La digitalizzazione della guerra

Infrastrutture, armi autonome e sistemi predittivi basati sull'AI sono gli ambiti della sempre più stretta relazione tra uso civile e uso militare delle tecnologie digitali. Ma anche la narrazione della AI è uno strumento di guerra.

Giulio De Petra

Pubblicato l'08.02.2025: https://centroriformastato.it/la-digitalizzazione-della-guerra/

Intervento all'iniziativa "Guerra e tecnologie: il complesso digitale-militare", tenutasi il 20.01.2025, nel ciclo "Guerra, pace, sistema mondiale", promosso dall'Università di Roma "La Sapienza" insieme alla Fondazione Lelio e Lisli Basso, in collaborazione con la Campagna Sbilanciamoci!, Rete italiana Pace e Disarmo, Greenpeace Italia e con il patrocinio di RUniPace – Rete delle Università per la Pace.

L'utilizzo delle tecnologie digitali nei teatri di guerra non è recente, ma certamente ha avuto un fortissimo impulso negli ultimi anni. La guerra tra Russia e Ucraina e quella tra Israele e Palestina sono gli scenari dove con più evidenza è possibile osservare le caratteristiche della combinazione sempre più stretta tra tecnologie digitali e dispositivi militari (se ne è scritto recentemente su questo sito). Per comprenderne meglio le implicazioni è utile suddividere e analizzare questo connubio in tre ambiti tecnologici: quello delle infrastrutture; quello delle armi autonome; quello dei sistemi predittivi di supporto alle decisioni basati sull'AI.

Civile e militare

Prima di analizzarli è utile però rilevare una caratteristica che attraversa i tre ambiti e può fornire una chiave di lettura più generale: la stretta integrazione tra usi civili ed usi militari delle tecnologie digitali (lo ha

descritto efficacemente e con ricchezza di riferimenti Michele Mezza nel suo recente "Connessi a morte. Guerra, media e democrazia nella società della cybersecurity", Donzelli Editore, 2024). E abbiamo assistito nei due teatri di guerra non solo a una più stretta intersezione di civile e militare, ma anche a una inversione rispetto al tradizionale rapporto tra usi militari e usi civili.

È tradizionale considerare l'innovazione tecnologica, e quindi anche quella digitale, come un percorso che inizia nell'ambito militare, che non solo finanzia ma indirizza la ricerca e consente efficaci opportunità di sperimentazione sul campo. È solo successivamente che i prodotti, diretti e indiretti, della innovazione in ambito militare vengono utilizzati a fini commerciali in ambito civile, con modalità anche molto lontane dalle loro iniziali finalità. L'esempio più noto riguarda la stessa architettura di Internet, che è stata progettata in ambito militare (col nome di Arpanet) per garantire la permanenza della capacità della rete anche se alcuni dei nodi di connessione diventavano inutilizzabili.

Oggi invece assistiamo sempre più spesso al percorso inverso: dispositivi e pratiche dell'utilizzo civile della tecnologia digitale vengono utilizzati in azioni militari.

L'esempio più clamoroso è lo scoppio simultaneo, provocato dall'esercito israeliano, di migliaia di cercapersone in possesso degli affiliati ad Hezbollah in Libano. Dispositivi del tutto analoghi agli smartphone che ognuno di noi indossa a contatto del proprio corpo, protesi digitale resa indispensabile dalle conseguenze della trasformazione digitale, sono stati trasformati, anche grazie alla rete che li connette, in ordigni micidiali che hanno ucciso e mutilato i loro inconsapevoli portatori. Metafora simbolicamente potente della possibile nocività di questi dispositivi anche in ambito civile.

Un altro esempio riguarda la pratica più diffusa di utilizzo degli smartphone, usati come macchine fotografiche, che è la condivisione delle immagini che immette in rete in tempo reale la descrizione di persone o cose che popolano il mondo che ci circonda. È questo il modo in cui, nei teatri di guerra, chiunque, militare o civile che sia, condividendo immagini riprese con il proprio smartphone con presidi militari vicini o lontani, può indirizzare la

traiettoria di proiettili, missili o droni verso il luogo in cui si trovano i “nemici”.

Le infrastrutture digitali

Dell’importanza delle infrastrutture digitali in ambito militare si è parlato recentemente molto, a proposito della rete Starlink costruita e gestita dalla società SpaceX di Elon Musk, che è nata apparentemente per un uso in ambito civile. Ma la prevalente utilità distintiva di questa infrastruttura è in ambito militare e nella navigazione in alto mare. Quasi tutti gli altri usi possono essere infatti coperti anche con tecnologie diverse da quella dei satelliti di Starlink, con prestazioni spesso migliori e costi anche inferiori. Ma dove nessuna fibra, nessuna antenna, nessun ponte radio può arrivare, Starlink al momento non ha concorrenti e ha acquisito, grazie al basso costo della messa in orbita dei suoi satelliti, un vantaggio competitivo che potrà essere colmato solo tra molti anni. L’impiego nei teatri di guerra, dove gli altri sistemi di comunicazione sono facilmente messi fuori uso, e dove la comunicazione tra soldati e tra questi e i droni è indispensabile, è quindi l’impiego principale di Starlink. Che, essendo privata, viene concessa o a pagamento, o come merce di scambio per l’accrescimento del potere e degli interessi economici del suo proprietario. Questo spiega, ad esempio, perché la rete viene concessa inizialmente gratuitamente all’Ucraina, ma ne viene impedito l’uso per attaccare il territorio della Crimea, ne viene poi revocato l’uso gratuito, infine nuovamente concesso all’Ucraina questa volta dietro pagamento da parte degli USA. Infrastruttura comunque non impenetrabile, se l’esercito russo nei territori di confine è riuscito anch’esso a connettersi Starlink, “bucando” i sistemi di sicurezza.

Ma le infrastrutture digitali in ambito militare non sono soltanto quelle di comunicazione. Esistono anche le infrastrutture digitali che consentono la logistica degli eserciti e quelle civili che consentono il funzionamento stesso degli apparati statali. Sono, ad esempio, i data center e i computer delle forze armate e dell’amministrazione statale che devono essere messi al sicuro. E le grandi aziende digitali come Amazon e Google questo si propongono di fare, e lo fanno offrendo ospitalità nei propri data center in territorio americano (ne hanno parlato su questo sito Andrea Coveri e Dario Guarascio). Le infrastrutture digitali, al pari delle tradizionali infrastrutture di comunicazione (ferrovie, aeroporti, porti) sono infatti esse stesse oggetto

di attacchi militari, che possono essere anche attacchi informatici. È la cosiddetta “cyberguerra”, che si rivolge anche alle componenti digitali, oggi vitali, delle tradizionali infrastrutture materiali, riuscendo a mettere fuori uso dighe, trasporti, energia.

Essendo lo spazio orbitale dei satelliti di Starlink una risorsa non infinita e nel prossimo futuro oggetto di contesa, è prevedibile che la “cyberguerra” si trasferirà presto nello spazio, e riguarderà gli stessi satelliti e il loro funzionamento.

Le armi autonome

Le armi autonome (per una analisi accurata si veda “Etica delle macchine. Dilemmi morali per robotica e intelligenza artificiale” di Guglielmo Tamburrini, Carocci Editore, 2020) sono quelle capaci di selezionare e attaccare un obiettivo senza intervento umano. Una definizione così generale può comprendere anche dispositivi militari rudimentali, come ad esempio le mine antiuomo, che scoppiano solo quando il peso che le comprime supera una determinata soglia. Ma lo sviluppo effettivo di armi autonome avviene con l’utilizzo, in molte componenti, di sistemi di telecomunicazione e di AI. Parallelamente al loro sviluppo si è sviluppato il tentativo di definire vincoli al loro utilizzo basati sul Diritto Internazionale Umanitario (DIU) in tempo di guerra. Elemento centrale di questi tentativi è stato il ruolo del controllo umano nell’utilizzo dei nuovi sistemi. Più il controllo umano è effettivo ed esteso, meno gravi sono i rischi connessi all’uso di questo tipo di armi.

L’esempio più diffuso di armi autonome sono i velivoli di ogni tipo, genericamente chiamati droni. Se sono telecomandati vi è controllo umano, anche se la lontananza di chi governa il drone dal luogo dell’azione, e l’interfaccia usata per guidarlo, fa somigliare una azione di guerra a un videogioco (anche qui identità tra uso civile e militare), e diminuisce già solo per questo nell’operatore umano la percezione delle conseguenze letali e degli effetti collaterali dell’azione che sta svolgendo. Ma telecomandare il drone può diminuire la sua efficacia. Se chi telecomanda è molto lontano vi sono tempi di latenza del segnale che possono essere non tollerabili. Ma, soprattutto, anche se è più vicino, vi è il rischio che i canali di telecomunicazione possano essere disturbati o distrutti. Se a questo

aggiungiamo l'utilizzo di sistemi di AI sempre più potenti, vi sono le condizioni per lo sviluppo e l'utilizzo sempre più esteso di droni senza controllo umano nel corso dell'azione. Abbiamo le cosiddette "munizioni che vagano", alle quali viene assegnato un obiettivo, e che restano in volo finché l'obiettivo non viene avvistato e colpito. Abbiamo gli sciami di droni che si coordinano tra loro nel corso dell'azione, senza alcun controllo centrale. Abbiamo aeroplani a guida autonoma, di cui sono stati sperimentati combattimenti con altri velivoli sempre guida autonoma. Abbiamo natanti a guida autonoma, molto utilizzati dalla marina ucraina nel Mar Nero. E oltre a velivoli e natanti, anche veicoli a guida autonoma, che l'esercito ucraino ha recentemente massicciamente utilizzato nella battaglia di Lyptsi, villaggio di confine della regione di Kharkiv (ne parla il sito di "Guerre di Rete").

In tutti questi casi l'assenza di controllo umano implica la possibilità di errori di riconoscimento dell'obiettivo, e l'incapacità di valutare i danni collaterali dell'azione o le variazioni del contesto.

Si è detto che le macchine sono più affidabili degli umani nella possibilità di commettere errori. Ma questo, fa notare Guglielmo Tamburrini, riguarda solo la frequenza e non la gravità delle conseguenze dell'errore, che possono essere anche catastrofiche. Considerazioni ed esempi che, anche in questo caso, rimandano a quanto è stato analizzato e valutato nel caso civile delle auto a guida autonoma.

Sistemi predittivi di supporto alle decisioni

Lo sviluppo più recente, e più preoccupante, nel quale troviamo tutte insieme le principali criticità dell'uso dell'AI in ambito bellico, è quello dei sistemi di supporto alle decisioni, sistemi predittivi basati prevalentemente su sistemi di AI. Anche qui è evidente la stretta interrelazione con sistemi usati in ambito civile. L'esempio più calzante riguarda i sistemi di supporto alle decisioni in ambito finanziario, dove la quantità di dati utilizzati e la velocità del calcolo servono ad anticipare decisioni di acquisto o di vendita da parte dei competitori, che a loro volta fanno uso dello stesso tipo di sistemi. L'analogia con la decisione di colpire un bersaglio in una azione bellica è immediata, così come è immediata l'analogia sulle conseguenze

catastrofiche che ne possono derivare: la crisi finanziaria del 2008 in ambito civile, o lo scoppio di un conflitto nucleare in ambito militare.

È interessante approfondire la relazione in ambito militare tra il decisore umano e il sistema di raccomandazione che lo assiste: un insieme sociotecnico dove prevale inevitabilmente l'elemento tecnico. Il decisore umano in ambito militare, al quale il sistema di supporto dovrebbe offrire più solidi e affidabili elementi di valutazione, deve spesso prendere decisioni in tempi sempre più ristretti. Opera inoltre anche in questo caso un pregiudizio favorevole alla macchina: è più difficile prendere una decisione che non accoglie il suggerimento del sistema di supporto, al quale si attribuisce la capacità di considerare quantità di dati molto più ampie di quelle conosciute dal decisore. Prendere una decisione coerente col suggerimento del sistema è inoltre una giustificazione efficace nel caso che la decisione si riveli sbagliata. Questo pregiudizio opera, ad esempio, anche in ambito medico: si pensi all'utilizzo di sistemi di supporto alle decisioni nel momento della diagnosi.

C'è un caso, di cui si è molto parlato, relativo alla guerra tra Israele e Palestina, nella cui analisi confluiscono non solo molte delle considerazioni fin qui fatte, ma che nuove e drammatiche ne suggerisce.

Si tratta del sistema di AI "Lavender", rivelato da una inchiesta di Yuval Abrahm sulla rivista israeliana +972, sostanzialmente confermata dall'esercito israeliano.

Lavender ha lo scopo di suggerire "target", obiettivi da colpire sul territorio di Gaza. I bersagli da uccidere sono gli affiliati di Hamas a ognuno dei quali, sulla base di indizi della più diversa natura, viene assegnato un rango (capo, ufficiale, soldato semplice, fiancheggiatore), rango che, come vedremo, genera effetti significativi nelle procedure di "eliminazione" del bersaglio. Sempre sulla base di questi indizi vengono individuati i luoghi dove l'obiettivo può essere colpito. L'inchiesta segnala che un altro sistema di AI del tutto analogo, chiamato "The Gospel", ha invece lo scopo di individuare gli obiettivi non umani (depositi di munizioni, rampe di lancio di missili, centri di comando, centrali elettriche, reti di distribuzione idriche, ingressi dei tunnel, etc.).

Vediamo più analiticamente il funzionamento di Lavender così come descritto dall'inchiesta di +972 e le implicazioni che ne derivano (dalla

relazione di Daniele Amoroso dell'Università di Cagliari alla conferenza annuale di Nexa del 13/12/2024).

1. Addestramento del sistema, cioè raccolta e classificazione di dati per l'alimentazione del sistema. In questa fase sono stati definiti come indizi per essere considerati appartenenti all'ala militare di Hamas caratteristiche non univoche (ad es. il cambiare frequentemente indirizzo). Oppure sono stati indicati tra gli obiettivi possibili anche tipologie protette dal DIU, ad esempio, gli operatori della protezione civile. Oppure si considera come dato indicativo della presenza di civili il numero di connessioni telefoniche attive, dimenticando che in quel contesto manca l'energia elettrica per ricaricare i cellulari.
2. Individuazione e validazione del target. Cioè, a partire dai dati raccolti (di ogni tipo, e accumulati nel corso degli anni, in cui Gaza è stato il luogo più sorvegliato al mondo), individuazione di possibili obiettivi. Decisione di colpire tutti i militanti di Hamas (37.000). Accettazione di un errore quantificabile nel 10%. Equiparazione del suggerimento di Lavender a un "ordine superiore", in quanto tale da contraddire da parte dell'operatore umano solo in presenza di una grave presunzione di errore. Tempi di validazione ridotti per garantire il numero di attacchi previsti.
3. Pianificazione degli attacchi. La scelta fatta è di colpire quando i presunti militanti di Hamas sono in casa, per semplificare le procedure operative. Fissazione di soglie di civili sacrificabili, donne e bambini inclusi, in relazione al rango dell'obiettivo. Da poche decine fino a centinaia. Uso di munizioni non "intelligenti" (e quindi con più grandi margini di errore) per eliminare militanti di basso rango. Costano meno e ci sono scorte abbondanti.
4. Esecuzione dell'attacco. Mancata verifica della presenza in casa dell'obiettivo da colpire dopo il tempo passato dall'avviso dell'attacco.

La narrazione della AI

C'è un uso dell'intelligenza artificiale in un contesto di guerra ulteriore e diverso da quelli finora indicati, che si aggiunge agli altri, ma anche li contraddice. L'inchiesta sul funzionamento di Lavender ha mostrato che descrivere l'uso della AI in guerra come operazione chirurgica per colpire il nemico riducendo al minimo i danni collaterali è falsa. I danni collaterali

vengono quantificati in decine, o addirittura centinaia di vittime civili, in relazione al rango dell'obiettivo.

Ma c'è un'altra, ulteriore considerazione da fare.

Nel caso della guerra di Gaza noi abbiamo la possibilità (e la sventura) di assistere a un caso reale. E osservandolo è difficile non considerare che quello che è successo a Gaza è nei fatti indipendente dall'uso di Lavender o di Gospel. Quando vengono sganciate bombe potentissime sopra un piccolo territorio densamente abitato, che può essere paragonato a un formicaio (e tale sembra quando si osservano i movimenti dei puntini neri che rappresentano gli abitanti di Gaza, ripresi dai sistemi di videosorveglianza utilizzati dai droni) è evidente che si tratta di un massacro indiscriminato.

Rispetto a questo massacro è il "racconto" dell'intelligenza artificiale che viene usato come giustificazione di un metodo molto tradizionale di fare la guerra, analogo a quello che abbiamo conosciuto nella seconda guerra mondiale con il culmine di Hiroshima e Nagasaki.

È quindi la narrazione dell'intelligenza artificiale a essere usata come strumento di guerra. Che contribuisce a svelare la retorica positiva della narrazione della AI anche quando viene utilizzata in ambito civile.