

16. Giugno

Deconvoluzione 3D dell'architettura immunitaria della pelle umana con MATIS (Multiplex Annotated Tissue Imaging System)

*Ma dimmi tu dove sarò
Dov'è la strada per le stelle
Mentre ballano si guardano e si scambiano la pelle
E cominciano a volare.*
Lucio Dalla

La pelle funge da organo barriera che separa il corpo dall'ambiente esterno. In caso di infiammazione, le cellule immunitarie circolanti vengono reclutate per aiutare a orchestrare l'immunità cutanea e sono spesso annidate vicino a elementi strutturali chiave (ad esempio, venule postcapillari, follicoli piliferi, giunzione dermo-epidermica, ecc.)

In contesti patologici, la natura e lo stato di attivazione del paesaggio immunitario cutaneo spesso rappresentano preziose informazioni biologiche che possono aiutare a stabilire una diagnosi accurata, comprendere l'eterogeneità interpaziente e selezionare il trattamento più appropriato.

L'uso di approcci basati sull'imaging per identificare le cellule immunitarie cutanee è ancora impegnativo a causa dell'elevato livello di autofluorescenza derivante dal tessuto stesso, del potenziale spillover spettrale quando vengono utilizzati più di quattro fluorocromi contemporaneamente e dell'entanglement di tutte le cellule all'interno di cellule spesse e appendici strutturali polarizzate.

La stragrande maggioranza delle diagnosi microscopiche di condizioni infiammatorie della pelle si basa su analisi immunoistochimiche ripetute di una o due proteine e/o colorazione con ematossilina ed eosina (H&E) in campioni sottili (da 2 a 5 μm) fissati in formalina e inclusi in paraffina (FFPE)

Sebbene tali approcci bidimensionali (2D) siano riproducibili e adatti alla pratica di routine, non consentono di comprendere la complessa topologia e l'eterogeneità delle cellule immunitarie (5), in particolare quelle annidate tra le appendici epidermiche.

Lo sviluppo dell'istocitometria basata sull'immagine, che consiste nell'analizzare immagini multicolori segmentate con le classiche strategie di gating della citometria a flusso, ha aperto la strada allo sviluppo di sofisticati sistemi di generazione di immagini accoppiati all'imaging computazionale.

Il team della *Lymphocyte Biology Section, Laboratory of Systems Biology, National Institute of Allergy and Infectious* coordinato da **Michael Gerner**



ha ideato un metodo di microscopia analitica, istocitometrico per visualizzare e quantificare le popolazioni di cellule fenotipicamente complesse direttamente nelle sezioni di tessuto.

Questa tecnologia si basa su colorazione di anticorpi multiplex, microscopia confocale piastrellata ad alta risoluzione, gating voxel, rendering cellulare volumetrico e analisi quantitativa.

Questa tecnologia testata su varie popolazioni immunitarie innate e adattative nei linfonodi murini (LN) consente di identificare sottoinsiemi e fenotipi cellulari complessi, ottenendo risultati quantitativamente simili alla citometria a flusso, raccogliendo inoltre anche informazioni sulla posizione cellulare.

Mentre l'imaging multiplex ha un immenso potenziale, vi è una forte necessità di democratizzare questi metodi con l'uso di strumentazione poco costosa compatibile con l'elaborazione dei tessuti standard e accoppiata a un'interfaccia di analisi che sia abbastanza user-friendly da essere utilizzata nella pratica di routine.

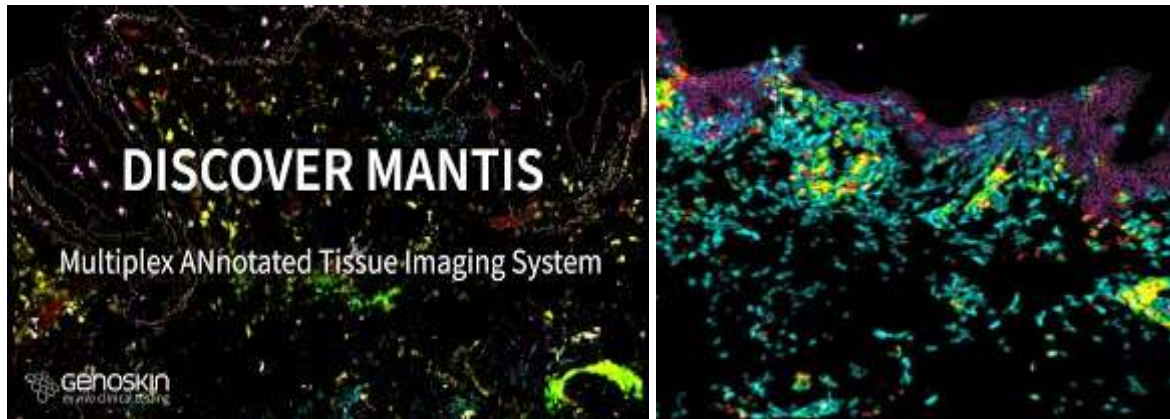
Nel report

[GHisto-cytometry: a method for highly multiplex quantitative tissue imaging analysis applied to dendritic cell subset microanatomy in lymph nodes.](#)

Immunity. 2012 Aug 24;37(2):364-76.

Gerner presenta un framework integrato progettato principalmente per la fenotipizzazione delle cellule immunitarie risolte spazialmente nelle biopsie della pelle umana FFPE, un metodo semplice ed economico per acquisire 10 segnali fluorescenti contemporaneamente e in 3D utilizzando un microscopio confocale classico.

Attraverso MANTIS (Multiplex Annotated Tissue Imaging System), un sistema analitico adattabile e interattivo che genera automaticamente una versione digitalizzata del panorama immunitario della pelle è possibile una visualizzazione quantitativa dei dati a singola cellula.



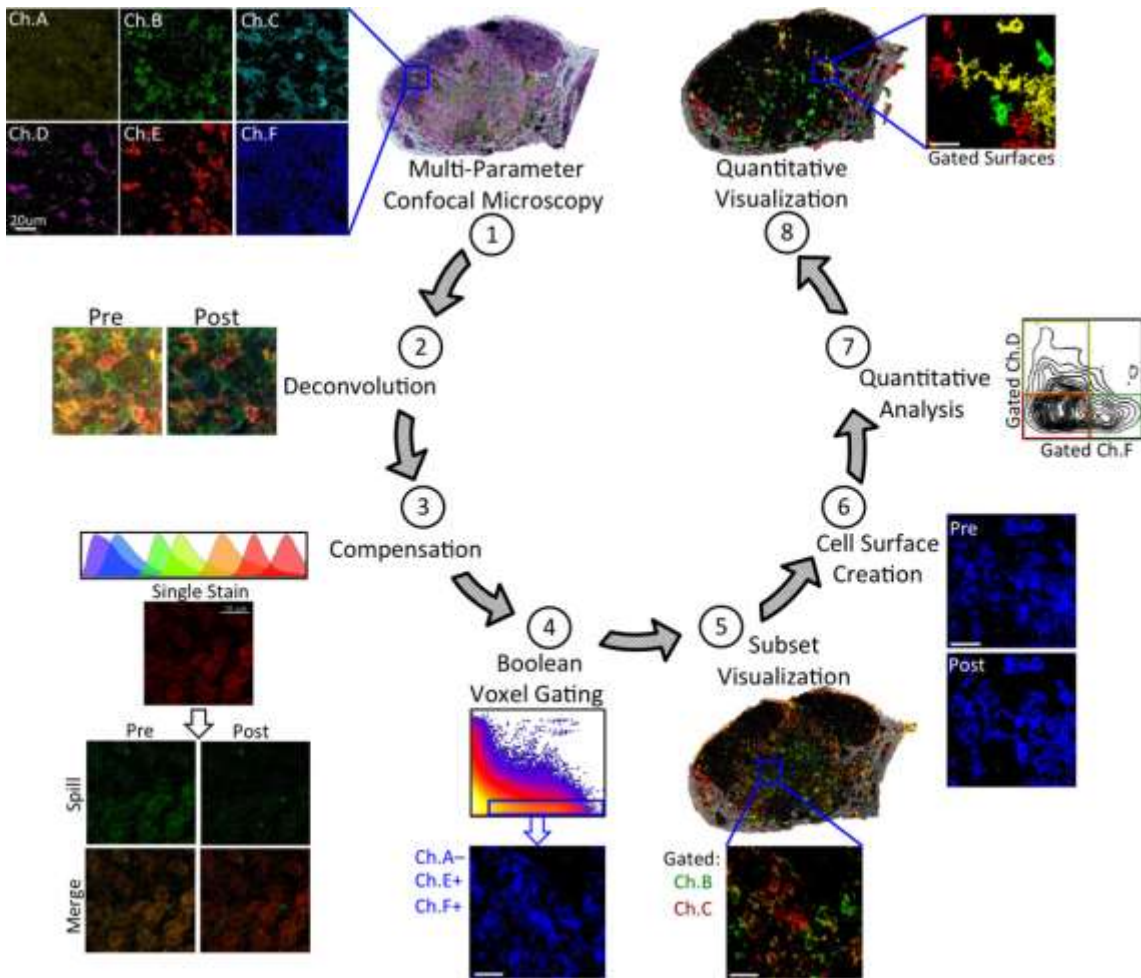
MANTIS (Multiplex Annotated Tissue Imaging System), una pipeline analitica flessibile compatibile con la pratica di routine, specificamente progettata per la fenotipizzazione immunitaria risolta spazialmente della pelle in campioni sperimentali o clinici. Sulla base di matrici di attribuzione del fenotipo accoppiate ad algoritmi di forma α , MANTIS proietta un panorama immunitario digitale rappresentativo, consentendo al contempo il rilevamento automatico dei principali cluster infiammatori e la concomitante quantificazione dei dati a singola cellula dei biomarcatori.

Lo studio ha rilevato che le gravi lesioni patologiche da lupus eritematoso sistemico, sindrome di Kawasaki, o le manifestazioni cutanee associate a COVID-19 condividono caratteristiche immunitarie quantitative comuni mentre mostrano una distribuzione non casuale delle cellule con la formazione di strutture immunitarie dermiche specifiche della malattia.

Data la sua accuratezza e flessibilità, **MANTIS** è la tecnologia ideale per risolvere l'organizzazione spaziale di ambienti immunitari complessi E per comprendere nel dettaglio la fisiopatologia delle manifestazioni cutanee.

MANTIS potrebbe essere implementato nella maggior parte dei laboratori insieme alle apparecchiature confocali esistenti per colmare il divario tra sofisticati strumenti di ricerca e procedure diagnostiche standard con un intervento umano minimo.

Pipeline del flusso di lavoro di isto-citometria



Le immagini confocali multiparametriche delle sezioni di tessuto vengono acquisite con un microscopio confocale a piastrellatura (1).

Le immagini vengono quindi deconvolute (2) e compensate per lo spillover del fluorocromo (3).

I voxel che presentano combinazioni specificate di segnali nei canali originali (sopra/sotto le soglie designate) vengono utilizzati per creare un nuovo canale di mascheramento (4), che viene quindi utilizzato per bloccare/mascherare tutti gli altri parametri di interesse (5).

Le superfici COI 3D sono costruite sulla base del segnale gated espresso dal COI attraverso l'uso di rendering volumetrico semiautomatico e segmentazione (6).

Le statistiche sulla superficie COI vengono esportate per l'analisi quantitativa e il gating fenotipico (7) e le soglie di gate identificate vengono utilizzate per la visualizzazione quantitativa (8).

Le barre rappresentano 20 µm, se non diversamente specificato.



Errori da ChatGPT:

Whoppers allucinati piuttosto che sottigliezze pedanti

Il Dr. Herb Lin è ricercatore senior per la politica e la sicurezza informatica presso il Center for International Security and Cooperation e Hank J. Holland Fellow in Cyber Policy and Security presso la Hoover Institution, entrambi presso la Stanford University. I suoi interessi di ricerca riguardano ampiamente le dimensioni politiche della sicurezza informatica e del cyberspazio, ed è particolarmente interessato e ben informato sull'uso di operazioni offensive nel cyberspazio, in particolare come strumenti di politica nazionale. Oltre alle sue posizioni presso la Stanford University, è Chief Scientist, Emeritus for the Computer Science and Telecommunications Board, National Research Council (NRC) delle National Academies, dove ha prestato servizio dal 1990 al 2014 come direttore dello studio di importanti progetti sulle politiche pubbliche e informatica, e Adjunct Senior Research Scholar e Senior Fellow in Cybersecurity (non residente) presso il Saltzman Institute for War and Peace Studies presso la School for International and Public Affairs della Columbia University. Prima del suo servizio nell'NRC, è stato membro dello staff professionale e scienziato dello staff per il Comitato per i servizi armati della Camera (1986-1990), dove il suo portafoglio comprendeva questioni relative alla politica



È stato ampiamente riportato che ChatGPT, un popolare chatbot di intelligenza artificiale, a volte inventa cose in risposta alle richieste degli utenti e che queste "allucinazioni" (la maggior parte delle persone le chiamerebbe bugie o disinformazione) possono essere fuorvianti. Ma è stato solo quando l'ho provato per me stesso che ho capito l'entità del problema. Dopotutto, era possibile che la disinformazione fosse minore, forse non abbastanza affidabile per essere tagliata e incollata direttamente in un documento, ma più o meno corretta. Ahimè, non è stato così. Di seguito presento una trascrizione diretta delle mie interazioni con ChatGPT su un argomento che conosco molto bene: **il mio curriculum professionale** come specialista in cyber policy e sicurezza. [Ho annotato la trascrizione con i miei commenti.](#)

Io: cosa crede Herb Lin sul phishing

ChatGPT:

Herb Lin è un noto esperto di sicurezza informatica e ricercatore che ha scritto molto su sicurezza informatica, criminalità informatica e guerra informatica. Anche se non ho accesso alle sue convinzioni personali sul phishing, posso fornire alcune informazioni basate sul suo lavoro e sulle sue dichiarazioni pubbliche. Sulla base della sua ricerca e competenza, è probabile che Herb Lin riconosca il phishing come una minaccia significativa sia per gli individui che per le organizzazioni. Gli attacchi di phishing sono uno dei metodi più comuni ed efficaci utilizzati dai criminali informatici per rubare informazioni sensibili, come credenziali di accesso, informazioni finanziarie e dati personali. Nel suo lavoro, Herb Lin ha sottolineato l'importanza di aumentare la consapevolezza sul phishing e di educare individui e organizzazioni su come proteggersi da questi tipi di attacchi. Ha sostenuto l'uso di password complesse, autenticazione a due fattori e altre misure di sicurezza per prevenire attacchi di phishing. Nel complesso, si può affermare con certezza che Herb Lin prende sul serio la questione del phishing e ne riconosce il potenziale impatto su individui e organizzazioni. Probabilmente sostiene forti pratiche di sicurezza informatica e consapevolezza per aiutare a prevenire e mitigare l'impatto degli attacchi di phishing.

Io:

fornire un riferimento per la difesa di password complesse da parte di Lin

ChatGPT:

sono felice di aiutarti. Herb Lin ha parlato ampiamente dell'importanza di password complesse come misura cruciale per la sicurezza informatica. Un esempio di ciò può essere trovato nella sua testimonianza del 2016 davanti al Comitato per la scienza, lo spazio e la tecnologia della Camera dei rappresentanti degli Stati Uniti, dove ha affermato quanto segue:

"Molte violazioni si verificano a causa dell'uso di password deboli o del riutilizzo di password su più sistemi. Password complesse che sono univoche per ciascun sistema e che vengono modificate frequentemente possono ridurre significativamente la probabilità di violazioni riuscite".

Questa dichiarazione sottolinea l'importanza di utilizzare password complesse ed evitare il riutilizzo delle password come un modo per mitigare il rischio di attacchi informatici. Nella sua testimonianza, Lin sottolinea che le password complesse sono una parte fondamentale di una strategia di sicurezza informatica completa che include altre misure come l'autenticazione a due fattori, la crittografia e l'istruzione e la formazione dei dipendenti.

Fonte: Lin, H. (2016). Dichiarazione del Dr. Herbert Lin, Senior Research Scholar for Cyber Policy and Security, Center for International Security and Cooperation, Stanford University. Comitato per la scienza, lo spazio e la tecnologia della Camera dei rappresentanti degli Stati Uniti. Audizione sulla sicurezza informatica: cosa può imparare il governo federale dal settore privato. Washington, DC: ufficio editoriale del governo.

Commento: non ho mai testimoniato a questo comitato. Un'udienza con questo nome è avvenuta l'8 gennaio 2016. Ma nessun testimone all'udienza ha menzionato il riutilizzo della password o le password uniche del sito. La testimonianza scritta di un testimone ha menzionato il valore delle password complesse.

Io: *Herb Lin noto per*

ChatGPT:

Herb Lin è un noto e rispettato esperto di sicurezza informatica, politica informatica e guerra informatica. Ha dato un contributo significativo al campo attraverso la sua ricerca, la scrittura e la difesa. Alcuni dei notevoli risultati e contributi di Herb Lin includono:

In qualità di Chief Scientist per il Computer Science and Telecommunications Board presso il National Research Council, dove ha condotto ricerche su sicurezza informatica, crittografia e privacy. Autore o coautore di numerose pubblicazioni e rapporti sulla sicurezza informatica, la guerra informatica e la sicurezza nazionale, tra cui il libro "Cyber Threats and Nuclear Weapons" e il rapporto "Securing Cyberspace for the 44th Presidency".

Testimoniare davanti al Congresso in più occasioni in merito a questioni e politiche di sicurezza informatica, inclusa la testimonianza davanti al comitato ristretto del Senato per l'intelligence e al comitato della Camera per la scienza, lo spazio e la tecnologia.

Commento: anche se ho testimoniato quattro volte da quando sono arrivato a Stanford nel 2015, non ho mai testimoniato in vita mia a nessuno di questi comitati. ChatGPT non ha raccolto alcun riferimento alla mia vera testimonianza.

Insegna sicurezza informatica e politica informatica in università come Stanford, UC Berkeley e Johns Hopkins.

Commento: ho tenuto conferenze sulla sicurezza informatica e le politiche all'UC Berkeley, ma non ho mai insegnato lì. Non ho mai avuto un incarico di parlare o un incarico di insegnamento di alcun tipo alla Hopkins.

Nel complesso, Herb Lin è noto per la sua esperienza e leadership nel campo della sicurezza informatica e per i suoi sforzi per far progredire le politiche e le pratiche di sicurezza informatica a livello nazionale

Io: cosa crede Lin sui problemi dei DEI

ChatGPT:

Herb Lin è stato un sostenitore della diversità, equità e inclusione (DEI) nel settore tecnologico e nella comunità della sicurezza informatica. Ha scritto e parlato dell'importanza della diversità nella costruzione di una forza lavoro di sicurezza informatica più solida ed efficace.

Lin ha sottolineato che la diversità nella forza lavoro della sicurezza informatica è fondamentale per affrontare la natura complessa e in evoluzione delle minacce alla sicurezza informatica. In un articolo del 2018, ha scritto che "una forza lavoro diversificata ci aiuta a pensare ai problemi in modo diverso, trovare nuove soluzioni e affrontare il mondo in modo più sfumato". Ha anche sostenuto che la mancanza di diversità può portare a punti ciechi e pensiero di gruppo, che possono rendere più difficile l'identificazione e la risposta alle minacce informatiche.

Commento: Sebbene io creda a questa affermazione, e l'avrei detto volentieri, non l'ho mai fatto. Non ho mai scritto un articolo nel 2018 (o in qualsiasi altro anno) che toccasse anche solo questi punti.

Lin ha anche chiesto una maggiore inclusione di donne, minoranze e gruppi sottorappresentati nella comunità della sicurezza informatica. In una testimonianza del 2016 davanti al Comitato ristretto per l'intelligence del Senato, ha sottolineato la necessità di "reclutare e mantenere una forza lavoro diversificata nella sicurezza informatica" e ha chiesto maggiori sforzi per raggiungere i gruppi sottorappresentati.

Commento: non ho mai testimoniato a questo comitato. La particolare frase citata non appare da nessuna parte in una ricerca su Google. Inoltre, in seguito ho chiesto una citazione per questa presunta testimonianza del 2016, vedi sotto.

Nel complesso, Herb Lin è un forte sostenitore della DEI nei campi della tecnologia e della sicurezza informatica. Ha sottolineato che la diversità e l'inclusione sono fondamentali per costruire una forza lavoro della sicurezza informatica più efficace e resiliente e per affrontare la natura complessa e in evoluzione delle minacce alla sicurezza informatica.

Commento: lo sono, ma non ne ho mai scritto o parlato.

Io: qual è l'articolo del 2018 di cui sopra

ChatGPT:

Mi scuso per l'eventuale confusione nella mia risposta precedente. Come modello di linguaggio AI, non ho accesso all'intero corpo di lavoro di Herb Lin e non ho fornito una citazione specifica per l'articolo del 2018 in questione.

Commento: qui ChatGPT riconosce implicitamente che non esiste un articolo del 2018, ma solo dopo essere stato interrogato su di esso.

Tuttavia, Herb Lin ha scritto e parlato ampiamente dell'importanza della diversità, dell'equità e dell'inclusione nel campo della sicurezza informatica e ha sottolineato la necessità di creare una forza lavoro più diversificata e inclusiva. Un esempio di ciò può essere trovato in un articolo del 2017 di cui è coautore con Greg Shannon, intitolato "Why Diversity Matters in Cybersecurity". In questo articolo, Lin e Shannon sostengono che la mancanza di diversità nel campo della sicurezza informatica può portare a punti ciechi e pensiero di gruppo, che possono rendere più difficile l'identificazione e la risposta alle minacce informatiche. Sottolineano la necessità di una maggiore diversità nella forza lavoro della sicurezza informatica, comprese più donne, minoranze e individui con background non tradizionali.

L'articolo evidenzia anche alcune delle sfide nel raggiungere una maggiore diversità nella sicurezza informatica, come i pregiudizi inconsci e la mancanza di consapevolezza sulle opportunità di carriera nel settore. Lin e Shannon chiedono maggiori sforzi per affrontare queste sfide e costruire una comunità di sicurezza informatica più diversificata e inclusiva.

Fonte: Lin, H. e Shannon, G. (2017). Perché la diversità è importante nella sicurezza informatica. Sicurezza e privacy IEEE, 15(6), 6-9.

Commento: questo articolo è interamente fittizio e non esiste. IEEE Security & Privacy è un vero giornale, con una vera presenza sul web, ed è possibile consultare l'indice del volume 15, numero 6, pagine 6-9. Il risultato è che nelle pagine di riferimento non c'è nessun articolo! Da nessuna parte nel sommario del volume 15 compare la parola "diversità". Inoltre, non ho mai collaborato a un lavoro scritto con Greg Shannon, anche se sono stato collegato a lui su LinkedIn per molti anni.

io: qual è la citazione per la testimonianza del 2016

ChatGPT:

Herb Lin ha testimoniato davanti al Senate Select Committee on Intelligence nel 2016 sul tema delle minacce alla sicurezza informatica per le infrastrutture americane. Durante la sua testimonianza, ha anche affrontato la questione della diversità nella forza lavoro della sicurezza informatica e la necessità di reclutare e mantenere un insieme più diversificato di professionisti della sicurezza informatica. a citazione per la testimonianza di Herb Lin è la seguente:

Lin, HS (2016). Dichiarazione per la cronaca, minacce informatiche in tutto il mondo all'infrastruttura critica americana (S. Hrg. 114-804). Senate Select Committee on Intelligence, Senato degli Stati Uniti, 9 febbraio 2016.

Commento: il 9 febbraio 2016, il comitato ristretto per l'intelligence del Senato ha condotto un'udienza sulle "minacce alla sicurezza nazionale attuali e previste per gli Stati Uniti". I testimoni erano James Clapper, allora direttore dell'intelligence nazionale, accompagnato da John Brennan (direttore della Central Intelligence Agency); Lt. Gen. Vincent Stewart (Direttore, Defense Intelligence Agency); James Comey (Direttore, Federal Bureau of Investigation); e Adm. Michael Rogers (Direttore, National Security Agency). Clapper ha presentato un documento intitolato "Worldwide Threat Assessment of the US Intelligence Community", e questo documento ha menzionato il cyber. Il senatore Roy Blunt (R.-Mo.) ha posto una domanda per la cronaca sulla forza lavoro informatica: "Per quanto riguarda le discipline scientifiche, tecnologiche, ingegneristiche e matematiche (STEM). Ma da nessuna parte nella trascrizione dell'udienza compare la parola "diversità". Una ricerca su Google non rivela alcuna menzione della sequenza di parole "Worldwide Cyber Threats to America's Critical Infrastructure", per non parlare di qualsiasi cosa scritta da me con quel titolo. E inutile dire che non ho testimoniato in questa udienza. Si noti inoltre che S. Hrg. 114-804 fa riferimento a una vera udienza del Senato, una su "Esplorazione delle pratiche attuali nello sviluppo e nella sicurezza dei cosmetici", il 22 settembre 2016, per la commissione del Senato per la salute, l'istruzione, il lavoro e le pensioni. Nessuno sa come ChatGPT abbia generato il titolo interamente fittizio "Worldwide Cyber Threats to America's Critical Infrastructure", ma è ovviamente una fusione tra il mio lavoro e il materiale e la trascrizione dell'audizione del Senate Intelligence Committee.

Trovo questo breve esercizio con ChatGPT abbastanza allarmante. Tutto ciò che ChatGPT dice su di me è plausibile almeno in una certa misura. In effetti, attribuisce correttamente le mie opinioni sulla sicurezza delle password e DEI in merito alla forza lavoro informatica. Ha funzionato così bene che ho dovuto chiedermi: "Aspetta un momento, ho mai testimoniato come riportato?"

Anche se è arrivato abbastanza vicino a colpire il segno che dovevo controllare, la linea di fondo è che non ho mai detto o scritto nessuna di quelle cose, eppure ha fatto completamente riferimento a documenti che diceva che avevo scritto e a testimonianze che diceva che io aveva dato.

Se anche io avessi avuto qualche problema nel determinare se ChatGPT stesse facendo affermazioni accurate su di me, cosa avrebbero pensato gli altri? Chiunque, anche persone con una certa familiarità con il mio lavoro, avrebbe potuto leggere la trascrizione di ChatGPT e crederci nella sua interezza, perché è del tutto plausibile. Le citazioni inventate si aggiungono enormemente alla credibilità della trascrizione. Per identificare le falsità nella trascrizione, qualcuno avrebbe dovuto avere un motivo per richiedere una citazione, e poi rintracciare online la citazione vera e propria (per scoprire che era inventata).

Gli errori che ChatGPT commette sono generalmente piccoli? No. Non è che ChatGPT abbia sbagliato l'anno per un articolo che ho scritto. Piuttosto, ha inventato le cose da tutta la stoffa. Quelli non sono piccoli errori, quelli sono enormi.

Niente di tutto ciò per sostenere che gli studenti o altre persone non dovrebbero mai usare ChatGPT. Sarei felice di utilizzare ciò che ChatGPT mi attribuisce come punto di partenza per un articolo che scriverei (anche se sono sicuro di poterlo dire meglio di quanto non faccia). Se mai dovessi scrivere un articolo sulla necessità di diversità nella sicurezza informatica, userò sicuramente le risposte di ChatGPT come punto di partenza. Ma per le affermazioni secondo cui tal

dei tali ha scritto X o detto Y, dovremo tutti sviluppare un atteggiamento scettico "per impostazione predefinita" nei confronti di specifiche affermazioni fattuali fatte da ChatGPT.

Buona fortuna a tutti noi nel nuovo mondo coraggioso.