



Santarelli: «L'AI non sostituirà le spie. Intelligence europea? Il problema è chi cede i propri segreti».

Descrizione

(Adnkronos) «L'intelligenza artificiale sta democratizzando capacità che fino a pochi anni fa appartenevano a cerchie ristrette di analisti. In pochi secondi è possibile incrociare fonti aperte, ricostruire profili, mettere in relazione persone, aziende e avvenimenti. Ma chiamare tutto questo «intelligence» rischia di generare un equivoco. Perché raccogliere e aggregare informazioni non significa fare spionaggio.

È uno dei punti su cui insiste Marco Santarelli, analista investigativo delle reti informative e consulente sui temi della sicurezza internazionale, del terrorismo e dell'intelligence. Nei suoi lavori più recenti ha sostenuto che, quanto cresce il peso dell'AI, tanto torna centrale la Humint: la raccolta di informazioni attraverso reti e relazioni umane, soprattutto quando l'obiettivo non è conoscere ciò che è pubblico ma penetrare ciò che qualcuno vuole tenere segreto.

Partiamo dall'AI. Lei sostiene che ci sia un salto rispetto alla prima stagione dei social network.

«Con Facebook abbiamo assistito a una gigantesca raccolta di dati: gusti, preferenze, comportamenti. Oggi quei database esistono già. Con l'intelligenza artificiale il passaggio, a mio avviso, è dalla quantità alla qualità. Non si tratta soltanto di sapere cosa facciamo, ma di aggregare quelle informazioni, metterle in relazione e costruire modelli sempre più sofisticati. È qui che gli agenti e i sistemi automatizzati cambiano la scala del problema. Il processo diventa molto più rapido e molto meno visibile all'utente».

È in questo quadro che lei legge anche il caso Anthropic e le dimissioni del ricercatore Jacob Coxon?

«Quel caso mi ha colpito soprattutto dal punto di vista comunicativo. Abbiamo un ricercatore che lascia l'azienda mettendo in guardia sui rischi dei sistemi più avanzati e, quasi immediatamente, il vertice della stessa azienda riconosce che il problema esiste. Normalmente davanti a una rottura interna di questo tipo ci aspetteremmo una dinamica diversa. Non dico che questo dimostri una

pianificazione, ma trovo interessante il modo in cui la vicenda ha contribuito ad accendere ancora di più l'attenzione sui pericoli dell'AI. In una fase come questa bisogna osservare non soltanto la tecnologia, ma anche la narrazione costruita intorno alla tecnologia•.

Un giornalista oggi può chiedere a un modello AI di ricostruire in pochi secondi un profilo per il quale prima sarebbero servite ore o giorni. Non viene meno uno dei tradizionali vantaggi informativi dell'intelligence?

Viene meno una parte di quel vantaggio. La capacità di aggregazione dell'AI rende accessibile a moltissime persone qualcosa che prima richiedeva software specifici, competenze e molto tempo. Ma bisogna stare attenti a non confondere questa capacità con lo spionaggio. Una cosa è l'Osint, una cosa la business intelligence o una due diligence, un'altra ancora sono spionaggio e controspionaggio•.

Posso chiedere a un sistema di ricostruire il profilo di una persona o le connessioni di un'azienda. Posso ottenere moltissimo da fonti aperte. Ma l'AI non mi dice se una determinata persona è stata infiltrata in un'organizzazione per rubare un brevetto. Per arrivare a quell'informazione servono ancora fonti, informatori, presenza fisica sul territorio, reti costruite nel tempo•.

È una distinzione sulla quale Santarelli insiste anche nei suoi scritti. L'AI si sta affiancando alla Humint nelle attività di raccolta e controspionaggio, non sostituendo la componente umana.

Quindi più cresce l'AI, più diventa importante il fattore umano? Sembra un paradosso.

Per me è esattamente così. Più cresce la tecnologia, più l'intelligence deve conservare una rete informativa umana. L'AI può essere un formidabile strumento di controllo, verifica e aggregazione, ma esiste un livello dell'informazione che nasce soltanto dalla presenza sul campo. Pensiamo a un porto strategico, a un cavo sottomarino, a un ambiente industriale sensibile. Bisogna capire chi si muove, con chi parla, perché. Questo non coincide con l'analisi automatizzata di informazioni già disponibili•.

C'è poi un problema ulteriore: l'abbondanza di informazioni sintetiche rende più difficile distinguere ciò che è autentico da ciò che è manipolato. Un'immagine può essere modificata, una ricostruzione può essere orientata. L'intelligence non può limitarsi ad assorbire ciò che trova in rete: deve anche chiedersi da dove arriva quell'informazione e chi può avere interesse a farla circolare•.

Arriviamo all'ipotesi di una intelligence europea. È realisticamente possibile avere un servizio di Bruxelles?

Politicamente è una bella idea. Operativamente è molto più difficile. Già all'interno dei singoli sistemi nazionali il passaggio delle informazioni segue procedure, livelli di classificazione e catene di responsabilità molto precise. Immaginiamo di moltiplicare questo problema per ventisette. Il punto non è creare un ufficio a Bruxelles: è capire quali informazioni i servizi nazionali sarebbero davvero

disposti a trasferirgli?•.

•?Lâ?intelligence vive anche di segreti che uno Stato considera propri. Non penso che, almeno in tempi brevi, i grandi servizi europei siano pronti a cedere con facilitÃ reti, fonti, capacitÃ operative o informazioni particolarmente sensibili. La collaborazione giÃ esiste ed Ã molto forte in diversi settori. Ma una cosa Ã collaborare, unâ?altra Ã centralizzare?•.

Quindi piÃ¹ che una â?CIA europea?• immagina una rete piÃ¹ stretta tra i servizi nazionali?

•?Quella mi sembra una prospettiva piÃ¹ concreta, almeno nel breve periodo. Esistono ambiti nei quali si puÃ² condividere di piÃ¹: il finanziamento del terrorismo, i movimenti finanziari transfrontalieri, le criptovalute, determinate minacce cyber. E ci sono obiettivi sui quali gli interessi europei convergono chiaramente. Ma lâ?idea che ogni Paese metta semplicemente in comune tutto ciÃ² che sa Ã unâ?altra cosa?•.

Il modello Five Eyes, osserva, dimostra proprio quanto sia difficile separare la condivisione dellâ?intelligence dalla fiducia politica costruita nel tempo. Santarelli ha sottolineato recentemente come gruppi piÃ¹ ristretti di servizi europei stiano giÃ cooperando su obiettivi particolarmente difficili, a partire da Russia e Cina: piÃ¹ plausibile, dunque, procedere per cerchi di fiducia e missioni comuni che decretare dallâ?alto la nascita di un unico servizio. *Giornale Diplomatico*

Sul cyber, invece, la rincorsa tecnologica sta favorendo chi attacca o chi difende?

•?Sta cambiando innanzitutto lâ?economia del settore. Lâ?immagine romantica dellâ?hacker solo in una stanza che con pochi mezzi riesce a mettere in difficoltÃ una grande organizzazione non descrive piÃ¹ tutto il sistema. La potenza computazionale costa, la sicurezza avanzata costa, e questo concentra capacitÃ molto sofisticate nelle mani di chi dispone delle risorse per sostenerle?•.

•?Per questo dobbiamo porci un problema di sovranitÃ tecnologica. Se apparati pubblici, forze di polizia o strutture sensibili utilizzano tecnologie che non controlliamo fino in fondo, dobbiamo sapere da dove provengono, chi le produce, quali dipendenze creano. In questo senso credo vada rafforzata la logica del Golden Power: non guardare soltanto alla proprietÃ di unâ?azienda, ma alle tecnologie davvero strategiche per il Paese e alla loro filiera?•.

La stessa preoccupazione riguarda i segreti industriali: lâ?uso non controllato di piattaforme AI puÃ² esporre codici, know-how e informazioni riservate, trasformando una questione aziendale in un problema di sicurezza nazionale quando sono coinvolti settori come difesa, energia o telecomunicazioni.

Lei arriva a proporre un controllo molto piÃ¹ forte anche sui brevetti. Non rischia di diventare unâ?impostazione eccessivamente dirigista?

•?Non parlo di controllare la ricerca scientifica o di bloccare lâ?innovazione. Il problema Ã conoscere e proteggere ciÃ² che ha un valore strategico. Oggi la tecnologia arriva con estrema rapiditÃ sia a chi la utilizza legittimamente sia a chi vuole usarla per scopi criminali. Dobbiamo

preoccuparci non soltanto di quanto costa un prodotto, ma di dove atterra, di chi può utilizzarlo e con quali conseguenze?.

Alla fine, per, nessuna tecnologia può promettere sicurezza assoluta.

Assolutamente. Tutto ciò che è collegato a una rete presenta una superficie di attacco. E oggi il cyber non colpisce soltanto il sistema informatico, colpisce la persona. Se ricevo una telefonata con la voce perfettamente riprodotta di mio figlio che mi dice di avere bisogno immediatamente di denaro, il problema non è soltanto tecnico: è emotivo?.

Per questo la sicurezza deve diventare cultura diffusa. Le persone devono imparare a controllare l'origine di un file, un indirizzo, i metadati di un documento, a riconoscere le anomalie. Sono nozioni che dovrebbero cominciare a essere insegnate già dalle elementari. Non trasformeremo tutti in esperti di cyber, ma possiamo rendere molto più difficile sfruttare la vulnerabilità più semplice: quella umana?.

In un suo recente articolo ha scritto: «Al metodo metodologica, la spia culturale?». A questa, in fondo, la sintesi?

Sì. L'intelligenza artificiale può elaborare una quantità enorme di informazioni e trovare collegamenti con una velocità che un essere umano non potrà mai avere. Ma l'intelligence non è soltanto elaborazione. È comprensione del contesto, capacità di leggere le persone, di costruire una relazione, di capire ciò che non viene detto. A volte, mentre tutto accelera, il compito dell'analista è esattamente il contrario: rallentare, separare il rumore dall'informazione e dare al decisore qualcosa che abbia davvero un significato?.

?

cronaca

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione

Ottobre 13, 2026

Autore

redazione