognizione, logistica, operazioni informatiche, comando e controllo e sistemi semi-autonomi e autonomi. […]

Recenti notizie e analisi hanno ulteriormente evidenziato il ruolo dell'IA nel consentire falsificazioni e manipolazioni digitali di foto, audio e video con risultati sempre più realistici: tali prodotti fittizi sono noti come deep fakes. Queste capacità di IA potrebbero essere impiegate come parte di operazioni mirate a minare le capacità informative. Infatti, la tecnologia deep fake potrebbe essere usata per generare notizie false, influenzare l'opinione pubblica, erodere la fiducia dei cittadini e tentare il ricatto di funzionari governativi. Per questo motivo, alcuni analisti sostengono che le piattaforme di social media, oltre a impiegare strumenti di rilevamento dei deep fakes, dovrebbero rafforzare le soluzioni di classificazione e autenticazione dei contenuti. […]

Per rispondere efficacemente ai rischi generati da tali contingenze, l'era digitale richiede la creazione di elevate capacità di "cyber deterrenza". Infatti, il combattimento non si sta solo muovendo verso la robotica, ma sta anche diventando "etereo". Ad esempio, durante la sua incursione in Georgia nel 2008, la Russia è diventata la prima nazione a schierare attacchi cibernetici sui sistemi di comando, controllo e comunicazione del nemico per supportare un'invasione di terra. Allo stesso modo, per ritardare il programma nucleare iraniano, gli Stati Uniti e Israele hanno presumibilmente lanciato il virus Stuxnet, che ha compromesso le capacità delle centrifughe impegnate nel processo di arricchimento dell'uranio. La Cina è entrata in possesso di grandi database di informazioni sul personale governativo degli Stati Uniti, oltre a penetrare nelle reti degli appaltatori della difesa, delle compagnie aeree e delle aziende tecnologiche statunitensi. Questi esempi, che rappresentano solamente "la punta dell'iceberg", illustrano i sostanziali progressi nella tecnologia delle armi negli ultimi due decenni, a cui gli osservatori a volte si riferiscono come una "rivoluzione negli affari militari". […]

In uno scenario geopolitico sempre più definito da tecnologie nuove ed emergenti, la difesa nazionale si pone come una delle aree di sviluppo più consequenziali per il XXI secolo. […] Le tecnologie emergenti e disruptive stanno sfidando il modo in cui la deterrenza, la difesa e, più in generale, le strategie di sicurezza sono formulate e applicate a livello nazionale e multilaterale. Le dimensioni territoriali non rappresentano più il fattore principale per determinare il potere di uno Stato. Lo sviluppo tecnologico, l'agilità di manovra nonché la velocità e l'accuratezza del processo decisionale conteranno più delle risorse a disposizione. Pertanto, un attore di piccole dimensioni - ma con notevoli capacità tecnologiche - potrebbe essere in grado di sfidare con successo una grande potenza. […]

La deterrenza nucleare ha prodotto stabilità strategica adoperando una combinazione di negoziazione, dichiarazioni pubbliche e programmi mirati all'acquisizione di armamenti. Nell'ambiente attuale e del prossimo futuro, acquisire più armi non produrrà maggiore stabilità e la capacità di negoziare su questioni strategiche e di controllo degli armamenti con gli avversari è significativamente ridotta rispetto al passato. Trovare un modo per coordinare questo nuovo ambiente strategico e rafforzare la stabilità internazionale non è intuitivo. Infatti, considerando che gli Stati stanno cercando di ampliare la deterrenza contro rischi emergenti e contro nuove armi non nucleari, il vecchio paradigma della stabilità è ormai compromesso e dovrà essere rinnovato tenendo conto delle armi abilitate da tecnologie dirompenti e dei loro effetti sulla deterrenza. […]

In linea generale, il contesto del prossimo futuro richiede quindi il mantenimento di un primato tecnologico credibile, in grado di alimentare una deterrenza efficace che induca ipotizzabili aggressori ad effettuare - prima delle rispettive iniziative - una valutazione costo-beneficio. Senza questo primato, l'asimmetria esistente tra sistemi autocratici e democratici sarà difficilmente mitigata da qualsivoglia diplomazia e forma di diritto internazionale. […]

Si tratta di sfide globali che le nazioni non possono affrontare in solitario: per sfruttare le potenzialità e mitigare i rischi connessi all'applicazione dell'IA è opportuno valorizzare l'influenza reciproca in ottica d'interconnessione e interoperabilità a livello internazionale. Il confronto odierno avviene ed avverrà infatti con attori e regole diverse, in una cornice legale ancora da costruire, specialmente per quanto attiene le minacce ibride. Siamo dunque di fronte a molte variabili, che concorrono a creare un contesto in costante evoluzione. L'innovazione tecnologica è infatti, per sua natura, un elemento dinamico. Altrettanto lo sono gli scenari geopolitici e le diverse evoluzioni culturali che determinano le scelte dei singoli Paesi. La definizione di regole e principi etici è un cammino articolato, che è necessariamente destinato ad attraversare tale complessità per trovare un terreno comune, una sintesi capace non già di rincorrere, bensì di accompagnare e favorire l'avanzamento tecnologico in ogni campo. Da qui l'esigenza di una "consultazione permanente" tra tutti gli attori che concorrono alla definizione delle regole del vivere civile e di quelle che governano, di conseguenza, le regole del conflitto: giuristi, militari, politici, diplomazia e, non ultimo, i tecnologi: coloro che ricercano, studiano, progettano e realizzano i sistemi di difesa. Insieme, queste diverse sfere devono operare per la stessa causa: costruire una logica dinamica, circolare e iterativa che adatti il linguaggio delle macchine alle esigenze umane, tenendo conto delle questioni etiche. Un processo circolare che non deve fermarsi mai, che deve considerare scenari sempre più complessi e che permetta all'uomo di mantenere il senso del limite nella propria idea di potenza e dell'uso della forza. […]

CAPITOLO V E VI

La regolamentazione dell'intelligenza artificiale oltre i confini dell'Unione Europea: un esame comparativo

La normativa nel quadro di riferimento europeo e il caso italiano

di Antonio Malaschini

Non esiste al momento alcuna normativa di carattere complessivo sull'intelligenza artificiale, salvo la proposta dello scorso anno dell'Unione Europea.

Nei diversi paesi l'IA è regolamentata nei fatti attraverso il riferimento a norme esistenti, come Cyber Security e commercializzazione ed uso dei prodotti informatici; con l'ampliamento anche in via interpretativa della disciplina a tutela dei diritti personali o sociali; con standard di produzione e utilizzazione già pensati per altri beni: una regulation by design, quindi, piuttosto che regole rigide. Il che comporta ai nostri fini, una prevalenza degli esecutivi, più capaci di utilizzare la normativa secondaria, rispetto ai legislativi più costretti ad un iter procedurale complesso.

Perchè questo "ritardo" legislativo? Le ragioni sono molteplici: la relativa novità del fenomeno; lo sviluppo continuo di una tecnologia sempre più avanti della proposta normativa; un ritardo, forse anche culturale, dei legislatori; la ritrosia del mondo della ricerca e della produzione ad una disciplina ritenuta potenzialmente limitatrice; la complessità delle questioni, etiche e giuridiche, da affrontare.

Ma va in particolare sottolineato il carattere duale, civile e militare, del fenomeno. In diversi, importanti paesi prevalgono le valutazioni di politica globale e di confronto strategico, che non vogliono lasciare agli avversari vantaggi, appunto, strategico-militari.

Ad esempio la Cina, che per la disciplina di carattere civile fa largo uso di strumenti di indirizzo e di definizione di standards, pone nel suo "New Generation AI Development Plan" del 2017 l'area di intervento militare come privilegiata accanto a quelle dello sviluppo economico e della governance sociale.

Negli Stati Uniti la normativa sulla IA ha poi quasi sempre una sua collocazione all'interno del bilancio della difesa, evidenziando il ruolo centrale che la Presidenza, anche attraverso i suoi "Executive Orders", ha assunto nella gestione della questione. E si può anche ricordare come la National Security Commission On AI, istituita con la legge di bilancio della difesa del 2019, ponga al primo posto nelle sue conclusioni il difendere l'America e il vincere la sfida tecnologica. Analoga posizione è assunta dalla Gran Bretagna, ove un documento della Camera del Lords su questo tema è significativamente intitolato "no room for complacency".

E' evidente che pur in questo quadro di mancata, complessiva regolazione, ben diverse sono le tutele che offrono oggi, quantomeno nel campo degli usi civili, i sistemi democratici come USA, Gran Bretagna ed altri rispetto a Cina e Russia: non prevedendo tra l'altro quest'ultima neanche una distinzione tra disciplina civile e militare dell'IA.

Dai paesi prima ricordati si distingue l'Unione Europea che, nell'aprile del 2021, ha presentato una propria proposta ai paesi membri fondata su una IA umanocentrica, rispettosa di sicurezza, trasparenza, privacy, tutela dei dati, responsabilità sociale e ambientale, controllo umano dei sistemi militari. Con forti preoccupazioni, quindi, di carattere etico sugli usi e sulle prospettive dell'IA. All'indirizzo dell'Unione Europea si adeguerà naturalmente la risposta italiana in corso di definizione.

In conclusione, è necessario rinforzare il dialogo internazionale per giungere ad una disciplina comune sugli usi civili della IA, nel solco delle proposte europee. Per gli aspetti militari il confronto, specialmente oggi, è estremamente complicato e ricalca, forse in peggio, quello degli anni '50 sulle armi nucleari. Che ha tuttavia condotto, in un momento altrettanto difficile, ai trattati di non proliferazione che, almeno fina ad oggi, hanno impedito l'uso delle armi atomiche.