

21 OTTOBRE 2026

# Commenti

Nuova Serie

## LA SUPERINTELLIGENZA ARTIFICIALE SEGNA LA FINE DELLA MATEMATICA E AMPLIFICA IL DIVARIO DELLA DIFESA CYBER SU SCALA GLOBALE

Enrico Prati\*

L'ottobre del 2026 passerà probabilmente alla storia come il momento in cui la pratica della matematica è stata archiviata nella sua qualità di attività umana, a favore del definitivo passaggio di testimone all'intelligenza artificiale generativa. Con un susseguirsi di innovazioni senza precedenti che nasce dall'invenzione dei transformers nel 2017 da Google Brain, l'anno 2026 ha segnato un'ulteriore accelerazione che ha reso obsoleto quanto accaduto via via nei mesi precedenti a un ritmo sconosciuto e difficilmente assimilabile dalla comunità della scienza e della tecnologia.

Nel giro di pochi mesi infatti OpenAI, sbaragliando la concorrenza costituita da Anthropic, Google, Meta e DeepSeek, ha dapprima confutato in maggio una storica congettura del grande matematico Paul Erdos formulata nel 1946, poi in agosto ha pubblicato dieci soluzioni di altrettante congetture di grande importanza in matematica e in settembre ha prodotto la dimostrazione di una soluzione di uno dei problemi del millennio inerente l'equazione di Navier-Stokes che si usa per descrivere il movimento dei liquidi e dei gas.

Mentre la comunità dei matematici reagiva, a partire da una lettera di venticinque premiati con la Medaglia Fields – il Nobel della matematica assegnato ogni quattro anni – con espressioni di dissenso per la modalità di ottenimento di questi risultati e del loro rilascio al grande pubblico senza passare attraverso un processo di revisione tra pari, OpenAI pubblicava appunto all'inizio di ottobre più di trecento dimostrazioni di altrettante congetture della matematica. Alcune di queste resistevano da periodi dell'ordine di 50-90 anni. La metà delle dimostrazioni sono corredate di certificato Lean4 che assicura ragionevolmente la correttezza della dimostrazione prodotta.

### **La minaccia cyber tra multi-dominio e multilivello**

Questo vero e proprio tsunami di risultati mai visto nella storia della scienza richiederà *secoli-uomo* di studio da parte di matematici esperti per assicurarne la comprensione umana e la verifica, ma di fatto modifica profondamente il modo di lavorare non solo nella matematica, ma anche nell'informatica, nella fisica, nella progettazione e nella sicurezza, senza considerare l'adattamento che questi strumenti impongono nell'insegnamento rivolto alle nuove generazioni.

Dal momento che il mondo della sicurezza è basato su codici che sfruttano teoremi matematici e la complessità algoritmica, l'impatto sulla cybersecurity è dirompente. Se da un lato avremo la consueta scienza aperta prodotta nelle università dalla comunità di matematici, dall'altro avremo nuovi modelli matematici sviluppati dalle aziende che detengono questi strumenti.



COMMENTO  
N.059 NS/2026



\*Università degli  
Studi di Milano

Le opinioni espresse  
non impegnano  
necessariamente la  
Fondazione CSF

Queste aziende, basate principalmente in USA e in Cina, non condividono i modelli più potenti della loro intelligenza artificiale generativa, e non sono tenute a condividere gli eventuali risultati nel campo della matematica e quindi della cybersecurity che si dovessero rivelare strategici.

Le Agenzie governative, a loro volta, saranno gli acquirenti di questi risultati oppure in alternativa svilupperanno modelli matematici per la crittografia e la crittanalisi basati su teoremi che resteranno sconosciuti alle potenze rivali, e codici di attacco informatico generati dall'intelligenza artificiale.

### ***Datacenter: il nesso tra l'autonomia energetica e l'autonomia di difesa cyber***

C'è un legame stretto tra l'impiego di queste tecnologie, la potenza di calcolo e il costo in termini di energia, che limita l'impiego dei modelli più profondi a un numero ristretto di attori. Per fare un esempio, l'equazione di Navier-Stokes – collegato anche a una controversia con Anthropic sulla paternità dei risultati che hanno abilitato OpenAI a concludere la dimostrazione – ha richiesto l'utilizzo di diecimila agenti che hanno cooperato tra di loro, per un costo in bolletta elettrica di quindici milioni di dollari.

Saranno quindi le grandi aziende e i Governi che potranno dotarsi di strumenti di offesa e difesa basati su questo tipo di intelligenza artificiale, nella misura in cui possono allocare sistematicamente risorse energetiche dedicate all'alimentazione di immensi datacenter. L'asimmetria nella disponibilità di risorse energetiche, anche conseguente a diversi gradi di autonomia nell'approvvigionamento e nella produzione, si tradurrà nella diversa disponibilità di strumenti di difesa e protezione da aggressioni esterne.

Questi datacenter – isolati dal resto della rete – annoverano già centinaia di migliaia di GPU (Anthropic ad esempio usa un *cluster* da quattrocentocinquanta mila GPU prodotte da Nvidia che costerebbero al pubblico circa sessanta mila dollari ciascuna). Nel caso di dati confidenziali come quelli di carattere governativo e industriale ad alto livello di sicurezza, dovranno eseguire modelli parzialmente pre-addestrati e poi affinati obbligatoriamente su dati proprietari in modo da preservarne la confidenzialità, alimentati da centrali elettriche che risulteranno obiettivi critici da difendere per il mantenimento della capacità di calcolo.

I codici da soli quindi non sono sufficienti, senza la disponibilità di un'industria microelettronica, di datacenters, di fonti di energia e di centrali. Le alleanze geopolitiche dovranno tenere conto di questi fattori per assicurare l'accesso alle fonti di energia e alla microelettronica, al fine di assicurare un sistema adeguato di protezione dalle minacce cyber globali collegate alla violazione di codici e di attacchi basati su prove difficili da risolvere matematicamente.

LA SUPERINTELLIGENZA  
ARTIFICIALE SEGNA LA  
FINE DELLA MATEMATICA E  
AMPLIFICA IL DIVARIO  
DELLA DIFESA CYBER  
SU SCALA GLOBALE

Le opinioni espresse  
non impegnano  
necessariamente la  
Fondazione CSF



Fondazione CSF