La Weaponization dell'Intelligenza Artificiale

La diffusione di sistemi di intelligenza artificiale sempre più economici ed efficaci sta avendo, e avrà in grado sempre maggiore, effetti distruttivi su numerosi ambiti della vita umana. L'**ambito militare** è sicuramente uno di questi. L'intelligenza artificiale sta progressivamente diventando il centro focale della competizione internazionale per la *leadership* tecnologica, e non stupisce che tale competizione si manifesti anche nello sviluppo e accumulazione di armi autonome – così dette *Autonomous Weapons System*.

La peculiarità di queste armi risiede nella loro potenziale capacità di comprendere le caratteristiche dell'ambiente circostante e definire in modo autonomo le strategie più efficaci per raggiungere un dato obbiettivo. Sistemi di intelligenza artificiale stanno venendo attualmente integrati in tecnologie militari quali sistemi di difesa missilistica, veicoli aerei senza equipaggio (**UAVs**) o sottomarini senza equipaggio (**UUVs**). Il drone Harpy utilizzato dall'esercito israeliano è, ad esempio, a giudicare dalla sue caratteristiche tecniche, un'arma completamente autonoma[1].
Oltre che all'integrazione dell'intelligenza artificiale in sistemi e piattaforme nei quattro domini – terra, aria, mare e spazio – la *weaponization* (letteralmente, "trasformazione in arma") dell'intelligenza artificiale si riferisce anche al suo utilizzo indipendente per compromettere o distruggere i network nemici attraverso attacchi nello spazio cibernetico – il quinto dominio.
Questa rivoluzione in campo militare avrà plausibilmente effetti dirompenti sugli equilibri di potere internazionali, e comporterà notevoli cambiamenti dottrinali circa il modo di condurre una guerra.

Da un lato, l'applicazione di queste tecnologie in operazioni

militari permette, dal punto di vista tattico, una migliore e più facile analisi in tempo reale del campo di battaglia e una migliore consapevolezza delle condizioni esterne da parte del battaglione. Fornisce poi alle truppe sul campo strumenti intelligenti che possano migliorare il loro processo decisionale. Migliora inoltre la precisione delle operazioni militari e dei loro effetti, potenzialmente riducendo il numero di vittime collaterali o civili. Fornisce aiuti logistici alle truppe, riducendo e ottimizzando i costi legati alle operazioni e permette, infine, di portare a termine i compiti militari più faticosi, noiosi, pericolosi o moralmente complessi[2].

D'alto lato, il processo di *weaponization* comporta però **numerosi rischi**. In primo luogo, la proliferazione di queste tecnologie e la prospettiva di una corsa agli armamenti aumenta inevitabilmente l'instabilità del sistema internazionale, specialmente se si considera che l'adozione queste tecnologie favorisce un considerevole rafforzamento militare di nuovi attori quali attori non-statali o "Stati paria". Il rischio legato a tali tecnologie è inoltre amplificato dalla ridotta capacità di controllare e limitare le conseguenze indesiderate quando queste vengono utilizzate.[3] Estremamente problematico è inoltre l'aspetto legato all'attribuzione di responsabilità. La possibilità di negare plausibilmente la responsabilità per un attacco (*plausible deniablity*), caratteristica anche di più convenzionali attacchi cyber, è definita come l'abilità di un attore A di lanciare un attacco contro un attore B in modo che la sua responsabilità sia difficilmente comprovabile[4]. Questo implica che un attore in possesso di armi autonome può ritenere di poter lanciare un attacco con relativa impunità, fattore che contribuisce anch'esso all'aumento dell'instabilità del sistema internazionale. A tal riguardo, il 14 settembre 2019 un drone ha attaccato alla raffineria Saudi Aramco, in Arabia Saudita, causando una perdita del 5% della produzione petrolifera globale: quasi un anno dopo,

rimane ancora poco chiaro chi sia stato il mandante di questo attacco[5].

In aggiunta a tali problematicità, occorre poi menzionare rischi più specificatamente legati all'intelligenza artificiale. Primo fra tutti, quale che sia l'ambito di applicazione, è stato largamente evidenziato come i sistemi di **intelligenza artificiale** presentino importanti problemi di estrinsecazione di **pregiudizi** nel loro processo decisionale. Se tali pregiudizi vengono incorporati in sistemi utilizzati nel campo militare, o a fronte di una intenzionale manipolazione dei dati da parte del nemico o di problemi dell'algoritmo o del dataset utilizzato, questi sistemi falliranno nel produrre gli effetti desiderati con disproporzionali effetti negativi a danno dei soggetti del pregiudizio.

Un altro rischio specifico di questi sistemi è quello connesso alla facilità con cui questi possano essere attaccati. A tal proposito Comiter afferma che la manipolazione dell'intelligenza artificiale è legata a delle *"limitazioni fondamentali sottostanti questi sistemi"*[6]. In altre parole, esistono dei fattori matematici che caratterizzano sia l'algoritmo che i *dataset* utilizzati tali per cui i sistemi di intelligenza artificiale risulteranno inevitabilmente vulnerabili. In questo senso, tali vulnerabilità sono sostanzialmente diverse da quelle che vengono sfruttate in un attacco cyber classico, poiché non sono causate da un errore umano nella scrittura del codice ma sono connaturate all'intelligenza artificiale stessa.

Lasciare che scelte di vita o morte vengano potenzialmente assunte, in modo arbitrario, da armi autonome pone infine un fondamentale **quesito etico** circa la deresponsabilizzazione dell'essere umano nel compiere queste scelte. A livello di società, è necessario che ci si interroghi se questa è la direzione verso cui desideriamo andare.

La tensione esistente tra potenzialità e problematicità legate alla *weaponization* dell'intelligenza artificiale ha portato le Nazioni Unite ad instituire, già nel 2013, un gruppo di esperti per deliberare circa la possibilità di bandire internazionalmente i sistemi di armi autonome. Ad oggi le negoziazioni non sembrano tuttavia avallare tale proposta. Esemplificativa in tal senso è la posizione degli Stati Uniti i quali, nel 2018, dichiaravano la necessità di sviluppare *"una comprensione internazionalmente condivisa circa i rischi e benefici di questa tecnologia prima di decidere una specifica risposta di policy"* dichiarandosi convinti che fosse prematuro intraprendere negoziazioni su qualunque strumento legale o politico[7].

In generale, sembra che gli Stati stiano comprendendo il potenziale di queste armi, la loro potenza ed efficacia, e che siano pertanto restii a limitarne lo sviluppo; bisognerebbe nondimeno chiedersi a quale costo societario si stia intraprendendo tale strada.

Note

[1] Harpy NG. (n.d.). Retrieved from http://www.iai.co.il/2013/36694-16153-en/Business_Areas_Land.aspx

[2] Joe Burton and Simona R. Soare, *Understanding the Strategic Implications of the Weaponization of Artificial Intelligence*, 2019 11th International Conference on Cyber Conflict: Silent Battle, NATO CCD COE Publications, 2019.

[3] *Ibid.*

[4] Adam P. Liff, 2019, *Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War*, Journal of Strategic Studies, Vol. 35, No.3, p. 412

[5]

https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html?login=email&auth=login-email

[6] Marcus Comiter, *Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It* , Belfer Center for Science and International Affairs, Harvard Kennedy School, 2019

[7] https://futureoflife.org/2019/05/09/state-of-ai/?cn-reloaded=1

Articolo a cura di **Carolina Polito**

https://www.ictsecuritymagazine.com/articoli/la-weaponization-dellintelligenza-artificiale/