L’uso dell’intelligenza artificiale nelle applicazioni di sicurezza fisica

di Angelo Carpani - libero professionista, laureato in Ingegneria elettronica presso il Politecnico di Milano, iscritto all’Ordine degli Ingegneri della Provincia di Como (n.2368 sez.A), esperto nella progettazione di impianti di videosorveglianza in ambito comunale.

Questo articolo prende spunto da una conversazione che ho avuto con **Pierre Racz**, Presidente e CEO di **Genetec Inc**., in occasione del Global Press Summit che si è tenuto presso l’Experience Center Genetec di Washington DC all’inizio del mese di febbraio di quest’anno in rappresentanza di essecome-securindex con cui collaboro da tempo, a proposito dell’intelligenza artificiale applicata nel mondo della videosorveglianza e, più in generale, nella sicurezza fisica.

L’aumento dell’uso dell’intelligenza artificiale sta accedendo molti entusiasmi per le possibilità della tecnologia, ma questo può essere pericoloso nelle applicazioni di sicurezza fisica. Questo articolo ha lo scopo di sfatare alcuni “miti” legati all’intelligenza artificiale (di seguito IA) e di invitare ad adottare un approccio responsabile al suo utilizzo.

I computer dotati di IA hanno una coscienza?

Una macchina, seppur dotata di IA, esegue funzioni preimpostate, ma non comprende quel che “elabora”, in altre parole non è autocosciente!

Federico Faggin, padre del microprocessore, insieme al fisico **Giacomo Mauro D’Arian**o nel libro *“IRRIDUCIBILE – La coscienza, la vita, i computer e la nostra natura”* (Mondadori), nel tentativo di descrivere i meccanismi fisici che regolano la coscienza, non essendo essa clonabile e non riproducibile come, ad esempio, si può fare con la memoria di un computer, ritiene che sia un fenomeno che ricade sotto le leggi della fisica quantistica. Il cervello umano non è clonabile: per quanto si possa conoscere una persona, non si saprà mai cosa stia pensando!

Mentre l’informazione classica si può copiare, quella quantistica non è copiabile nè riproducibile. Mentre i bit classici possono essere copiati tutte le volte che vogliamo, questa operazione è fisicamente impossibile per i bit quantistici (“qubit”) in base ad un teorema che i fisici chiamano di “non-clonazione”.

Il fatto che i meccanismi fisici che regolano la coscienza ricadano sotto le leggi della fisica quantistica, non deve indurre a pensare che un domani un computer quantistico possa comprendere quel che “elabora”. Nemmeno un computer quantistico potrà avere la versatilità del nostro cervello. I computer quantistici aumentano certamente a dismisura la potenza e la velocità di calcolo rispetto ai computer tradizionali ma questo non significa che facciano cose mirabolanti che un computer classico non possa fare in tempi diversi. Se, ad esempio, si chiedesse ad un computer quantistico di simulare la molecola molto complessa di un nuovo farmaco, esso potrebbe farlo in pochi minuti mentre un computer classico, anche il più potente, richiederebbe migliaia di anni.

L’intelligenza artificiale non è “creativa”!

L’uomo “crea” dal nulla, il computer esegue. Non a caso si parla di intelligenza artificiale “generativa” che è una cosa ben diversa. L’intelligenza artificiale effettua le proprie elaborazioni sulla base di algoritmi e dati inseriti dall’uomo, facendo correlazioni statistiche e “generando” risultati, più o meno sofisticati, estraibili soltanto dai dati memorizzati dentro la macchina dagli esseri umani. Quindi i risultati

prodotti non sono frutto di "creatività". Non c'è nulla nella fisica classica, che è una scienza deterministica, che indichi la presenza di coscienza e di libero arbitrio in essa.

Cos'è l'intelligenza artificiale in un contesto di sicurezza fisica?

Ciò che esiste in realtà è una tecnologia sviluppata per imparare ad utilizzare set di dati per consentire di eseguire compiti che normalmente richiedono l'intelligenza umana. Come ho accennato in un precedente articolo, gli algoritmi di *Machine Learning (ML)* e di *Deep Learning (DL)* sono i sottosistemi dell'intelligenza artificiale che utilizzano i dati appresi come, ad esempio, avviene nelle telecamere per rilevare e classificare accuratamente gli oggetti: l'apprendimento automatico utilizza tecniche statistiche per ottenere il riconoscimento di oggetti, veicoli ed esseri umani o altro.

Le macchine sono eccezionalmente brave nelle attività ripetitive e nell'analisi di grandi set di dati (come i video) ed è qui che l'intelligenza artificiale nel suo stato attuale può portare i maggiori vantaggi. L'intelligenza artificiale può essere usata per aiutare i team di sicurezza a fare ciò che già fanno, solo più velocemente e con maggiore precisione, su enormi set di dati: come ad es. "guardare" centinaia di ore video per trovare un'auto rossa in modo che un operatore della sicurezza possa concentrarsi su altri compiti. Si risparmiano così agli operatori innumerevoli ore trascorse alla ricerca di individui specifici all'interno di lunghe riprese video, consentendo loro di reindirizzare i propri sforzi verso altre loro responsabilità e ad altre aree dell'organizzazione di cui fanno parte.

Anche i sistemi di intelligenza artificiale commettono errori

Anche i sistemi di intelligenza artificiale commettono errori e questo è pericoloso in un contesto di sicurezza fisica. *Jen-Hsun Huang*, CEO di *Nvidia*, nella conferenza annuale per gli sviluppatori di Nvidia, ha parlato degli errori che spesso commettono le IA generative: le cosiddette *"allucinazioni"*, cioè la tendenza per alcune intelligenze artificiali a inventare risposte che sembrano plausibili ma che non sono basate su fatti. I sistemi AI vengono addestrati sulla base di dati/modelli storici e la loro accuratezza dipende in larga misura dalla quantità, dalla qualità e dalla diversità dei dati di addestramento. Distorsioni e limitazioni nei dati di addestramento possono portare a risultati distorti o errati. Inoltre l'intelligenza artificiale, proprio perché non è creativa, non è in grado di prevedere tutti gli incidenti di sicurezza, in quanto basa i propri comportamenti sulla base di dati/modelli storici noti e potrebbero avere difficoltà a rilevare minacce nuove o in evoluzione. A questo proposito mi viene in mente quanto accaduto nel gennaio 2009 a New York in cui un aereo di linea ammarò sul fiume Hudson a causa di un multiplo *bird strike* (impatto con volatili) che mise fuori uso i motori dell'aereo. Quanto accaduto fu oggetto della sceneggiatura di un noto film *Sully* in cui il pilota, che salvò la vita a 155 persone, di fronte ad una commissione di indagine che metteva in discussione quanto accaduto ritenendo improbabile il multiplo bird strike ritenendolo un evento senza precedenti, il pilota rispose: *"Tutto è senza precedenti finché non capita per la prima volta"!*

La policy di Genetec: adottare un approccio responsabile all'IA

Sebbene l'intelligenza artificiale possa essere utilizzata per migliorare le misure di sicurezza fisica, la tecnologia stessa non è quindi immune dai rischi per la sicurezza. La tecnologia IA può automatizzare attività ripetitive e banali consentendo al personale addetto alla sicurezza di concentrarsi su attività più complesse e strategiche. Tuttavia, il giudizio umano, le intuizioni e le capacità decisionali sono ancora cruciali nella maggior parte degli scenari di sicurezza. L'intelligenza artificiale può contribuire ad aumentare le capacità umane e migliorare l'efficienza, ma richiede sempre la supervisione e l'interpretazione dei risultati da parte dell'uomo.

Genetec assicura che i propri modelli di intelligenza artificiale non vengano utilizzati per prendere decisioni critiche e la *policy* è quella di garantire che un essere umano sia sempre coinvolto e che i dati siano presentati in modo tale che l'essere umano possa prendere una decisione informata.