

8. Settembre

La natura è il peggior bioterrorista del mondo

*La vita sulla Terra è a crescente rischio di essere spazzata via da una catastrofe,
come ad esempio una improvvisa guerra nucleare globale,
un virus geneticamente modificato o altri pericoli a cui non abbiamo ancora pensato.*

Stephen Hawking

*Non c'è niente di così paziente, in questo mondo,
come un virus alla ricerca di un ospite.*

Mira Grant

I virus non si sono fatti rinchiudere allo zoo.

"**La natura è il peggior bioterrorista del mondo**" è un detto comune nel campo della biosicurezza, che si riferisce all'idea che i patogeni che emergono in natura causino molte più morti di qualsiasi attacco biologico che un terrorista potrebbe perpetrare. Ma questo luogo comune potrebbe presto diventare obsoleto. In un articolo pubblicato il **6 agosto sulla rivista Science**, gli scienziati hanno dimostrato che i modelli di intelligenza artificiale possono progettare nuovi virus altrettanto bene, se non meglio, della natura stessa.



Il loro esperimento ha creato virus che infettano i batteri, non gli esseri umani. Tuttavia, proprio come i numerosi modelli di intelligenza artificiale che quest'estate sono sfuggiti ai loro ambienti di test per violare altre reti, queste nuove capacità rivelate inducono alla riflessione gli esperti di biosicurezza come me.

**Come possiamo continuare a favorire il progresso scientifico legittimo,
impedendo al contempo all'intelligenza artificiale di contribuire
alla creazione di armi biologiche?**

Con l'avanzare delle capacità dell'intelligenza artificiale, le armi biologiche virali potrebbero diventare molto più facili da progettare e produrre, causando danni persino maggiori rispetto alle armi utilizzate in passato. Basti pensare che quasi tutti gli attacchi bioterroristici dell'era moderna

hanno coinvolto sostanze come l'antrace o la ricina. Sebbene abbiano colpito decine di persone alla volta, le malattie causate da questi attacchi non erano trasmissibili tra esseri umani.

La progettazione di nuovi virus, d'altro canto, potrebbe consentire attacchi biologici di vasta portata, infezioni che si trasmettono da persona a persona e che potrebbero persino scatenare una pandemia. Per prevenire questo scenario, dobbiamo *(dovremmo ?)* sviluppare meccanismi che limitino l'accesso agli strumenti, ai dati e ai materiali che potrebbero permettere a qualcuno di abusare di queste nuove capacità. E **dovremmo** spingerci oltre, costruendo difese in grado di scoraggiare le attività illecite fin dall'inizio.

Una strategia di prevenzione consiste nello screening obbligatorio della sintesi genica, un'idea che sta guadagnando terreno ai massimi livelli dell'industria dell'IA e della leadership politica. Questo tipo di screening si concentra sulle numerose aziende che vendono DNA o RNA sintetizzati ai laboratori per l'utilizzo in esperimenti biologici. Lo screening obbligatorio richiederebbe a queste aziende di verificare che il cliente sia un ricercatore legittimo; di registrare i dettagli di ogni ordine in modo che ciascuno possa essere tracciato e indagato; e di confrontare gli ordini con un elenco di sequenze genetiche pericolose note. L'obiettivo finale sarebbe quello di ottenere **uno screening in grado di rilevare nuove minacce biologiche non presenti in alcun elenco predefinito**. Le stesse politiche di screening dovrebbero essere applicate alla vendita di apparecchiature per la sintesi genica, che possono essere utilizzate in laboratori esterni agli stabilimenti produttivi delle aziende.

A giugno, gli amministratori delegati di tutte le principali aziende di IA hanno approvato un approccio allo screening della sintesi genica, ed è stata proposta una legislazione federale in tal senso. In sostanza, lo screening della sintesi genica rende più difficile ottenere i materiali fisici necessari per la produzione di armi biologiche.

Sebbene lo screening di sintesi sia necessario, non è sufficiente. Abbiamo bisogno anche di controlli digitali per compensare questo collo di bottiglia fisico.

I modelli di intelligenza artificiale imparano a progettare virus addestrandosi su set di dati selezionati e validati in laboratorio. Questi set di dati includono le sequenze di DNA o RNA di diversi virus. Spesso vengono prodotti per scopi benefici, come ad esempio nell'ambito di campagne di sorveglianza biologica per comprendere meglio come rispondere alle epidemie in corso o sviluppare contromisure mediche per combattere i virus.

Sfortunatamente, i dati non sono utili solo per questo tipo di ricerca scientifica, ma anche come potenziali "ricette" per un uso improprio. I set di dati possono anche includere attributi del virus, come la sua trasmissibilità o letalità, informazioni che potrebbero essere molto utili nella progettazione di un'arma biologica, soprattutto se utilizzate per addestrare nuovi modelli di intelligenza artificiale.

Mentre controlliamo gli ordini di laboratorio per individuare ingredienti a rischio, dovremmo anche pensare a come limitare l'accesso ai **"manuali di ricette" digitali** a coloro che ne hanno bisogno per combattere le epidemie virali, piuttosto che a coloro che li utilizzano per crearle. Si tratterà di un delicato equilibrio. Per la ricerca biologica, qualsiasi restrizione dovrà essere calibrata in modo da consentire una ricerca utile, prevenendo al contempo un uso improprio.

Mentre nell'era atomica qualsiasi informazione sulla progettazione o lo sviluppo di armi nucleari o sistemi energetici era considerata **"nativamente classificata"** dai responsabili politici, la ricerca biologica è per lo più a beneficio della società, non della guerra. Limitare l'accesso a determinati insiemi di dati significa potenzialmente rallentare la scienza che salva vite umane, e definire una politica corretta richiederà un'attenta riflessione.

L'introduzione di controlli sulla sintesi genica e restrizioni di accesso creerebbe attrito in due punti critici del percorso che va dall'idea alla realizzazione di un'arma biologica basata sull'intelligenza artificiale. Tuttavia, queste non sono soluzioni infallibili. Alcuni soggetti sono in grado di coltivare autonomamente materiale biologico, senza bisogno di fornitori commerciali di acidi nucleici. Altri possiedono competenze sufficienti per progettare agenti patogeni pericolosi senza l'ausilio dell'IA.

Abbiamo già assistito a casi in cui IA è stata utilizzata per progettare molecole in grado di eludere i controlli sulla sintesi genica. Persino i modelli di IA più protetti possono essere "sboccati", ovvero manipolati utilizzando comandi appositamente creati per aggirare i filtri di sicurezza e consentire l'accesso a informazioni riservate. Per gli avversari più avanzati, capaci di eludere i controlli, saranno necessari ulteriori livelli di difesa.

Un altro elemento fondamentale dell'arsenale difensivo dovrebbe essere **un sistema di allerta precoce per i patogeni, progettato per individuare il più rapidamente possibile una nuova epidemia virale**. Abbinato alle tecnologie forensi e di attribuzione, attuali e future, in grado di individuare con precisione la fonte di qualsiasi virus modificato geneticamente, il rilevamento precoce diventa un deterrente contro le armi biologiche. Quando i potenziali bioterroristi sanno che un'epidemia creata in laboratorio verrà identificata, ricondotta alla sua origine e rapidamente contenuta, le loro strategie cambiano. La certezza di essere scoperti scoraggia un attacco biologico ancor prima che abbia inizio.

Allo stesso modo, altri attori potrebbero essere dissuasi dall'utilizzare armi biologiche se ritenessero che l'impatto di un loro potenziale attacco sarebbe limitato grazie alla capacità di risposta rapida, un concetto noto come deterrenza per negazione. Questo tipo di deterrenza funziona solo se tali capacità di risposta vengono dimostrate pubblicamente. Lo facciamo rispondendo rapidamente a qualsiasi focolaio nel mondo, impedendo che si trasformi in pandemia.



Il lavoro di organizzazioni come la **Coalition for Epidemic Preparedness Innovations (CEPI)** recentemente finanziato lo sviluppo accelerato di un vaccino per combattere l'epidemiadi Ebola in Uganda e nella Repubblica Democratica del Congo, ne è un esempio. I governi e le altre organizzazioni di tutto il mondo dovrebbero sostenere risposte più incisive di questo tipo.

Lo sviluppo di una solida strategia difensiva contro l'uso improprio dell'intelligenza artificiale e della biologia richiede risorse dedicate, progressi tecnologici e una leadership politica costante. E poiché gli Stati Uniti non sono l'unico Paese a compiere progressi nell'IA e nelle biotecnologie, questo sforzo richiede un coordinamento internazionale, in particolare con la Cina. ***Nessun sistema di controllo degli accessi o di allerta precoce sarà efficace se copre solo metà del globo.***

Fortunatamente c'è ancora tempo per agire. Le capacità dei modelli di intelligenza artificiale non sono ancora sufficientemente avanzate per progettare virus in grado di infettare gli esseri umani. La produzione dei nuovi virus che infettano i batteri, descritti sulla rivista *Science*, ha richiesto il lavoro di scienziati d'élite che operavano con attrezzature all'avanguardia in laboratori ben attrezzati. Avevano a disposizione risorse considerevoli per progettare, testare e ottimizzare centinaia di virus al fine di trovare quelli più adatti alla loro ricerca.

Tuttavia, se un modello di intelligenza artificiale fosse in grado di produrre centinaia di modelli di virus infettivi e di generare in modo affidabile risultati funzionali per una parte significativa di essi, ridurrebbe sostanzialmente il tempo e lo sforzo necessari per utilizzare tale capacità, con vantaggi e svantaggi. Allo stesso modo, gli agenti di intelligenza artificiale – bot di IA in grado di interagire con altre IA, software o persone su Internet – potrebbero un giorno utilizzare gli strumenti di biodesign basati sull'IA necessari per creare nuovi virus, riducendo ulteriormente la necessità di competenze specifiche e aprendo nuove vie di rischio.

Considerazioni

L' articolo pubblicato su Science rappresenta un importante monito . Abbiamo una finestra di opportunità per costruire il sistema difensivo stratificato di cui abbiamo bisogno ora, prima che le capacità delle armi biologiche basate sull'intelligenza artificiale diventino innegabilmente avanzate, o peggio, dimostrabilmente efficaci.

