Cybersecurity Trends

Edizione italiana, N. 1 / 2024

INTERVISTE VIP:

- NUNZIA CIARDI
- YURI RASSEGA
- FRANCESCO MARCHESANI

ISSN 2559 - 1797
ISSN-L 2559 - 1797

Folder centrale: Cybersecurity e Quantum Computing

Cybersecurity Trends

Leggi la rivista **online** quando
e dove vuoi!
Puoi scegliere tra news, articoli,
interviste, nuove sezioni,
approfondimenti,
rubriche e contenuti multimediali.

Scopri anche la nuova sezione
dedicata agli esperti della cyber security!
Al suo interno
Hacking Around e Technical Video.

Nella sezione Rubriche:
Bibliografia
Dalla Redazione
Dalle Aziende
Dalle Università
Eventi
Offerte di Lavoro

www.cybertrends.it

Indice

Quantum opportunità o minaccia?

Autore: Nicola Sotira

I computer quantistici rappresentano una frontiera rivoluzionaria nell'ambito dell'elaborazione dell'informazione. Sfruttando i principi della meccanica quantistica, questi dispositivi promettono di risolvere problemi complessi non risolvibili dai classici computer che conosciamo.

Una delle principali opportunità offerte dai computer quantistici è la capacità di eseguire calcoli estremamente complessi a velocità sorprendente. Questi sistemi possono esplorare una vasta gamma di soluzioni simultaneamente, grazie alla sovrapposizione quantistica, accelerando notevolmente la risoluzione di problemi computazionalmente intensivi.

Legata a questa tematica emerge quella della crittografia quantistica che appare una promettente soluzione alle sfide della sicurezza informatica nell'era digitale. Mentre la crittografia classica si basa su algoritmi matematici complessi, la crittografia quantistica sfrutta i principi della fisica quantistica per garantire una sicurezza ancora più elevata. Tuttavia, nonostante le sue potenzialità rivoluzionarie, la crittografia quantistica presenta sia prospettive promettenti che possibili minacce che richiedono attenzione.

Da un lato, la crittografia quantistica offre una sicurezza ineguagliabile grazie a principi fondamentali della fisica quantistica, come l'incertezza e l'interferenza. Il suo protocollo sfrutta la proprietà di indistinguibilità quantistica dei fotoni per garantire la sicurezza della trasmissione di chiavi crittografiche. Questo metodo impedisce efficacemente l'intercettazione delle chiavi crittografiche da parte di terze parti, rendendo praticamente impossibile il deciframeto dei dati trasmessi.

Inoltre, la crittografia quantistica potrebbe rivoluzionare settori sensibili come la sicurezza delle comunicazioni governative e finanziarie. La capacità di trasmettere informazioni in modo sicuro e privato potrebbe portare a una maggiore fiducia nelle transazioni online e a una maggiore protezione dei dati sensibili.

Tuttavia, nonostante le sue promesse, la crittografia quantistica affronta anche diverse sfide e minacce. Uno dei principali ostacoli è la complessità tecnologica e l'infrastruttura necessaria per implementare questa tecnologia.

Altri aspetti critici includono la vulnerabilità alle attuali minacce informatiche. Sebbene la crittografia quantistica offra protezione contro l'intercettazione delle chiavi crittografiche, rimane vulnerabile agli attacchi di tipo fisico, come la manipolazione dei dispositivi di misurazione dei fotoni. Inoltre, la scalabilità dei sistemi quantistici rimane una sfida aperta, con l'aumento delle dimensioni dei sistemi che potrebbe comportare un aumento esponenziale delle risorse richieste.

Infine, c'è il rischio che lo sviluppo della crittografia quantistica possa portare a una corsa agli armamenti cibernetici, in cui le nazioni e le organizzazioni cercano di sviluppare tecnologie quantistiche per ottenere un vantaggio strategico. Questo potrebbe portare a una maggiore instabilità nel panorama della sicurezza informatica globale.

La crittografia quantistica offre, pertanto, prospettive entusiasmanti per il futuro della sicurezza informatica, con il potenziale per rivoluzionare la protezione dei dati sensibili.

Un punto di attenzione occorre farlo sulla crittografia tradizionale, che potrebbe essere messa a rischio dall"avvento dei computer quantistici che rappresentano una minaccia significativa per quest'ultima. Gli algoritmi crittografici utilizzati comunemente, come l'RSA e l'ECC, potrebbero essere vulnerabili agli algoritmi quantistici che possono fattorizzare rapidamente numeri primi e compromettere la sicurezza dei dati crittografati. Questo potrebbe mettere a rischio la riservatezza delle comunicazioni, l'integrità dei dati e l'autenticazione delle informazioni. Inoltre, la presenza di computer quantistici potrebbe accelerare la decrittazione delle chiavi crittografiche precedentemente intercettate, compromettendo la sicurezza dei dati archiviati nel passato. Come sempre delizie e dolori che abbiamo cercato di rappresentare in questo numero cercando di fare divulgazione e dare qualche concreta soluzione. Buona Lettura… ■

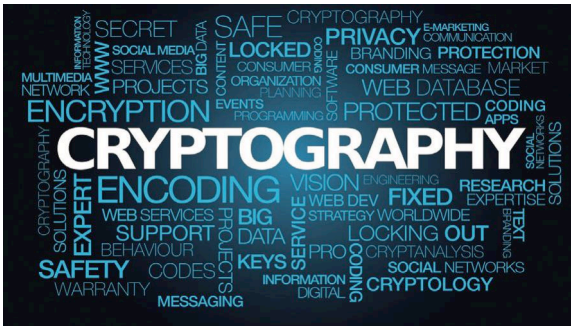
BIO

Nicola Sotira è Responsabile del CERT di Poste Italiane. Lavora nel settore della sicurezza informatica e delle reti da oltre venti anni con un'esperienza maturata in ambienti internazionali. Contesti nei quali si è occupato di crittografia e sicurezza di infrastrutture, lavorando anche in ambito mobile e reti 3G. Ha collaborato con diverse riviste nel settore informatico come giornalista contribuendo alla divulgazione di temi inerenti la sicurezza e aspetti tecnico legali. Docente dal 2005 presso il Master in Sicurezza delle reti dell'Università La Sapienza. Membro della Association for Computing Machinery (ACM) dal 2004 e promotore di innovazione tecnologica, collabora con diverse start-up in Italia e all'estero. Membro di Italia Startup nel 2014 dove con alcune società ha partecipato allo sviluppo e progetto di servizi in ambito mobile e collabora con Oracle Security Council.

Una nuova era nella gestione della crittografia.

Autore: Marc Manzano

La crittografia è la scienza che si occupa di studiare le tecniche per rendere sicure le comunicazioni, soprattutto in presenza di malintenzionati in grado di alterare o intercettare le informazioni. I suoi principali obiettivi sono la riservatezza (garantire la privacy dei dati), l'integrità (impedire la modifica non autorizzata dei dati), il non ripudio (garantire che i partecipanti a una comunicazione non possano successivamente negare la loro partecipazione) e l'autenticazione (verificare l'identità delle parti coinvolte). Negli ultimi tre decenni, l'evoluzione della crittografia è stata parallela alla crescita esplosiva della comunicazione digitale e di Internet. Negli anni '70 la crittografia era prevalentemente un ambito di interesse accademico e aveva la sua più ampia applicazione nel mondo militare.



La comparsa del World Wide Web all'inizio degli anni '90 ha reso necessario l'utilizzo di protocolli crittografici più robusti per proteggere le interazioni online in rapido aumento, portando alla crescita della crittografia a chiave pubblica e all'introduzione di protocolli crittografici come l'SSL. Gli anni 2000 hanno visto la proliferazione del commercio elettronico, la conseguente necessità di transazioni sicure, che hanno ulteriormente favorito innovazioni come algoritmi e protocolli crittografici più robusti che consentono un maggior numero di casi d'uso, e l'arrivo dell'infrastruttura a chiave pubblica e dei certificati digitali. Nel 2010, l'attenzione si è focalizzata sullo sviluppo di algoritmi quantum-resistant, preparandosi a un futuro in cui la crittografia tradizionale potrebbe essere potenzialmente violata dal quantum computing. Al giorno d'oggi, la crittografia è una realtà pervasiva e tecnologie come TLS o applicazioni di messaggistica sicura come Signal, Whatsapp o iMessage si basano fortemente su algoritmi e protocolli crittografici.

QRL
The Quantum-Resistant Ledger

Allo stesso tempo, il mondo della cybersecurity è esploso e l'offerta di soluzioni ha subito una significativa trasformazione, guidata dal rapido progresso della tecnologia e dall'evoluzione del panorama delle minacce informatiche. Inizialmente, la cybersecurity si basava principalmente su software antivirus e firewall progettati per proteggere da virus e accessi non autorizzati. Man mano che Internet è diventato un elemento indispensabile per le attività aziendali, la necessità di misure di sicurezza più sofisticate ha portato allo sviluppo di sistemi di rilevamento delle intrusioni (IDS) e di sistemi di prevenzione delle intrusioni (IPS). Tra la metà degli anni 2000 e il 2010 si è assistito all'ascesa del cloud computing, con il conseguente passaggio a soluzioni e servizi di sicurezza basati sul cloud che offrono scalabilità e flessibilità. In questo periodo si è assistito anche alla comparsa di strumenti di protezione dalle minacce avanzate (ATP), che affrontano minacce più complesse come gli exploit zero-day e le minacce persistenti avanzate (APT). Oggi le soluzioni di cybersecurity sono diventate opere di ingegneria molto avanzate, che sfruttano l'intelligenza artificiale (AI) e l'apprendimento automatico (ML) per il rilevamento predittivo delle minacce, la risposta automatica agli incidenti e l'analisi del comportamento, fornendo soluzioni di sicurezza più proattive e adattive. Inoltre, l'integrazione dei sistemi di gestione delle informazioni e degli eventi di sicurezza (SIEM)

BIO

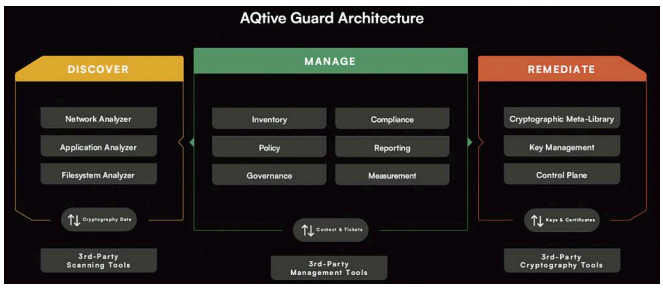
Marc Manzano è General Manager della Quantum Security, guida il gruppo di sicurezza quantistica presso Sandbox. I suoi attuali interessi di ricerca includono la crittografia post-quantistica, la crittografia leggera, la crittografia completamente omomorfa, l'intersezione tra apprendimento automatico e crittoanalisi, l'ottimizzazione delle prestazioni delle implementazioni crittografiche su un'ampia gamma di architetture e algoritmi quantistici. Ha presentato più di 25 articoli a conferenze internazionali, pubblicato più di dieci articoli su riviste scientifiche e collaborato a diversi libri scientifici relativi alla crittografia e alla sicurezza delle reti informatiche. Negli ultimi dieci anni, il Dott. Manzano ha guidato lo sviluppo di numerose librerie e protocolli crittografici sicuri. Il dottor Manzano è stato in passato Senior Staff Software Engineer presso Google e, prima ancora, è stato vicepresidente del Centro di ricerca sulla crittografia presso il Technology Innovation Institute, un centro di ricerca scientifica con sede negli Emirati Arabi Uniti. In precedenza, ha ricoperto diverse posizioni in cui era responsabile dell'implementazione di componenti crittografici fondamentali di una varietà di prodotti di comunicazione sicura, inclusa una piattaforma di voto elettronico. Il Dott. Manzano ha conseguito un dottorato di ricerca in Computers Network Security, conseguito sotto la supervisione dell'Università di Girona (Spagna) e della Kansas State University (Stati Uniti). Ha conseguito un Master in Informatica presso l'Università di Girona (Spagna), mentre ha svolto soggiorni di ricerca presso UC3M (Spagna) e DTU (Danimarca). Ha iniziato la sua carriera di ricercatore mentre conseguiva la sua laurea in ingegneria informatica presso l'Università di Strathclyde (Regno Unito).

offre una visibilità completa sugli ambienti IT, migliorando il rilevamento e la gestione degli incidenti di sicurezza. Questi progressi riflettono il continuo rincorrersi degli esperti della cybersecurity e dei cybercriminali.

Tuttavia, mentre le soluzioni di cybersecurity si sono trasformate in modo massiccio e la crittografia è alla base della nostra società digitale, per anni non sono state disponibili soluzioni in grado di gestire la crittografia in modo moderno e olistico, offrendo una visibilità completa degli asset crittografici, un controllo e una protezione automatizzati. La **gestione della crittografia** sta emergendo come un aspetto fondamentale della cybersecurity, concentrandosi sulla supervisione e sulla

gestione di chiavi crittografiche, algoritmi e policy in diversi ambienti IT. Le moderne piattaforme di gestione della crittografia sono state sviluppate per colmare questo gap, fornendo visibilità, gestione e sicurezza centralizzate per le risorse crittografiche. Queste piattaforme consentono alle organizzazioni di utilizzare l'agilità crittografica, permettendo loro di adattarsi rapidamente a nuovi algoritmi, protocolli o provider crittografici e di eliminare quelli vulnerabili, mitigando così i rischi associati ai progressi del quantum computing e all'evoluzione dei requisiti normativi. Inoltre, facilitano la compliance con le normative globali sulla protezione dei dati, garantendo che le procedure di sicurezza e privacy dei dati soddisfino gli standard più elevati. Inoltre, consentono una più rapida implementazione dello Zero Trust. Con il passare del tempo, il ruolo della gestione della crittografia è destinato a diventare sempre più centrale nelle strategie di cybersecurity sia per il settore pubblico che per quello privato, garantendo che con l'evolversi delle minacce digitali si evolvano anche le nostre capacità di proteggere le infrastrutture digitali.

In SandboxAQ abbiamo sviluppato AQtive Guard, la nostra moderna piattaforma di gestione unificata della crittografia. AQtive Guard consente ai clienti di scoprire le risorse crittografiche nella loro infrastruttura IT aziendale, di creare un inventario crittografico che consente il monitoraggio, di fornire verifiche dei rischi e della conformità in base alle policy, alle normative e agli standard di sicurezza aziendali e di offrire funzionalità di rimedio. Il nostro prodotto si integra con le applicazioni di terze parti a cui i clienti potrebbero già avere accesso e sfrutta il suo approccio olistico per fornire ulteriore valore ai clienti.

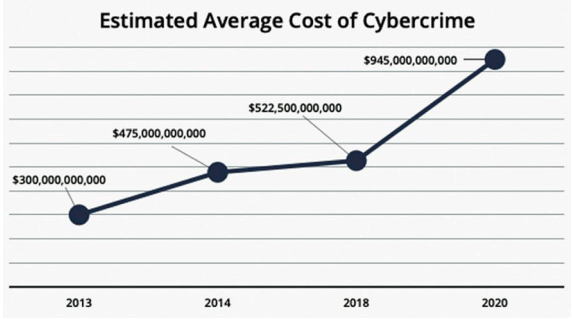


Ad oggi, abbiamo assistito clienti come l'Aeronautica Militare degli Stati Uniti, il Dipartimento della Salute e dei Servizi Umani, l'Agenzia per i Sistemi Informativi della Difesa (DISA), aziende come Vodafone, SoftBank, Informatica, Cloudera e diverse banche di livello mondiale, aiutandoli a la loro posizione di sicurezza attraverso la modernizzazione della crittografia. Abbiamo anche aderito a diversi consorzi di settore come il National Institute of Standards and Technology (NIST) NCCoE, il GSMA's PQTN, la Linux Foundation's PQCA e la MITRE's PQC Coalition. Queste associazioni svolgono un ruolo cruciale nel formare i leader globali sulle misure di sicurezza proattive e sulla protezione dei loro dati più sensibili. ■

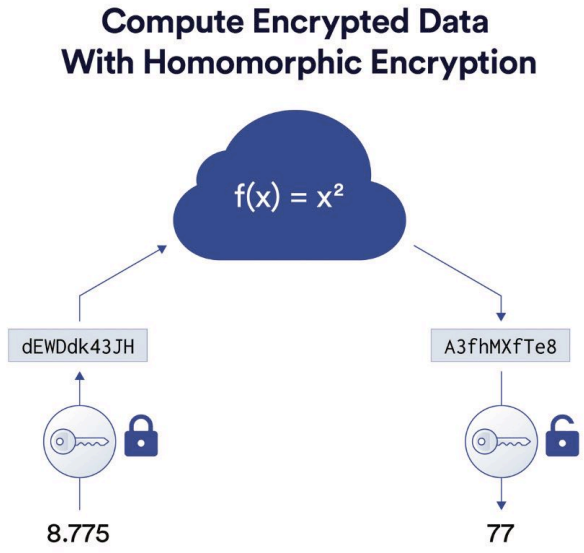
Data-In-Use Encryption: il Cambiamento Fondamentale della Crittografia dei Dati.

Autore: Ryan Lasmaili

Nell'era digitale, i dati sono la pietra miliare dell'economia globale e la loro protezione è fondamentale. Nonostante ciò, un volume significativo di informazioni sensibili circola in chiaro, accessibile a chiunque abbia capacità di intercettazione. Questa vulnerabilità ha profonde implicazioni, non solo per la privacy individuale ma anche per la stabilità economica globale. L'impatto del cybercrime sull'economia mondiale ha raggiunto l'allarmante cifra di 1.000 miliardi di dollari nel 2020, pari a oltre l'1% del PIL mondiale. Questa cifra evidenzia l'urgente necessità di rafforzare le misure di protezione dei dati (McAfee, 2020).



Nel campo della cybersecurity, i paradigmi tradizionali di crittografia - crittografia dei dati a riposo e crittografia dei dati in transito - sono stati utilizzati come strumenti fondamentali per proteggere i dati da accessi non autorizzati. Tuttavia, queste misure da sole non riescono a risolvere le vulnerabilità a cui sono esposti quando i dati devono essere decifrati per essere elaborati. La crittografia dei dati a riposo protegge i dati memorizzati su disco, mentre la crittografia in transito protegge i dati che transitano sulle reti. Tuttavia, una volta che i dati per essere accessibili o per essere elaborati, vengono decriptati, entrano in uno stato che li rende vulnerabili alle minacce informatiche. Questo stato di decriptazione, spesso trascurato, è il momento in cui i dati sono più vulnerabili, in quanto diventano un allettante obiettivo per i cyber-attaccanti che cercano di sfruttare la breve finestra di tempo in cui le protezioni dei dati sono disattivate. La necessità di decifrare i dati prima di essere elaborati non solo comporta una grave falla di sicurezza, ma sottolinea anche i limiti dei metodi di crittografia tradizionali nel fornire una protezione completa dei dati in un'era in cui la privacy e la sicurezza dei dati sono fondamentali. Questa falla evidenzia l'urgente necessità di soluzioni innovative, come la crittografia completamente omomorfa, che permettano di elaborare i dati senza mai decifrarli, mantenendo così la loro riservatezza per tutto il loro ciclo di vita.



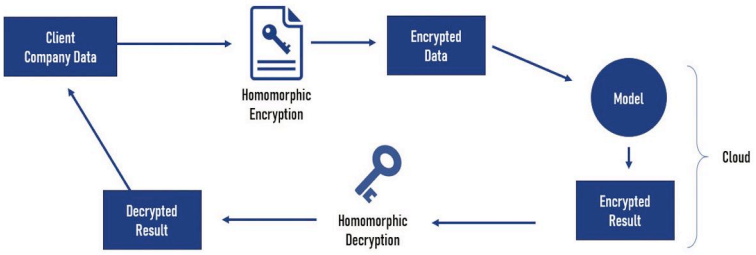
BIO

Ryan Lasmaili è cofondatore e CEO di Vaultree, un'azienda pionieristica specializzata nella tecnologia di crittografia Data-In-Use (come FHE) più veloce al mondo per i database. La sua passione per le innovazioni tecnologiche, che vanno dalla tecnologia spaziale all'EnviroTech, risale alla sua infanzia. Negli ultimi 12 anni, Ryan si è dedicato alle startup tecnologiche, concentrandosi sullo sviluppo di soluzioni innovative a sfide importanti. Con un background in matematica finanziaria, Ryan possiede una solida base per la risoluzione dei problemi. La sua passione consiste nell'affrontare questioni complesse, in particolare nel campo della cybersecurity. Cerca costantemente l'opportunità di applicare il suo pensiero fuori dagli schemi per affrontare le sfide della crittografia e della protezione dei dati, sia attuali che future, considerandole come le sue imprese più importanti. Al di là delle sue attività professionali, Ryan si diletta nell'esplorazione del mondo sottomarino attraverso le immersioni subacquee, che considera ironicamente "un'alternativa economica alla gravità zero". Il suo amore per i viaggi gli permette di assecondare la sua curiosità di conoscere nuove persone e di sperimentare in prima persona culture diverse.

La Fully Homomorphic Encryption (FHE) consente di elaborare i dati mentre sono crittografati. Questo approccio garantisce la sicurezza dei dati contro le minacce informatiche anche durante l'elaborazione, contrastando le vulnerabilità critiche associate ai dati in chiaro.

Lo sviluppo di algoritmi FHE in real-time, come quelli sviluppati da Vaultree, azienda irlandese che realizza tecnologie crittografiche, rappresenta un significativo passo in avanti nella crittografia. Questa innovazione facilita il processo di elaborazione dei dati crittografati, eliminando le limitazioni computazionali precedentemente legate a FHE. Questo progresso non solo mitiga i rischi di sicurezza legati ai dati in chiaro, ma apre anche nuove opportunità di business sfruttando l'intero valore dei dati in modo sicuro e rispettoso della privacy.

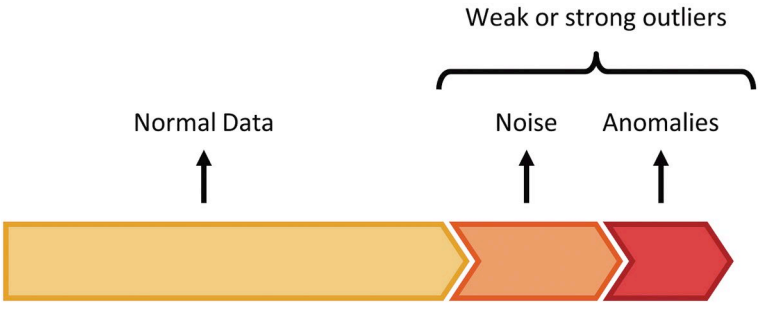
Nel suo fulcro, FHE opera in base al principio dell'omomorfismo, una proprietà matematica che garantisce che le operazioni eseguite sui dati crittografati (testo cifrato) producano risultati equivalenti al processo della decodificazione, come se fossero eseguite sui



dati originali non crittografati (testo in chiaro). Questa capacità è garantita da complesse strutture matematiche e da algoritmi che consentono sia l'addizione che la moltiplicazione sui cifrari, operazioni fondamentali che possono essere combinate per eseguire in modo sicuro qualsiasi calcolo arbitrario.

Il fondamento matematico di FHE prevede intricate strutture algebriche, come i reticoli, che vengono utilizzate per costruire schemi di crittografia in grado di gestire operazioni additive, moltiplicative, di sottrazione e di divisione sui testi cifrati. Uno schema FHE inizia tipicamente con la crittografia dei dati utilizzando una chiave pubblica, generando un testo cifrato che nasconde i dati originali. I calcoli vengono quindi eseguiti su questi testi cifrati attraverso operazioni algebriche accuratamente progettate che imitano i calcoli desiderati sui testi in chiaro.

Un aspetto fondamentale della struttura matematica di FHE è la gestione del «rumore» che si accumula con ogni operazione eseguita sul testo cifrato. Questo rumore, se non controllato, può crescere fino a oscurare i dati cifrati, rendendoli inutili. Gli schemi FHE incorporano tecniche di gestione del rumore per garantire che, nonostante l'accumulo di rumore, il sistema possa comunque decifrare con precisione il risultato delle computazioni eseguite sui dati cifrati.



L'introduzione del rumore e la sua gestione è un elemento cruciale in FHE, che garantisce sia la sicurezza della crittografia sia l'integrità della computazione. Ad esempio, nel caso di schemi FHE basati su reticolo, i dati crittografati sono rappresentati come punti all'interno di un reticolo ad alta dimensione. Le operazioni sui dati cifrati si traducono in operazioni all'interno di questo spazio reticolare, con strategie di gestione del rumore che assicurano che queste operazioni non portino il sistema al di fuori dei limiti dello spazio decifrabile.

La capacità di elaborare i dati mantenendoli crittografati offre alle aziende possibilità senza precedenti. Consente la condivisione sicura dei dati e l'analisi basata sulla collaborazione tra diversi settori, favorendo l'innovazione

e la creazione di nuovi modelli di business senza compromettere la privacy dei dati. Questo approccio può portare a vantaggi competitivi e guidare la crescita utilizzando i dati in modi in precedenza impossibili a causa della privacy o delle restrizioni normative.

Inoltre, l'uso di dati crittografati facilita la conformità alle severe leggi sulla protezione dei dati, come il GDPR e il CCPA. Mantenendo i dati sempre crittografati le organizzazioni possono rispettare più facilmente le normative sulla privacy, riducendo al minimo il rischio di violazione dei dati e le relative sanzioni. Ciò aumenta la fiducia dei clienti e rafforza la reputazione dell'azienda come responsabile della privacy dei dati.

In passato, le aziende hanno dovuto muoversi in un complesso panorama di requisiti di conformità, che spesso richiedevano per l'elaborazione la decriptazione dei dati sensibili, introducendo rischi significativi per la sicurezza. FHE può non solo semplificare la conformità alle severe normative sulla protezione dei dati, ma anche ridurre significativamente l'onere di conformità per le aziende. Di conseguenza, le aziende possono trasferire le risorse dalla gestione della conformità alle attività aziendali centrali, favorendo la crescita e l'innovazione. Questo cambiamento segna un passaggio decisivo verso un futuro in cui le aziende possono concentrarsi sui loro obiettivi primari senza compromettere la privacy e la sicurezza dei dati, favorendo un ambiente in cui la conformità è perfettamente integrata nel tessuto delle operazioni digitali e vista come un'opportunità di business e non come un ostacolo al business.

Alcuni degli ultimi progressi, tra cui gli sforzi in corso per integrare nuove funzionalità FHE nei servizi cloud, consentiranno alle aziende di sfruttare la scalabilità e la flessibilità del cloud computing, garantendo al contempo la privacy e la sicurezza dei dati. Questa combinazione non solo migliora la protezione dei dati, ma ottimizza anche le risorse di calcolo. Riducendo la necessità di processi di decodifica e ricodifica, le aziende possono ottenere un'elaborazione dei dati più efficiente, riducendo le richieste di calcolo e i costi associati.

Con la crescita dell'economia digitale, l'importanza di gestire in modo sicuro i dati - a riposo, in transito e, soprattutto, **in-use** - diventa sempre più fondamentale per salvaguardare gli interessi economici e facilitare la crescita. L'adozione di strategie di gestione dei dati basate sulla crittografia rappresenta un progresso significativo verso la sicurezza del nostro futuro digitale e lo sfruttamento del potenziale dei dati crittografati per promuovere la ricchezza economica globale.

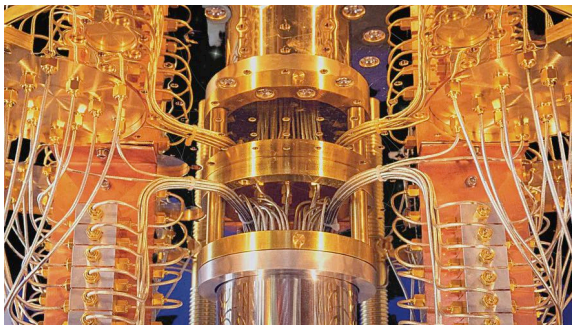
Homomorphic Encryption

Nel mondo di oggi, dove i nostri momenti più personali sono digitalizzati, la privacy dei dati emerge non solo come una sfida tecnica, ma come una preoccupazione strettamente personale. Si tratta di salvaguardare le nostre storie più intime, di proteggere l'essenza di chi siamo in una realtà digitale in cui le informazioni fluiscono liberamente. Lo sviluppo della crittografia dei dati in-use, rappresentato da tecnologie come la Fully Homomorphic Encryption (FHE), è un segnale di speranza in questa ricerca. Queste tecnologie promettono un futuro in cui i nostri dati - i nostri ricordi digitali - possono attraversare il mondo cibernetico al riparo da occhi indiscreti, anche quando

vengono utilizzati. Non si tratta solo di proteggere bit e byte, ma di preservare la dignità umana e la libertà in un'epoca in cui la privacy è troppo facilmente compromessa. Con lo sviluppo di tali innovazioni, ci avviciniamo a un mondo in cui rispettare la privacy dei dati equivale a onorare l'essenza stessa della nostra umanità, assicurando che le nostre identità digitali e reali siano protette con lo stesso zelo. Promuovendo la crittografia dei dati in uso, non ci limitiamo a migliorare la sicurezza informatica, ma prendiamo posizione per il diritto umano fondamentale alla privacy, alimentando un futuro in cui la tecnologia sia al servizio dell'umanità, salvaguardando le nostre storie e i nostri segreti con la riverenza che meritano. ■

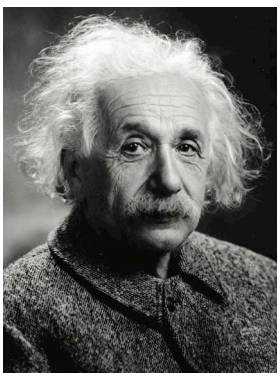
Quantum computing ibrido. Il futuro è già qui.

Autore: Francesco Corona

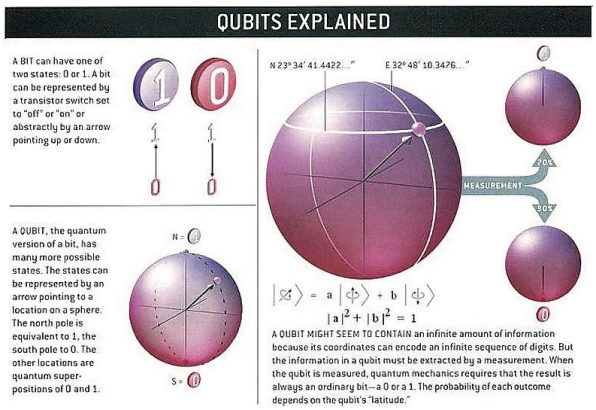


GENERALITÀ. Nella rivista Cybersecurity Trends n.2 del 2021 ripercorrevamo le tappe fondamentali che portarono alla nascita delle prime sperimentazioni di computer quantistici passando attraverso la computazione parallela degli anni novanta (https://www.cybertrends.it/dalla-processazione-parallela-al-computer-quantistico/ [B000]) sino ai nostri giorni. Concludevamo infine l'articolo con il seguente pensiero: "Il computer quantistico sarà molto utilizzato per alcune casistiche risolutive dove la componente Non Polinomiale (NP) dello spazio delle soluzioni e quindi la natura probabilistica risulta una predominante. Citiamo alcuni di questi scenari: reti neurali e intelligenza artificiale, chimica e biochimica, scenari di controllo dei domini della conflittualità (aria, acqua, terra, spazio e dominio cibernetico), settori finanziari e di trading, algoritmi predittivi, alte energie ed energie rinnovabili, biotecnologie e virologia, tecnologie dei materiali e nanotecnologie, simulazioni e test previsionali, cybersecurity, crittografia e analisi malware… Saremo quindi difronte a una nuova generazione di computer ibridi che supereranno i limiti attuali imposti dalla legge di More… verso un nuovo orizzonte degli eventi più consono alle esigenze di coniugare i fenomeni naturali con la tecnologia e consentire all'uomo di raggiungere traguardi evolutivi di portata epocale." Direi che questo nuovo orizzonte degli eventi è già qui, dopo soli tre anni dalla pubblicazione dell'articolo, grazie soprattutto all'impulso che la ricerca avanzata, sia accademica sia industriale, ha saputo fornire in così poco tempo in questo settore, quello ibrido, sapientemente orchestrato, soprattutto nel cloud, con applicazioni di intelligenza artificiale, machine learning e applicazioni di analisi predittive e simulazioni di scenari. Cercheremo, per quanto ci è concesso, di fornire un aggiornamento adeguato all'attuale orizzonte degli eventi puntando agli aspetti inerenti quelle applicazioni ibride che trovano negli ambienti cloud una naturale configurazione di sviluppo più adatta al mercato dei prossimi decenni.

POTENZA QUANTISTICA. Il segreto della potenza di un computer quantistico risiede nella sua capacità di generare e manipolare bit quantistici, o qubit. I qubit possono rappresentare numerose possibili combinazioni di 1 e 0 contemporaneamente rispetto ai computer classici basati sulla macchina di Turing. Questa capacità di trovarsi simultaneamente in più stati è chiamata Sovrapposizione (Superposition). Per mettere i qubit in sovrapposizione, i ricercatori manipolano tali qubit in una CPU quantistica utilizzando laser o raggi a microonde. Grazie a questa possibilità un computer quantistico con diversi qubit in sovrapposizione può analizzare simultaneamente un vasto numero di potenziali risultati. Il risultato finale di un calcolo emerge solo quando i qubit sono stati misurati, il che fa immediatamente "collassare" il loro stato quantistico a 1 o 0. È possibile inoltre generare coppie di qubit che sono in "Entanglement", ciò significa che la modifica dello stato di uno dei qubit cambierà istantaneamente lo stato dell'altro in modo controllato anche se sono separati da distanze molto elevate. L'entanglement è una proprietà delle particelle elementari con i loro movimenti di spin rilevata dallo stesso Einstein nel famoso esperimento EPR (Eistein-Podolsky-Rosen) [B006].



In realtà l'aggiunta di qubit a una CPU quantistica produce un aumento esponenziale della sua capacità di elaborazione. Tuttavia le macchine quantistiche sono molto più soggette a errori dei computer classici a causa della non coerenza prodotta dall'interazione con l'ambiente esterno che genera perturbazioni dello stato coerente. Ecco perché i qubit vengono raffreddati criogenicamente oppure mantenuti in uno stato di coerenza nelle così dette camere a vuoto.



BIO

Francesco Corona è ricercatore e docente di Cyber Intelligence, già direttore del master di Hacking e Ingegneria della Sicurezza presso Link Campus University Rome; è stato docente a contratto per 11 anni presso la Facoltà di Ingegneria Gestionale di Roma2 Tor Vergata Dipartimento di Ingegneria dell'Impresa. Ha svolto intensa attività di ricerca nel capo dell'Intelligenza Artificiale e delle Reti Neurali per conto del CNR-IASI di Roma. Svolge attività di ricerca in svariati settori e in particolare in quello della Cybersecurity per conto di primari player nazionali e internazionali. Nel 2013 consegue il prestigioso Premio Nazionale per l'innovazione e il premio ICT Confindustria. f.corona@unilink.it

APPLICAZIONI QUANTISTICHE. Le macchine quantistiche risultano interessanti per la risoluzione di problemi legati alla bioingegneria molecolare e all'ottimizzazione di funzioni matematiche e simulazioni perché inducono soluzioni rapide in contesti di analisi parallela dei dati. Le macchine quantistiche potrebbero inoltre essere utilizzate per accelerare i processi di intelligenza artificiale e machine learning. Siamo ancora in uno stadio embrionale delle differenti declinazioni di ricerca ma la comunità scientifica e industriale si trova in un vero e proprio fermento innovativo rivoluzionario. Potrebbero tuttavia essere necessari alcuni anni prima che i computer quantistici raggiungano il loro pieno potenziale. Le università e le imprese che vi lavorano stanno svolgendo attività accademico-formative adeguate ad affrontare l'attuale carenza di ricercatori qualificati.

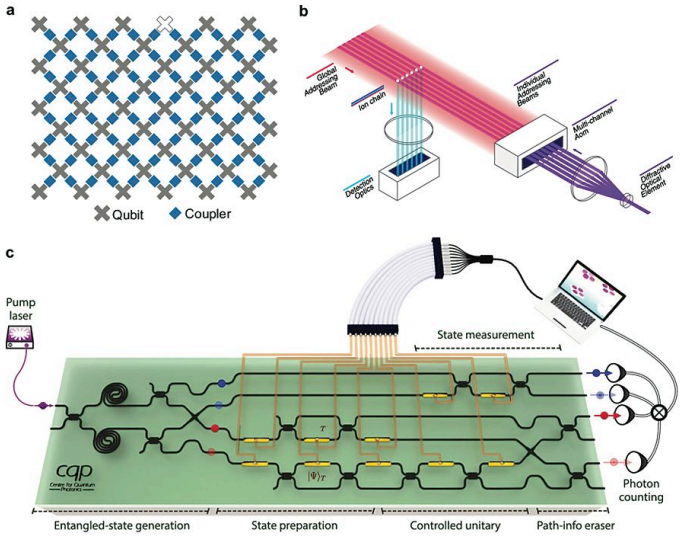


Fig.1 *- Esempi di architetture di calcolo quantistico. (a) Architettura a 53 qubit utilizzata da Google. Vista schematica dall'alto di qubit superconduttori (grigio) con accoppiatori adattivi (blu). (b) Hardware da 11 qubit utilizzato da IonQ. Gli ioni intrappolati in una catena lineare vengono rilevati e manipolati tramite componenti ottici. (c) Architettura basata sull'ottica lineare utilizzata da PsiQuantum. I fotoni si propagano attraverso i percorsi definiti (linee nere) con porte logiche quantistiche e regioni di accoppiamento. Rif. [B001]*

L'informatica quantistica richiede connessioni con il mondo esterno. Tali connessioni potrebbero riguardare la collaborazione tra un computer quantistico e una risorsa informatica esterna tradizionale come un supercomputer in un approccio computazionale cosiddetto ibrido. Quindi è possibile produrre risultati-output dei calcoli quantistici per computer-input di ultima generazione per essere poi fruibili dagli operatori finali. In entrambi i casi, esiste un paradosso tra la necessità di isolare i qubit nei computer quantistici dalle interruzioni causato dall'ambiente esterno in particolare l'accesso ai risultati computazionali in ambienti tradizionali a temperatura ambiente. IBM, ad esempio, si è dedicata alla realizzazione di una classe speciale di amplificatori a microonde a basso rumore, noti come amplificatori a limitazione quantistica (QLA), per affrontare questa sfida. Le prestazioni dei QLA devono essere migliorate prima che possano supportare le future generazioni di computer quantistici "di grandi dimensioni" distribuiti nel cloud. In sintesi un computer quantistico è costituito da tre parti fondamentali:

A. Lo spazio di alloggiamento del Quantum Processor Unit dimensionato a n-qubits.

B. Un metodo per il trasferimento dei segnali ai qubit.

C. Un sistema di interpretazione dei dati e invio dei risultati a un elaboratore.

I sistemi qubit richiedono pertanto un attento controllo dello stato di coerenza per funzionare in modo

utile. Tale controllo può essere gestito anche utilizzando le classiche risorse informatiche associate al computer quantistico. La struttura di un'architettura informatica ibrida quantistico-classica operativa può essere vista come quattro "strati" distinti:

1. Strato quantistico in cui esistono i qubit e dove avviene il calcolo quantistico.
2. Strato di controllo e misurazione a temperature criogeniche che controlla il funzionamento e la misurazione dei qubit.
3. Strato del processore di controllo a temperatura ambiente; esso controlla la sequenza di operazioni e misurazioni necessarie all'algoritmo quantistico, inclusa la determinazione della necessità e il controllo delle operazioni interattive.
4. Strato del processore host, tipicamente una macchina in cloud che fornisce accesso a reti e array di archiviazione di grandi dimensioni e supporta interfacce utente, consente pertanto interazioni tramite istruzioni oltre alla mutuata lettura dei risultati quantistici.

Tipologia di calcolo quantistico

Esistono ad oggi quattro casistiche di calcolo quantistico (batch, interattivo, integrato e distribuito) ciascuna delle quali viene di seguito specificata:

A. **Calcolo quantistico in batch.** I client locali definiscono i circuiti e li inviano come lavori all'unità di elaborazione quantistica (QPU), che restituisce il risultato. L'unione di più circuiti in un unico lavoro, tuttavia, elimina i tempi di attesa, consentendo di eseguire più lavori parallelamente e quindi più velocemente. Esempi di problemi che possono trarre vantaggio dal calcolo quantistico batch includono tipologie analoghe all'algoritmo di Shor e alla stima delle fasi quantistica.

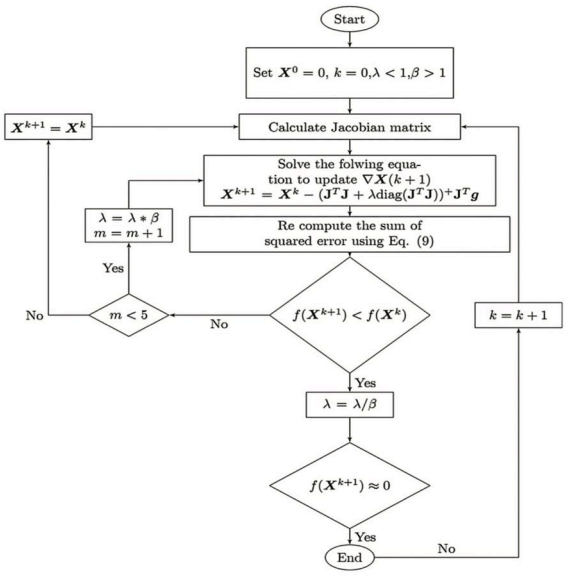
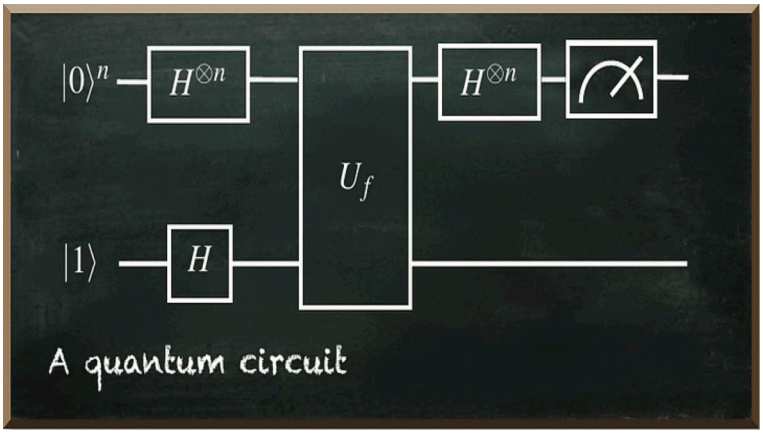


Fig.2 *- Algoritmo di Shor [B009]*

L'algoritmo di Shor è un algoritmo che consente di risolvere il problema della fattorizzazione dei numeri interi. L'algoritmo consiste di due passi: A) una riduzione del problema di fattorizzazione a un problema di calcolo dell'ordine eseguibile su un computer classico. B) La risoluzione, tramite un algoritmo (detto appunto quantistico) del problema come al punto A).

B. **Calcolo quantistico interattivo.** In questo modello, la risorsa di calcolo del client viene spostata nel cloud, con conseguente latenza inferiore ed esecuzione ripetuta del circuito quantistico impostato dall'utente con parametrizzazione specifica. I lavori possono essere raggruppati logicamente in una sessione unica e avere la priorità rispetto ai lavori non di sessione. Sebbene le sessioni consentano tempi di coda più brevi e problemi di esecuzione più lunghi, gli stati dei qubit decadono tra ogni iterazione. Esempi di problemi che possono utilizzare questo approccio sono gli autosolutori quantistici variazionali (VQE) e gli algoritmi di ottimizzazione approssimata quantistica (QAOA).



C. **Calcolo quantistico integrato.** Con il calcolo quantistico integrato, l'architetture classica e quantistica sono strettamente accoppiate, consentendo di eseguire calcoli classici mentre i qubit fisici sono coerenti. Sebbene limitato dalla durata dei qubit in coerenza e dalle necessità di correzione immediata degli errori, questo calcolo consente ai programmi quantistici di separarsi dai soli circuiti. I programmi possono ora utilizzare costrutti di programmazione comuni per eseguire misurazioni sui circuiti intermedi, ottimizzare e riutilizzare i qubit e adattarsi in tempo reale alla Quantum Processor Unit (QPU). Esempi di scenari che possono trarre vantaggio da questo modello sono la stima della fase adattiva di un fenomeno naturale e l'apprendimento automatico.

D. **Calcolo quantistico distribuito.** Il lungo tempo di coerenza fornito dai qubit logici consente calcoli complessi e distribuiti su risorse cloud eterogenee. Abbinata a una QPU composta da un gran numero di qubit, possiamo ipotizzare che questa architettura venga utilizzata per risolvere problemi come la valutazione di reazioni bio-chimiche complete che possono avvantaggiare particolari applicazioni commerciali e i problemi più difficili che l'umanità dovrà affrontare.

I componenti di calcolo quantistico hanno un modello operativo diverso da quello del software classico. In genere sono presenti uno o più componenti di calcolo classici che orchestrano l'esecuzione di componenti quantistici. Questa orchestrazione include le attività seguenti:

- Preparazione dei dati di input
- Invio di processi quantistico a un ambiente quantistico di destinazione
- Monitoraggio dell'esecuzione del processo
- Post-elaborazione dei risultati del processo

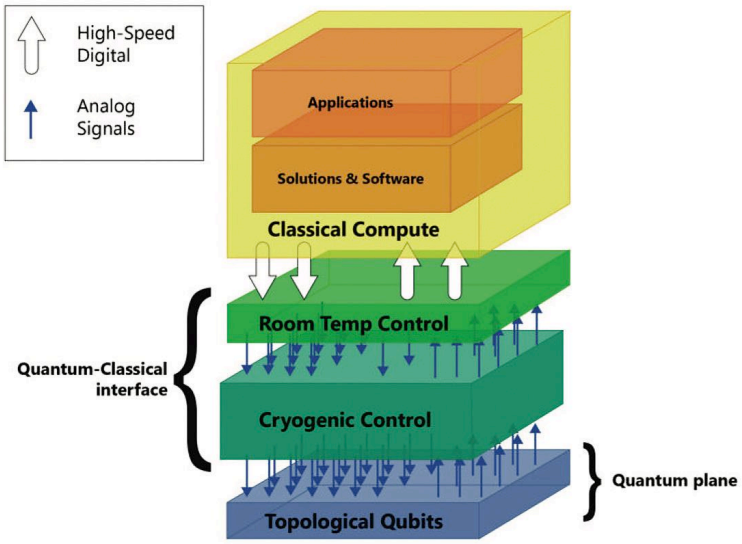


Fig.3 *- Stack di calcolatore ibrido quantistico-classico. Al vertice c'è la classica piattaforma informatica che include programmazione applicativa di alto livello e funzioni HMI. Al centro ci sono due piani di controllo, uno che opera a temperatura ambiente per collegarsi al computer classico e uno a temperature criogeniche per collegarsi con i qubit nel computer quantistico in fondo allo stack. (Microsoft Research Rif. [B004])*

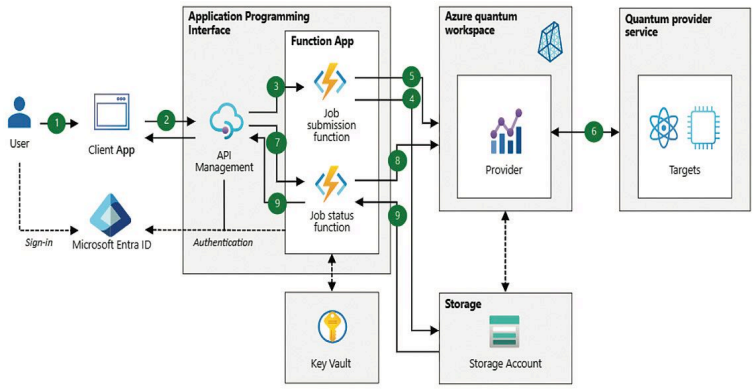


Fig. 4 *- Fonte Microsoft Azure [B005]*

Flussi di dati

Nella Fig. 4 forniamo un esempio di flussi fondamentali numerati da 1 a 9 riferiti a una architettura ibrida Microsoft Azure che si sviluppa in tre fasi:

Fase 1 computazione classica iniziale

1. Un utente connesso attiva l'esecuzione del processo quantistico tramite un'applicazione classica.

2. L'applicazione classica API (Application Program Interface) del processo personalizzata per inviare le richieste.

3. Il gateway API attiva la funzione di Azure per l'invio del processo il quale fornisce i dati di input.

4. La funzione inserisce i dati di input in Archiviazione.

5. La funzione invia il processo a un'area di lavoro specificando la destinazione o le destinazioni di esecuzione. La funzione identifica l'area di lavoro tramite credenziali nel modulo Key Vault ed esegue l'autenticazione nell'area di lavoro tramite strumenti di Identity Management.

Fase 2 computazione quantistica

6. Un provider quantistico esegue il processo in un ambiente di destinazione.

Fase 3 computazione classica finale

7. L'applicazione client monitorizza l'esecuzione del processo eseguendo il polling dello stato del processo tramite chiamate API.

8. Il gateway API monitorizza l'esecuzione del processo eseguendo il polling dello stato del processo dal provider quantistico.

9. Al termine del processo, i risultati di calcolo vengono archiviati nel data store. L'applicazione client ottiene i risultati usando un'API implementata sempre tramite una funzione specifica.

In realtà, numerose organizzazioni stanno lavorando su vari aspetti relativi alla necessità di connettere i computer quantistici con il mondo esterno. Di seguito sono riportati alcuni esempi di tali sforzi.

Il laboratorio Microsoft Quantum dell'Università di Sydney ha sviluppato un hardware che consente ai computer quantistici di connettersi con il mondo esterno mantenendo la stabilità dei qubit. Chiamato "Gooseberry", questo circuito CMOS specializzato include le funzioni digitali e analogiche necessarie per utilizzare ingressi digitali e generare molti segnali di controllo qubit paralleli. Gooseberry può scalare per supportare migliaia di qubit nelle future generazioni di computer quantistici. Funziona a 100 milliKelvin (mK) dissipando una potenza sufficientemente bassa da non superare la potenza di raffreddamento di un normale frigorifero disponibile sul mercato. Il laboratorio Microsoft Quantum ha anche sviluppato un core crio-calcolatore per scopi generali non specificati che funziona a temperature leggermente più elevate ottenibili nell'elio liquido. Gooseberry traduce queste istruzioni in impulsi di tensione per controllare i qubit. La combinazione del core crio-to-compute con Gooseberry è una soluzione al problema della creazione delle migliaia di I/O necessari per controllare migliaia di qubit.

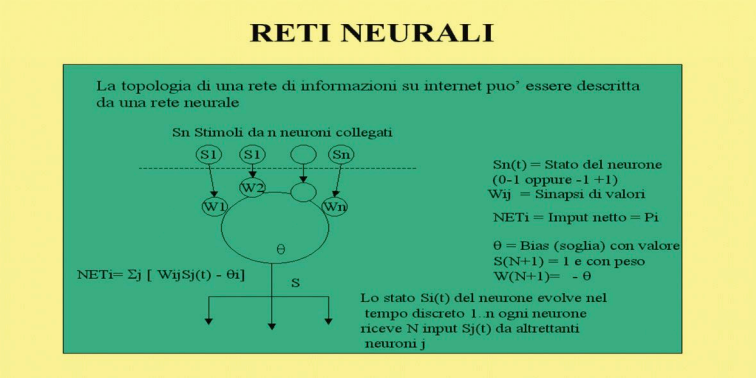
Il cosiddetto "collo di bottiglia del cablaggio di interconnessione" dell'informatica quantistica affrontato dal chip Gooseberry è al centro degli sforzi di Intel con un suo nuovo chip risolutivo chiamato Horse Ridge. Questo è invece un chip di controllo criogenico per qubit costruito utilizzando la tecnologia FinFET Low Power a 22 nm sempre di Intel. Horse Ridge porta le funzioni di controllo chiave per il funzionamento dei computer quantistici nel cosiddetto frigorifero criogenico. Un criocontroller basato su CMOS come Horse Ridge può ottenere il controllo coerente di un processore a due qubit agli stessi livelli di fedeltà (99,7%) dell'elettronica a temperatura ambiente. Questa è considerata una pietra miliare significativa in termini di elettronica di criocontrollo per l'informatica quantistica. Ciò fornirebbe un percorso commerciale a stretto giro verso la scalabilità quantistica.

QUANTUM MACHINE LEARNING. L'apprendimento automatico può essere suddiviso in due gruppi principali: apprendimento supervisionato (addestramento dei dati per prevedere il valore successivo), e non supervisionato (che agisce su dati generici non etichettati). Le macchine a vettori di supporto (SVM) rientrano nella categoria dell'apprendimento supervisionato. Gli algoritmi di apprendimento supervisionato imparano da un set di esempi. Nell'apprendimento supervisionato, esistono variabili di input (X) e una variabile di output (Y). Lo scopo dell'algoritmo è apprendere come la funzione viene mappata dall'input all'output.

Y = f(X)

L'obiettivo dell'algoritmo è l'approssimazione della funzione di mappatura tale da consentire quando si hanno nuovi dati di input (X), di prevedere le variabili di output (Y) per tali dati. Ad esempio, l'algoritmo di apprendimento supervisionato può utilizzare un set di dati addestrato per comprendere la differenza tra due tipi di animali (es. cani e gatti). L'algoritmo analizza le diverse caratteristiche (capelli, colore, occhi, orecchie, ecc.) per scoprire come appare ogni animale. Quindi viene introdotto un punto dati sconosciuto (un cane bianco). Utilizzando l'addestramento precedente, l'algoritmo prevederà in quale categoria potrà rientrare l'animale. Gli SVM sono tra gli algoritmi di apprendimento supervisionato più potenti. Per quelli non supervisionati con finalità di classificazione di oggetti in uno spazio n-dimensionale è possibile utilizzare le cosiddette Reti Neurale Multistrato di Kohonen.

Una Rete Neurale Artificiale (ANN) utilizza lo schema di funzionamento del cervello umano composto da neuroni collegati tramite sinapsi che ricevono stimoli elettrici, essa è dunque composta essenzialmente da un numero variabile di strati (layers) ben descrivibile tramite applicazioni quantistiche. Il primo e l'ultimo di questi strati, essendo predisposti allo scambio d'informazione con l'esterno, sono composti da un numero di neuroni pari alle dimensioni dell'input e dell'output, mentre gli strati interni o nascosti possono avere un numero di neuroni variabile, così come sarà potrà essere variabile il numero degli strati stessi.



L'informazione all'interno della rete è rappresentata da pesi numerici associati ai collegamenti tra i neuroni eccitati di due strati successivi. Nelle reti definite dal finlandese Teuco Kohonen, chiamate reti di Kohonen, i segnali di neuroni tra loro spazialmente vicini sono topologicamente e semanticamente simili; la relazione tra due segnali in ingresso è tanto più forte quanto più vicini sono i neuroni che si eccitano al loro ingresso. Durante l'apprendimento della rete, infatti, nello strato attivo si formeranno delle zone di neuroni che si specializzeranno nel riconoscimento delle caratteristiche topologiche dell'informazione presentata in ingresso. In genere in una rete di Kohonen sono sempre presenti due strati uno di ingresso e uno di uscita. Spesso i neuroni sono disposti in una griglia bidimensionale, altre volte in modo da formare un array monodimensionale (un vettore riga o colonna).

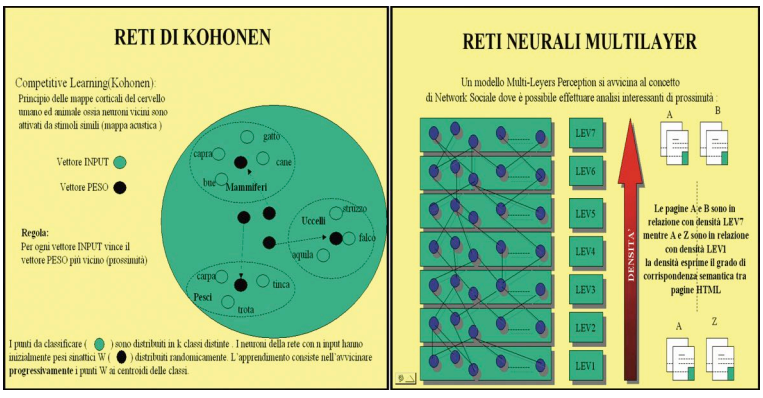


Fig.5 *- Schema di Rete Neurale Multistrato di Kohonen per l'analisi dei reticoli sociali [B008]*

Dopo queste osservazioni sulle reti neurali evidenziamo nella seguente figura uno schema di integrazione tra Machine Learning Classica (CML) e Machine Learning Quantistica (QML) con l'evidenza di metodi di processazione classica dei dati (CD) a tre bits (n) trasformabili in 3qbits corrispondenti a 2^n=8 dati quantistici (QD) che a loro volta si ritrasformano in dati classici (CD) dopo l'elaborazione.

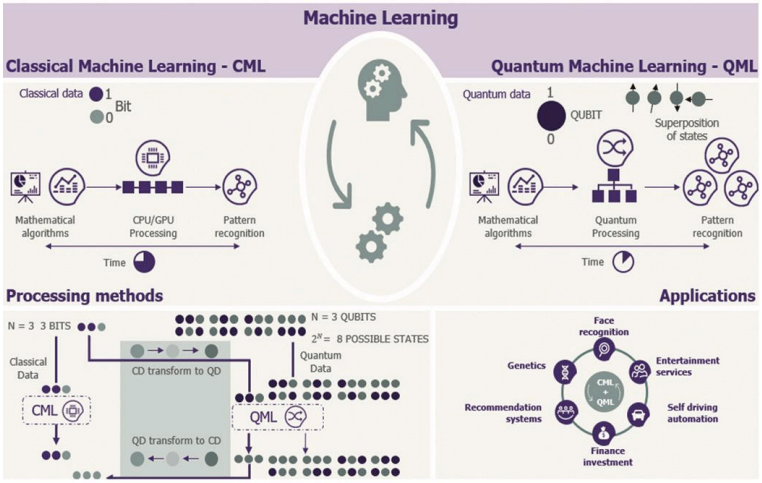


Fig. 6 *– Interazione tra una Machine Learning Classica (CML) e una Quantistica (QML)*

Quando i dati vengono proiettati in dimensioni sempre più elevate di complessità di calcolo, è difficile per i computer classici gestire calcoli così elevati. In altri termini gli algoritmi classici di apprendimento automatico sono troppo faticosi per i computer tradizionali. Fortunatamente, i computer quantistici hanno la potenza computazionale per gestire questi gravosi algoritmi. Come dicevamo, utilizzano leggi come la sovrapposizione e l'entanglement per risolvere i problemi più velocemente delle loro controparti classiche. L'apprendimento automatico quantistico consente agli scienziati di trasformare un algoritmo CML in un circuito quantistico QML in modo che possa essere eseguito efficientemente su una QPU per poi riportare nuovamente i risultati in domini classici. L'apprendimento quantistico è un campo estremamente nuovo e potremmo già prevedere l'impatto rivoluzionario che avrà sul nostro futuro. Ecco alcune delle aree di applicazione delle Quantum Machine Learning:

- Comprendere le nanoparticelle
- Creazione di nuovi materiali attraverso mappe molecolari e atomiche
- Modellazione molecolare per la scoperta di nuovi farmaci e ricerca medica
- Comprensione della struttura profonda del corpo umano
- Riconoscimento e classificazione di qualunque scenario di analisi
- Esplorazione dello spazio interstellare
- Risoluzione di problemi complessi di cifratura e sicurezza dello spazio cibernetico inclusa la cifratura omomorfica.

Con sviluppi sempre più sorprendenti di tipo CML + QML integrati e ibridati avremo pertanto la risposta vincente a tutti i problemi complessi nello spazio delle soluzioni, siano esse polinomiali(P) siano esse non polinomiali (NP). Una raccomandazione è tuttavia d'uopo. Questo tipo di strumenti dovrà sempre essere utilizzato in modalità etica per il bene e il progresso dell'umanità verso sempre più sfidanti orizzonti della conoscenza umana. ■

Bibliografia utile

[B000] https://www.cybertrends.it/dalla-processazione-parallela-al-computer-quantistico/

[B001] 1: Examples of quantum computing architectures. (a) 53-qubits... | Download Scientific Diagram (researchgate.net)

[B002] CMOS-based cryogenic control of silicon quantum circuits | Nature

[B003] Che cos'è un computer quantistico? • HelpMeTech

[B004] Merging quantum and classical computing in a hybrid system (microcontrollertips.com)

[B005]https://learn.microsoft.com/it-it/azure/architecture/example-scenario/quantum/quantum-computing-integration-with-classical-apps

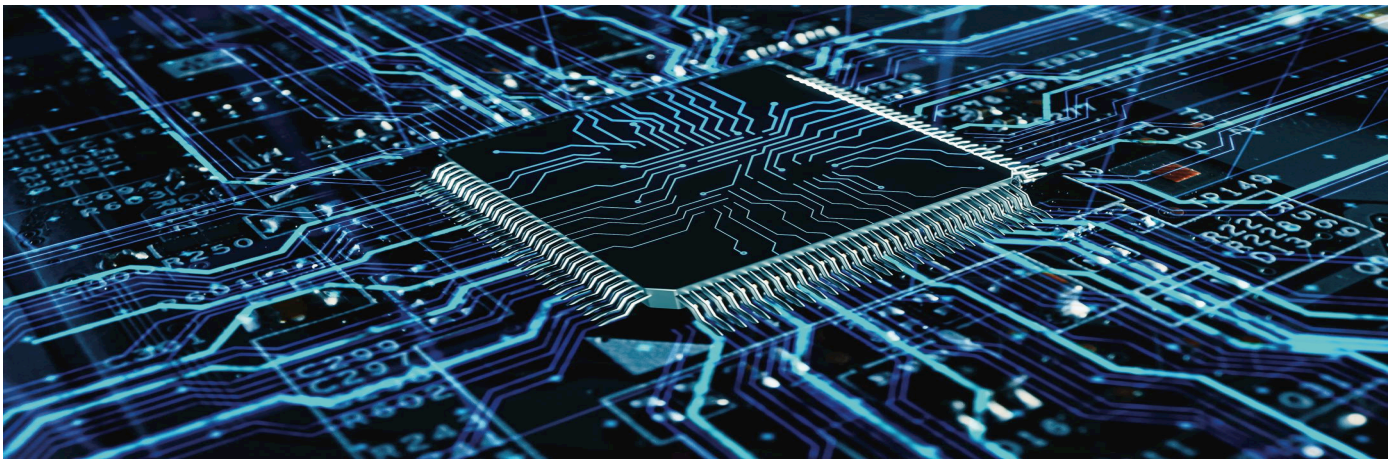
[B006] Paradosso di Einstein-Podolsky-Rosen - Wikipedia

[B007] Quantum Machine Learning Is The Next Big Thing. (thequantuminsider.com)

[B008] F. Corona - Web Intelligence. Manuale di Sicurezza ed Intelligence, Master MAIS Link Campus University, Roma 2006.

[B009] Algoritmo di Shor Wikipedia.

[B010] La sinapsi: il social network più sofisticato per le nostre cellule nervose - Medicalfacts



Rischi di security e privacy legati alla Generative AI.

Autore: Corradino Corradi

L'Intelligenza Artificiale Generativa (Generative AI) è una tecnologia in rapida evoluzione che presenta molte opportunità, ma anche alcuni rischi. Il suo grande successo è iniziato con il lancio di ChatGPT nel dicembre 2022 da parte di OpenAI.

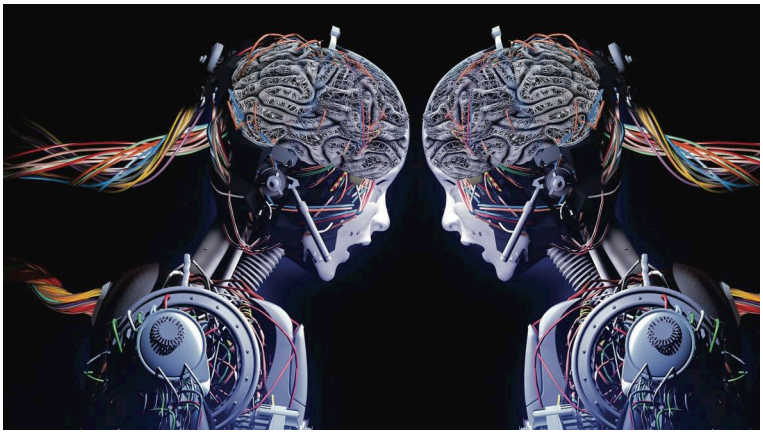
BIO

Corradino Corradi è responsabile della funzione ICT Security & Fraud Management di Vodafone Italia e all'interno del Gruppo Vodafone nel mondo ricopre il ruolo di Senior Member del Corporate Security Leadership Team. L'Ing. Corradi ha 10 anni di esperienza nel campo della security e della gestione delle frodi, della sicurezza dei pagamenti e della protezione delle infrastrutture critiche; è responsabile dell'implementazione delle strategie di sicurezza proattive e reattive, del coordinamento delle operazioni antifrode, nonché del coordinamento di grandi team di professionisti della sicurezza. Corradino Corradi è anche responsabile della gestione dei piani di Business Continuity e Crisis Management di Vodafone Italia. Ha inoltre esperienza nei settori di Risk Management, Compliance, Privacy e Data Protection, Awareness & Training di Frodi e Security, Security Operations Center e CERT, Security Audit e Certificazioni (ISO 27001, SOX, BS25999). In precedenza ha maturato più di 5 anni di esperienza come IT & Security Manager per i principali operatori italiani di telecomunicazioni e banche internazionali.

In questo articolo sono descritti soltanto i rischi e non le numerose opportunità di Generative AI con un focus particolare sulle minacce che DPO e CISO devono considerare prima di adottare Generative AI all'interno delle loro aziende

Tra i rischi principali della Generative AI ci sono **l'inaccuratezza e le allucinazioni, la possibile violazione di privacy e la confidenzialità delle informazioni, la possibile violazione del copyright e della proprietà intellettuale, i bias** (particolarmente allarmanti quelli relativi a genere ed etnia) e **la tossicità**.

L'inaccuratezza e le allucinazioni possono verificarsi quando i modelli di Generative AI generano contenuti che non sono accurati o che non hanno senso. Questo può essere dovuto a errori nei dati di addestramento o a limitazioni nei modelli stessi. Per ridurre questo rischio, è importante utilizzare dati di addestramento di alta qualità e verificare attentamente i risultati generati dai modelli.



Un esempio di inacurattezza di Generative AI si può verificare quando si utilizza un modello di generazione di testo per scrivere un articolo su un argomento specifico. Se il modello non ha abbastanza dati di addestramento sull'argomento o se non è in grado di capire il contesto e il pubblico, potrebbe

generare testi che contengono informazioni errate, irrilevanti o incoerenti. Per esempio, se si chiede al modello di scrivere un articolo sulla storia dell'Italia, potrebbe generare testi come:

- L'Italia è una repubblica democratica fondata nel 1946, dopo la caduta dell'Impero Romano. Il suo capo di stato è il presidente della repubblica, eletto ogni sette anni dal parlamento.

- L'Italia è una nazione ricca di arte e cultura, famosa per i suoi monumenti come il Colosseo, la Torre di Pisa e il Duomo di Milano. Tra i suoi artisti più noti ci sono Leonardo da Vinci, Michelangelo e Dante Alighieri, autore della Divina Commedia.

- L'Italia è uno dei paesi più belli del mondo, con un clima mite e una varietà di paesaggi. Si estende dalla catena montuosa delle Alpi al nord, alla penisola e alle isole del sud, bagnate dal Mar Mediterraneo.

Questi testi contengono sia inacurattezze che allucinazioni. Il primo testo confonde la fondazione della repubblica italiana con la fine dell'Impero Romano, che avvenne secoli prima. Il secondo testo elenca alcuni monumenti e artisti famosi, ma ignora molti altri aspetti della storia e della cultura italiana. Il terzo testo descrive l'Italia in modo generico e superficiale, senza entrare nei dettagli o nei fatti interessanti.

Per evitare questo tipo di inacurattezza, è necessario utilizzare modelli di Generative AI che siano addestrati su dati sufficienti e pertinenti sull'argomento, e che siano in grado di generare testi coerenti e informativi. Inoltre, è necessario revisionare e correggere i testi generati dai modelli, per verificare la loro accuratezza e qualità.

(source MS Co-pilot)

La privacy e la confidenzialità delle informazioni possono essere a rischio quando i dati sensibili vengono utilizzati per addestrare i modelli di Generative AI o quando i risultati generati dai modelli contengono informazioni sensibili. Per ridurre questo rischio, è importante seguire le migliori pratiche per la gestione dei dati e utilizzare tecniche di protezione dei dati come la crittografia e l'anonimizzazione.

Un esempio di violazione della privacy e della confidenzialità delle informazioni da parte di Generative AI potrebbe essere il seguente:

Un modello di Generative AI è stato utilizzato per generare una recensione di un ristorante a partire dal nome del ristorante e dalla data della visita. Il modello ha generato il seguente testo:

"Mi sono recato al ristorante La Pergola il 15 giugno con la mia famiglia e siamo rimasti molto soddisfatti. Il cibo era delizioso, il servizio impeccabile e l'ambiente accogliente. Abbiamo ordinato una varietà di piatti, tra cui la pasta alla carbonara, il pollo al forno, la pizza margherita e il tiramisù. Tutto era fresco e ben cucinato. Il conto è stato ragionevole, considerando la qualità e la quantità del cibo. Lo consiglio vivamente a chi cerca una buona cucina italiana in un'atmosfera rilassata."

Tuttavia, il modello ha violato la privacy e la confidenzialità delle informazioni sia del cliente che del ristorante. Il modello ha infatti utilizzato i dati personali del cliente, come il suo nome, il suo indirizzo email e il numero di telefono, che erano presenti nei dati di addestramento, per generare la recensione. In questo modo, il modello ha rivelato l'identità e le preferenze del cliente senza il suo consenso. Inoltre, il modello ha violato la confidenzialità delle informazioni del ristorante, in quanto ha generato una recensione falsa che non rifletteva la reale esperienza del cliente. Questo potrebbe danneggiare la reputazione e il business del ristorante.

Per evitare questo tipo di violazione, sarebbe necessario adottare delle misure preventive, come:

- Anonimizzare i dati personali dei clienti prima di utilizzarli per addestrare il modello, sostituendoli con dei segnaposto o delle etichette generiche.

- Verificare la veridicità delle recensioni generate dal modello, confrontandole con le fonti originali o con le testimonianze dei clienti reali.

- Informare i clienti e i ristoranti dell'uso di un modello di Generative AI per generare le recensioni e richiedere il loro consenso esplicito.

(source MS Co-pilot)

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il Garante per la protezione dei dati personali italiano ha emanato nella primavera del 2023 dei provvedimenti e delle prescrizioni specifiche per l'uso dei modelli di Generative AI (con particolare riferimento a Chat GTP). Tre le prescrizioni più significative ricordo:

- Richiedere il consenso informato e revocabile degli utenti prima di raccogliere e usare i loro dati personali per alimentare il modello di Generative AI.

- Informare gli utenti della finalità, delle modalità e dei destinatari dei dati raccolti e generati dal modello di Generative AI, nonché dei loro diritti in materia di accesso, rettifica, cancellazione, limitazione, opposizione e portabilità dei dati.

- Adottare misure tecniche e organizzative per garantire la sicurezza, la qualità e la trasparenza dei dati trattati dal modello di Generative AI, nonché per prevenire e segnalare eventuali violazioni dei dati.

- Limitare il tempo di conservazione dei dati al minimo necessario per la realizzazione della finalità del modello

di Generative AI e cancellare i dati una volta raggiunta tale finalità o in caso di revoca del consenso da parte degli utenti.

- Apporre un segno distintivo (ad esempio, un'icona o una sigla) alle chat generate dal modello di Generative AI, per evidenziarne la natura artificiale e distinguerle dalle chat reali.

Nel corso del 2023 altri garanti privacy hanno adottato provvedimenti o messo linee guida su Generative AI, sulla scia di quanto fatto dal Garante Privacy italiano.

Il copyright e la proprietà intellettuale possono essere a rischio quando i modelli di Generative AI generano contenuti che violano i diritti di proprietà intellettuale di terzi. Per ridurre questo rischio, è importante comprendere le leggi sulla proprietà intellettuale (che variano di nazione in nazione) e utilizzare solo dati di addestramento che non violino i diritti di terzi.

Un esempio di violazione del copyright e della proprietà intellettuale da parte di un modello di Generative AI potrebbe essere il seguente:

- Utilizzare un modello di Generative AI per generare delle poesie basandosi sui testi di famosi poeti italiani, senza citarne la fonte o attribuire il merito ai veri autori.

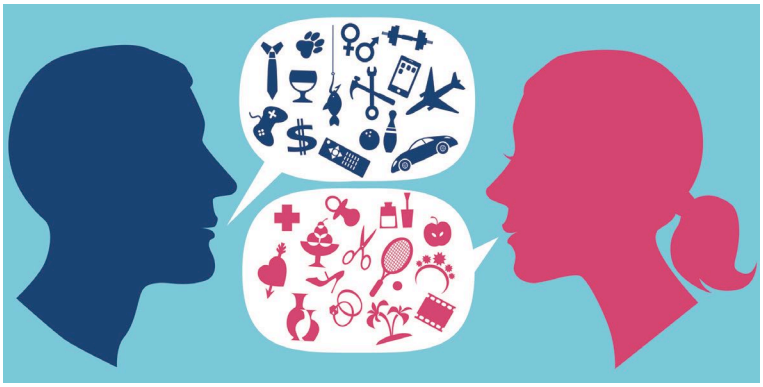
- Pubblicare le poesie generate come proprie opere originali su un sito web o una rivista letteraria, ottenendo profitti o riconoscimenti ingiusti.

- Ricevere una denuncia legale da parte dei detentori dei diritti delle opere originali, che accusano il generatore di plagio e di violazione del diritto d'autore.

(source MS Co-pilot)

Infine, bisogna aggiungere tra i rischi i **bias e la tossicità** che possono verificarsi quando i modelli di Generative AI generano contenuti che sono discriminatori o offensivi. Questo può essere dovuto a bias nei dati di addestramento o a limitazioni nei modelli stessi. Per ridurre questo rischio, è importante utilizzare dati di addestramento che rappresentino in modo equo tutte le parti interessate e verificare attentamente i risultati generati dai modelli per evitare contenuti discriminatori o offensivi.

Un esempio di bias e tossicità che può generare un modello di Generative AI è quello di produrre testi che usano termini sessisti, razzisti o omofobi per descrivere persone o gruppi. Questo può creare danni alla reputazione, offendere i destinatari dei testi e alimentare l'odio e la discriminazione nella società. Un modo per prevenire questo tipo di problema è quello di utilizzare strumenti di rilevazione della tossicità per filtrare i testi generati e correggere o eliminare quelli che contengono parole o espressioni inaccettabili. Inoltre, è utile educare



gli utenti sui rischi e le responsabilità dell'uso dei modelli di Generative AI e incoraggiare un uso etico e consapevole degli stessi.

(source MS Co-pilot)

Cosa aspettarsi per il futuro? Di sicuro ci sono alcuni trends di Generative AI già in atto che andranno a rafforzarsi:

- Maggiore concorrenza, in particolare nei modelli linguistici.
- Miglioramento della precisione e affinamento degli strumenti di autocontrollo (definiti in molti regolamenti di AI "guardrail").
- L'integrazione di AI in altri tools (per esempio le funzionalità di Copilot di Microsoft integrate nella suite Office oppure il miglioramento dei motori di ricerca Google e Bing "powered by" AI).
- Sul lungo termine, Intelligenza Generale Artificiale (AGI) indistinguibile dalle capacità umane (si pensi alle nuove capacità di GPT-5 e Google Bard).

Concludo con il ricordare che la tecnologia Generative AI è in rapidissima evoluzione e numerose sono le startup che stanno lavorando di modelli sempre più evoluti e sofisticati di Large Language Model - LLM (alla base di Generative AI; la lista dei rischi riportati nell'articolo non è quindi esaustiva e DPO/CISP devono adottare un mind-set di "continous learning" al fine di restare al passo con l'evoluzione tecnologia ed essere in grandi di realizzare una "risk analysis" in grado di soppesare con equilibrio rischi e opportunità introdotte da Generative AI. ■

Attacco informatico al Parlamento rumeno: un'analisi a freddo nel contesto globale.

Autore: Laurent Chrzanovski

Attacchi informatici rivolti agli organi legislativi, abbastanza "leggeri" fino a qualche anno fa.

Complessivamente gli attacchi informatici che negli ultimi anni hanno colpito gli organi legislativi di molti Stati sono stati una mera routine e in qualche modo innocui. Nella maggior parte dei casi si è trattato di *"defacement"* dell'home page di un sito web (cioè la modifica illecita della pagina iniziale espressione di una rivendicazione, di solito politica) unito solitamente a un attacco DDoS *(Denial of Service)*, che impediva a qualsiasi utente di accedere al sito fino a quando il problema non fosse stato risolto dai team di sicurezza.

Oggi a livello globale attacchi di "vecchio" tipo contro istituzioni statali sono ormai condotti quasi quotidianamente da gruppi di hacker affiliati a uno Stato o semplicemente spinti da una causa (terrorismo, ambientalismo, alter-globalismo, ecc.). Possiamo citare, ad esempio, l'attacco al sito web dell'Amministrazione federale svizzera durante la visita del presidente ucraino Volodymir Zelensky a Davos il 18 gennaio; oppure il potente attacco DDoS, che il 2 febbraio ha colpito il sito web della Direzione nazionale della sicurezza informatica rumena (DNSC), sferrato solo tre giorni dopo l'attacco alla Camera dei deputati, avvenuto il 30 gennaio.

In ogni caso, il dato da sottolineare è che queste operazioni non influivano sull'effettivo contenuto dei server, ma causavano disagio agli utenti e davano qualche grattacapo ai team di sicurezza.

Gli obiettivi strategici presi di mira dai gruppi criminali più esperti

Il motivo principale della "debolezza" degli attacchi contro gli organi legislativi è che la maggior parte degli attacchi più sofisticati che hanno come oggetto il furto di dati si sono concentrati su obiettivi e documenti con un livello di segretezza più alto più di quello a cui potrebbero accedere un parlamento o un senato. Per i più potenti gruppi hacker, la ricchezza di uno Stato consiste nei suoi dati altamente sensibili, sia quelli delle agenzie governative legate alla sicurezza nazionale, sia quelli dei settori chiave come la sanità o le infrastrutture critiche.

Questi obiettivi, costantemente sotto attacco sin dall'inizio della pandemia del Covid, se oggetto di violazione vedono il valore dei loro dati aumentare enormemente. Questo perché i dati possono non solo essere utilizzati da Stati avversari, ma possono essere anche venduti ad attori privati che operano in questi settori per ricavarne un enorme profitto.

Perché ora, e perché i parlamenti?

La risposta è complessa e racchiude molteplici cause: il deterioramento delle principali economie mondiali, causato da anni di pandemia, da un'instabilità geopolitica e militare mai vista dalla fine della Guerra Fredda, fattori ai quali si aggiungono l'inflazione, la speculazione e, di conseguenza, l'enorme necessità per i principali attori statali e privati di anticipare le decisioni prese dai loro concorrenti, e le loro ripercussioni nel quadro di una spietata competizione globale in cui non esistono né amici né alleati.

In tutti i Paesi dell'UE e dei Paesi membri del G20 e oltre, entrambe le Camere venivano in precedenza spiate attraverso la registrazione vocale utilizzando microfoni o spyware installati negli smartphone; come si è visto nel caso NSA e in quello, più recente, della Commissione e del Parlamento dell'UE. Da poco gli organi legislativi sono diventati un obiettivo primario dei gruppi hacker più noti. Senati e parlamenti trattano un'enorme quantità di dati: anche se la maggior parte di essi non sono nello specifico dati sensibili, ma alcuni di essi sono altamente rilevanti per i quattro grandi pilastri dell'economia, come gli argomenti trattati dalle commissioni specializzate che si occupano di settori strategici.

In questo contesto, i server delle Camere detengono alcuni "tesori" che possono essere utilizzati dagli Stati avversari o venduti illegalmente al settore privato. L'attacco, purtroppo riuscito, al centro dati del Parlamento rumeno – furto di 250 gigabyte e ransomware – è quindi l'ultimo di una lunga serie di attacchi iniziata ormai da tre anni.

Tenendo conto solo degli attacchi più rilevanti accaduti negli ultimi sei mesi, meritano di essere menzionati alcuni casi. Nel settembre 2023, il Parlamento canadese ha subito un potente attacco che ha portato al furto di molti dati; il mese successivo è stata la volta di entrambe le camere delle Filippine ad essere oggetto di un hacking massiccio, seguite da quelle del Belgio. Lo stesso giorno dell'attacco al Parlamento rumeno, uno dei principali data center privati utilizzati dal Parlamento svedese (parte del cloud pubblico nazionale) è stato completamente compromesso.

Senza raggiungere la portata critica degli eventi dello scorso anno ai danni del Pentagono o del governo

svizzero - in quest'ultimo caso il centro dati, gestito da aziende militari statali, è stato oggetto di un attacco ransomware con la minaccia di rendere pubblici tutti i documenti - due degli attacchi ai Parlamenti sopra citati meritano particolare attenzione.

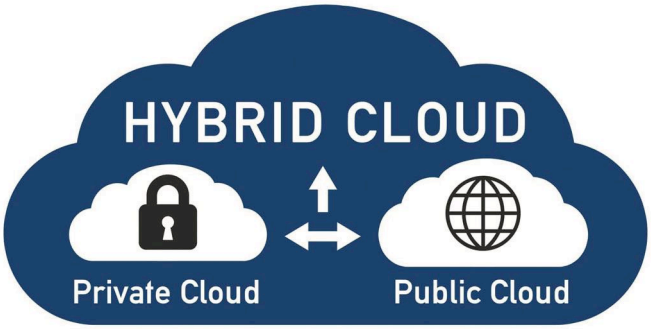
Da un lato, l'evento canadese ha impattato profondamente anche i dati del Ministero della Difesa, mentre l'incidente belga ha comportato il furto dati dell'ufficio del Primo Ministro, dell'ufficio del Re e di diversi altri ministeri. In realtà, entrambi questi attacchi altamente sofisticati hanno sfruttato l'organizzazione informatica di istituzioni diverse per avere un tale successo, il ché ci porta a presupporre che le Camere non fossero il loro obiettivo principale.

Lezioni da imparare

Abbiamo letto con interesse gli articoli pubblicati sui vari giornali nazionali ed esteri sul caso del Parlamento rumeno. Purtroppo, da anni sentiamo dire che la sicurezza informatica deve essere la "priorità zero" per tutti i governi e tutti gli enti statali, le stesse dichiarazioni senza seguito che vengono rilasciate dopo ogni incidente.

In questo contesto, le sfide sono enormi. Per primo la necessità di ogni Stato di reclutare un maggior numero di specialisti di sicurezza informatica, una sfida difficilmente compatibile con l'attuale periodo di recessione e di bilanci in crisi.

È poi necessario chiarire in quale modo una nazione voglia sviluppare il proprio "cloud governativo" o "cloud pubblico", questi non offrono maggiore sicurezza rispetto ai server statici a meno che non siano creati *ad hoc* con sistemi all'avanguardia.



Peggio ancora, il sistema "cloud-based" necessita molte connessioni remote sicure e una supply chain dei dati in transito quasi blindata. Ora, come abbiamo visto negli Stati Uniti (caso Solarwinds) e in Svizzera (cloud creato e gestito da aziende militari statali), anche le migliori supply chain possono essere violate.

Inoltre, alla fine dietro un servizio cloud c'è sempre un sistema di server fisici. Nel consueto scenario anglosassone del "cloud pubblico", garantito dalle più alte organizzazioni statali, ma anche in quella più ristretta del "cloud governativo", l'attacco informatico svedese del 29 gennaio rappresenta il peggior incubo possibile. Infatti, uno dei database utilizzati, appartenente alla società più affidabile della Finlandia, non è ancora funzionale e la perdita di documenti, tutt'ora in corso di quantificazione, riguarda, oltre ai documenti di Stato, i dati di importanti istituzioni bancarie e commerciali.

Infine, ma non meno importante, è fondamentale scegliere le migliori tecnologie e i migliori specialisti. A questo proposito, vanno sottolineati due elementi. Il primo è che tutte le tecnologie più sicure, che includono la crittografia quantistica e l'intelligenza artificiale, non sono in mano ad aziende europee; quindi, anche se queste aziende globali (con sedi negli Stati Uniti e Cina, principalmente) possono costruire le componenti fisiche sul territorio dell'UE, si creerà comunque una dipendenza extra-UE che potrebbe non essere compatibile con le norme del GDPR.

Se andiamo oltre, già da un punto di vista tecnologico, la domanda *"quis custodet custodes?"*, cioè chi custodisce i (dati), la Romania come molti altri Stati dell'UE, dovrà scegliere tra affrontare la "tradizionale" sfiducia comune nei confronti delle proprie agenzie di sicurezza statali (servizi di intelligence) e la rischiosa strada della privatizzazione della sicurezza, dell'hosting e del corretto funzionamento del cloud governativo. Questo è un rischio che solo gli Stati Uniti, la Cina la Russia o Israele possono permettersi, avendo tali aziende leader mondiali nella loro giurisdizione nazionale, con tanto di interpenetrazioni colle agenzie di intelligence dei loro stati.

Questi attacchi continueranno ... con l'intelligenza artificiale non si perde nulla...

Purtroppo, tali attacchi continueranno perché oltre ai dati critici/ultrasensibili che, se trovati, saranno immediatamente commercializzati, non bisogna sottovalutare le "big tech" dell'intelligenza artificiale - così come i gruppi di criminali informatici che posseggono questa tecnologia - e i miliardi di dati di cui hanno bisogno ogni giorno per migliorarne il funzionamento.

In assenza di un quadro legale ed etico, e pur senza esserne direttamente responsabile, l'intelligenza artificiale ha trasformato in bersaglio della criminalità informatica ogni entità pubblica o privata che possiede un massiccio centro di elaborazione dati, indipendentemente dalla loro sensibilità/riservatezza. L'IA ha bisogno di peta- ed exa- bit quotidiani estratti da tutte le fonti globali possibili, legali o meno, da prendere sul web o da acquisire.

BIO

Dottore di ricerca in Archeologia romana dell'Università di Losanna, Laurent ha poi ottenuto un diploma post-dottorale in Storia e Sociologia presso l'Accademia delle Scienze della Romania, l'abilitazione UE a dirigere Dottorati di ricerca nel campi della Storia e delle scienze affini. Oggi, Laurent è professore presso la Scuola dottorale e postdottorale dell'Universita' Statale di Sibiu. Tiene regolarmente corsi post-dottorato in Università di prestigio in diversi paesi dell'UE, in primis a Varsavia. E' autore/redattore di 31 libri, di oltre un centinaio di articoli scientifici e di altrettanti articoli destinati al grande pubblico.
Nel campo della cybersecurity, Laurent è membro e consulente contrattuale del gruppo di esperti dell'ITU. Ha fondato e gestisce ogni anno il trittico di congressi PPP "Cybersecurity Dialogues" (Romania, Svizzera, Italia) organizzati in collaborazione con un grande numero di istituzioni specializzate, internazionali e nazionali. Nello stesso spirito e con lo stesso spirito e con i stessi partner, è fondatore e redattore capo e redattore capo di Cybersecurity Trends, la prima rivista trimestrale di sensibilizzazione alla sicurezza informatica per adulti, pubblicata in quattro varianti adattate ad altrettanti ecosistemi lingusitsici e culturali. Il suo campo di studio è focalizzato sulla relazione tra i comportamenti umani nel mondo digitale e il bisogno di trovare il giusto equilibrio tra la sicurezza e la privacy per l'utente finale, cioè "l'e-cittadino" che siamo tutti diventati.

In conseguenza, nulla è perduto per gli hacker, poiché i documenti rubati più importanti saranno immediatamente utilizzati (se l'attacco è stato pagato da un'entità) o venduti a caro prezzo, mentre il resto dei dati verrà inglobato con altri dati, costituendo così "pacchetti" che diventino interessanti, in termini di volume, per i grandi attori (legali o criminali) del campo dell'intelligenza artificiale. ■

Associati, facciamo un lavoro da maratoneti.

Intervista VIP a Yuri Rassega.

Autore: Massimiliano Cannata

"Studiare con continuità, allargare continuamente la visione, rafforzare il dialogo con colleghi e stakeholders, comprendere che non esistono "due culture" contrapposte, sapere umanistico e abilità tecniche che si fanno la guerra. Il CISO del futuro dovrà maturare un profilo sfaccettato per fare tutto questo, praticando sensibilità diverse se vuole ottenere risultati. Innalzare la "resilienza" di sistema è un nostro compito precipuo, nella consapevolezza che possiamo contribuire con il nostro impegno a migliorare le nostre organizzazioni e la società nel suo complesso".

La sicurezza è una sfida in divenire. Possiamo provare a definire il ruolo e la funzione del Ciso?

CISO è l'acronimo che, come è noto, viene utilizzato per identificare chi guida i processi aziendali di gestione del cyber rischio. Si tratta di una figura relativamente giovane, che ha seguito l'evoluzione dell'Information Technology. Se si vuole parlare di ruoli e mansioni non si può prescindere dal contesto attuale, segnato da trasformazioni epocali che stiamo vivendo. L'identità del security manager non può non modificarsi in relazione alla metamorfosi sociale e organizzativa che caratterizza la società tutta. Aree di business, filosofie produttive, il modo di fare e concepire l'impresa sono fattori che incideranno sui nostri compiti e sul ventaglio di responsabilità che ci riguardano. Da una puntuale ridefinizione del CISO, che oggi si impone, le imprese non possono che trarne un diretto beneficio, con ricadute positive sui fattori della competitività.

Il CISO con quali attori della catena del valore deve interloquire nell'orizzonte di una sicurezza che non ha nulla a che vedere con la visione tradizionale della tutela del "recinto" e dello "spazio fisico", ma che oggi si misura con la terza dimensione dell'"infosfera"?

Il cambio di focus richiesto all'intera *value chain* ha imposto una protezione a 360 gradi degli asset. Gli attaccanti hanno ormai come obiettivi la rete, i dispositivi digitali, il "tesoro" di dati e informazioni che corrono sui binari virtuali. Per fare bene il nostro lavoro non possiamo certo "limitarci" a sventare la minaccia, ma dobbiamo curare in maniera integrata e continua un approccio alla materia della sicurezza, che presenta un habitus fortemente interdisciplinare. Bisogna conoscere e presidiare con accortezza le aree strategiche dell'azienda, per individuare le possibili vulnerabilità, aspetto quest'ultimo decisivo nella dinamica del mercato competitivo. Occorre un dialogo e uno scambio di know-how costante con tutti i soggetti all'interno dell'azienda. In quest'ottica risulta particolarmente prezioso maturare skills di carattere relazionale.

Capacità di valutazione del rischio è una competenza per definizione trasversale. Come va praticata?

Per fare delle scelte precise, che sono il "sale" di quest'attività, bisogna adottare metriche di tipo non puramente ed esclusivamente tecnico. Quello che un CISO mette in atto è un lavoro inizialmente lontanissimo dalle macchine che poi va a proteggere. Vanno presi in esame i diversi "pesi" del rischio, che in limitata percentuale va "accettato" e "controllato". Il nostro mestiere è divenuto più affascinante e nello stesso tempo più problematico,

credo sia un bene perché ci costringe a tenere alta l'attenzione su questioni di frontiera.

Nella "società del rischio", per usare la celebre definizione di Ulrich Beck, la sicurezza è una delle grandi questioni del nostro tempo. Associarsi aiuta a far maturare la giusta consapevolezza della centralità della sicurezza come valore?

Associarsi vuol dire mettere in campo un "tessuto connettivo di intelligenze" e di riflessione condivisa. Esistono nel nostro ambito molte associazioni che in varie forme e modi si preoccupano di seguire i temi della cyber security, che trovano sempre più spazio in molti organi di informazione. Bisogna tenere presente che per portare avanti un ventaglio ampio di competenze non basta la semplice passione che tutti noi che facciamo questo mestiere alimentiamo e nutriamo. Esigenze crescenti di *compliance*, di adeguamento normativo, la progettazione delle attività di *awareness*, l'aggiornamento continuo delle competenze, hanno determinato la nascita di ASSOCISO, che

ASSOCISO
Associazione Nazionale CISO

vuole essere un punto di convergenza, di confronto, teso a sviluppare un sentimento e un metodo di formazione comune.

Come hanno risposto le aziende alla vostra proposta associativa?

Molto buono il livello di risposta non solo delle grandi e medie imprese ma anche delle piccole, cosa per nulla scontata e che perciò va sottolineata. Nel fitto tessuto delle PMI credo sia, infatti, molto importante che si faccia strada una culture security diffusa. Obiettivo non semplice ma certamente necessario per innalzare la "resilienza" di tutto il sistema paese. Associso vuole avere un dialogo ordinato con tutti gli *stakeholder*, per affinare un profilo identitario del manager della security aperto al cambiamento e nel contempo per creare una piattaforma di dialogo dinamica. Tutte le aziende senza distinzione devono oggi occuparsi di cyber security, per farlo devono capire in fretta le area di competenza da sviluppare.

BIO

Presidente di ASSOCISO (www.associso.org), dal giugno 2016 Yuri Rassega è Chief Information Security Officer (CISO) di Enel, uno dei principali operatori mondiali del settore energetico, presente in 30 paesi nel mondo, principalmente producendo e distribuendo elettricità, servendo quasi 75 milioni di clienti. Ha la responsabilità di guidare tutti i processi di Cyber Security Risk Management, Governance, Engineering, Assurance, CERT (CSIRT) e Digital Identity Management del Gruppo. Entrò a far parte del gruppo Enel nel 2001 come responsabile (CIO) della funzione ICT in Enel Hydro SpA e nel tempo ricoprì le funzioni di responsabile del Global ICT Solution Centre AFC, HR and Procurement e Funzioni Holding e Global Audit ICT. Prima lavorare in Enel, Yuri Rassega ha lavorato, assumendo diverse responsabilità, nell'industria ICT, inclusi lo sviluppo di sistemi in ambito bancario, TELCO & ISP, ERP, SCADA, ACS, e soluzioni ICS per vari clienti. È stato co-founder di una start-up company impegnata nello sviluppo di soluzioni SCADA / ACS / ICS per l'automazione di impianti di depurazione acque reflue urbane, automazione acquedotti e sistemi HVAC. Dal 1999 al 2001, Yuri Rassega è stato CIO di una società Telco privata (servizio di telefonia fissa e Internet Service Provider) accompagnandone l'avvio dalla fase di "green-field" a quella di "scale-up". È membro di alcuni "expert working group" anche in ambito istituzionale, nazionale e internazionale, quali UE-sponsored Working Groups, WEF-World Economic Forum (5 publications), CIGRE D2 Committee member dal 2022, numerosi contributi in ambito G7 e G20. È "adjunct professor" in corsi di studio e Master presso diverse Università e Accademie civili e militari. È socio fondatore della "Accademia di Ingegneria e Tecnologia" - Italia. Contribuisce come relatore, come presidente di panel, come Advisory Board Member in numerose conferenze internazionali, in Europa, Nord America, Medio Oriente, Asia, sulle tematiche di sicurezza informatica, digital transformation e comunicazioni wireless, già dai primi anni 2000. È anche inventore avendo sviluppato alcuni strumenti digitali e metodi di rilevazione di frodi brevettati in Europa, Stati Uniti e in alcuni paesi dell'America latina.

Le normative in arrivo, pensiamo alla NIS 2, amplieranno il numero dei soggetti che dovranno occuparsi di sicurezza informatica, disegnando processi molto precisi. Imparare a riutilizzare le *best practices* sarà un vantaggio non da poco. A questo fine stiamo già progettando iniziative, in ambito associativo, per diffondere la cultura della sicurezza, che deve diventare un patrimonio comune.

Cosa si sta facendo per migliorare le collaborazioni internazionali su una materia come la* cyber security, *per definizione senza frontiere?

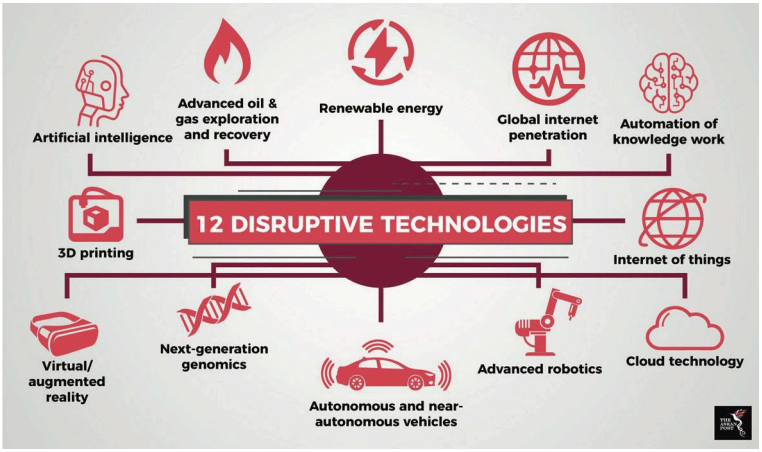
La materia, come Lei giustamente osserva, è per sua natura globalizzata. Si verifica però che mentre le *practices* e gli approcci di risposta sono per molti aspetti vicini, le normative per logica e struttura formale sono molto differenti tra i Paesi. Gli stimoli perché le aziende si attivino su questi temi non mancano, il problema riguarda la difformità legislativa, che è lo specchio di tradizioni e culture giuridiche molto diverse. In Europa, come è noto, ci si muove per direttive, che impongono successive trasposizioni negli ordinamenti nazionali, che spesso divergono. Il caso della NIS 1 e NIS 2 è emblematico, così come quello di una certificazione europea ancora lontano da venire.

Anche sulla velocizzazione della risposta credo si potrà fare molto meglio. Sono comunque ottimista, siamo allenati a navigare nel mare della complessità, il nostro è un lavoro da maratoneti della sicurezza. Bisogna fare le cose col tempo, senza stancarsi mai. Strade omogenee se ne troveranno. Negli ultimi anni è esplosa anche la materia normativa, su una disciplina che era letteralmente sconosciuta. In questo scenario occorre essere prima di tutto presenti e fare sistema, dando corpo a quella intelligenza collettiva sui processi, che il filosofo Pierre Lévy giustamente auspicava, in uno scritto che è rimasto un punto di riferimento della riflessione teorico-pratica sulla contemporaneità. ■

Per gestire la rivoluzione in atto dobbiamo essere consapevoli.

Intervista VIP a Nunzia Ciardi.

Autore: Massimiliano Cannata



"Lo sviluppo e la diffusione dell'IA e dei computer quantistici sta giustamente polarizzando l'attenzione non solo degli addetti ai lavori. Siamo di fronte alle due "disruptive technologies" del momento, che cambieranno profondamente i nostri comportamenti e stili di vita. Sono tecnologie complesse su cui si fonderà la competitività su scala globale, che dobbiamo maneggiare con competenza, sensibilità etica, rispetto della privacy, equità sociale".

Nunzia Ciardi, Vice Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale, già capo della Polizia Postale, offre un interessante spaccato sul futuro prossimo venturo. Nel suo argomentare emerge grande perizia ed equilibrio. La potenza degli strumenti che abbiamo a disposizione, precisa in diversi passaggi, rappresenta una sfida costante sul delicato terreno della sicurezza individuale e collettiva. Una sfida rispetto a cui non possiamo farci trovare impreparati.

Direttore, intelligenza artificiale, computer quantistici, si sta aprendo un nuovo imprevedibile capitolo della rivoluzione digitale?

L'evoluzione tecnologica contraddistingue la nostra epoca. Non sempre è facile cogliere la portata di eventi che appartengono alla nostra quotidianità e, tuttavia, tra un paio di decenni si guarderà in prospettiva alla rapidità esplosiva con la quale queste *"disruptive technologies"* si saranno inserite nelle nostre esistenze, segnando un prima e un dopo.

Oggi siamo tra il prima e il dopo e quindi il nostro ruolo principale è delicato: dobbiamo essere consapevoli della rivoluzione in atto, per gestirla, beneficiando dei progressi e riducendo al mimino i rischi che comporta. L'IA, ad esempio, con la sua portata rivoluzionaria, sta determinando immensi cambiamenti, interessando l'economia, il mercato del lavoro, la società, influendo sui rapporti di forza tra le potenze e modificando equilibri a lungo mantenuti. Anche l'avvento dei computer quantistici, almeno in certi ambiti, è destinato a essere dirompente.

Possiamo spiegare in maniera sintetica cosa sono i computer quantistici e come funzionano?

La tecnologia dei computer quantistici è molto complessa. Parliamo di calcolatori che sfruttano le leggi della meccanica quantistica, quella che studia le particelle subatomiche. Semplificando un bel pò, diciamo che questo abilita calcoli in parallelo come mai prima, moltiplicando esponenzialmente la velocità di calcolo per alcuni tipi di problemi estremamente complessi da compiere con i computer standard.

In che misura queste tecnologie impatteranno sulla* cybersicurezza*?

Bisogna sottolineare come i sistemi di sicurezza avanzati utilizzano già da anni l'IA, avvalendosi della capacità di analisi automatica di enormi quantità di dati in tempo reale, per rilevare, ad esempio, attività sospette o analizzare il comportamento di un malware. Con l'IA generativa, oggi è possibile

fare un ulteriore passo avanti fornendo all'analista di sicurezza una visione completa, chiara e immediata della situazione, suggerendo anche azioni specifiche da intraprendere, potendo con ciò colmare, almeno in parte, anche la carenza di competenze nel mercato del lavoro, non sostituendo i ruoli della sicurezza, ma elevando il loro livello, assolvendoli da compiti ripetitivi. Questo è un paradigma utile per guardare all'applicazione dell'IA in ogni campo: metterla al servizio dell'intelligenza naturale e creare un "Intelligenza Aumentata" dove l'etica e il fine siano appannaggio dell'uomo, assistito dalla rapidità, dalla potenza e dalla precisione di una macchina.

D'altra parte, l'utilizzo malevolo dell'IA da parte di cybercriminali e/o attori parastatali può avere impatti importanti anche per la sicurezza nazionale. Uno degli usi dell'IA è quello orientato all'identificazione e allo sfruttamento rapido della vulnerabilità nelle reti di infrastrutture critiche. In altri casi l'IA può essere determinante nello sviluppo di malware capaci di adattarsi e modificarsi in risposta agli sforzi di difesa, o per sfruttare sistemi di sorveglianza e spionaggio volti a identificare le catene di approvvigionamento più vulnerabili. All'IA possiamo tuttavia contrapporre proprio l'IA: ogni progresso tecnologico di uno dei due fronti si confronta con l'altro che utilizza la stessa tecnologia applicata per difendere i sistemi attaccati, per ingannare, intercettare o superare l'avversario.

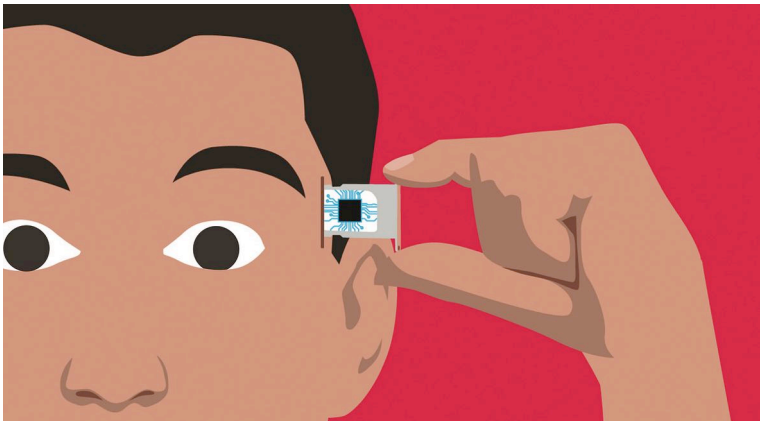
Gli scenari per la governance del rischio

Quali scenari si aprono nella governance del rischio, sulla spinta della prepotente diffusione dell'intelligenza generativa?

Va precisato innanzi tutto un aspetto molto importante: l'apporto dell'IA alla cybersicurezza non deve essere sovrastimato. Dobbiamo, infatti, considerare che gli esperti potrebbero essere soggetti al rischio di "automation bias", riponendo eccessiva fiducia nelle decisioni prese da sistemi automatizzati, presumendole prive di errori, superiori alle decisioni umane e così ignorando o sottostimando eventuali altre vulnerabilità non rilevabili dall'IA. Una corretta "Intelligenza Aumentata" deve considerare questi fattori, specialmente in contesti critici come la cybersicurezza o in altri settori particolarmente sensibili come la medicina, l'aviazione, la finanza e la difesa.

Cyber security *e computer quantistici, possiamo soffermarci anche su questo delicato binomio?*

Per rispondere alla domanda mi soffermerei subito su uno dei problemi nodali: la vulnerabilità – rispetto a questa tecnologia - di certe classi di algoritmi crittografici, algoritmi considerati fino ad ora super sicuri e su cui è di fatto basato l'intero impianto tecnologico esistente. Basti pensare alla crittografia delle blockchain o, più banalmente, al protocollo https che rende sicure le nostre transazioni su internet. A dicembre scorso un



team di ricercatori della Repubblica Popolare Cinese ha affermato di aver sviluppato un attacco all'algoritmo di crittografia asimmetrica RSA, che è usato praticamente ovunque, usando la potenza di calcolo di un computer quantistico attuale. Anche se la comunità scientifica ha dichiarato che questa specifica tipologia di attacco non è ancora realizzabile, ritengo che queste affermazioni non debbano essere sottovalutate.

AGENZIA PER LA CYBERSICUREZZA NAZIONALE

Il ruolo dell'ACN e il posizionamento dell'Europa

L'ACN può avere un ruolo di catalizzatore perché nel paese possa crescere la conoscenza dei "nuovi alfabeti" del digitale?

L'Agenzia per la Cybersicurezza Nazionale sta già operando in tal senso. Rimanendo al tema della nostra conversazione va detto che siamo impegnati nella promozione dell'uso della crittografia come strumento di cybersicurezza capace di assicurare un livello di protezione efficace e duraturo. L'obiettivo, coerente con le misure dalla Strategia Nazionale di Cybersicurezza e con le indicazioni della normativa nazionale ed europea, è quello di favorire l'impiego di crittografia lungo l'intero ciclo di vita dei sistemi e servizi ICT, in conformità ai principi della sicurezza e della tutela della privacy. Per questo motivo dobbiamo essere pronti all'arrivo dei computer quantistici facendo evolvere gli algoritmi di crittografia per renderli resistenti a questa nuova tecnologia adottando algoritmi cosiddetti "Post-Quantum Cryptography" (PQC).

In conclusione, guardiamo all'Europa. Dove si colloca il vecchio Continente in tema di "disruptive technologies"?

Gli enormi vantaggi economici connessi allo sviluppo tecnologico stanno influenzando anche la politica degli Stati, orientati a conseguire vantaggi competitivi in ambito non solo economico ma anche geopolitico e strategico. Si sta abbondantemente discutendo a livello globale circa l'opportunità, la bontà e l'efficacia di regolamentazioni più o meno rigide che disegnino un perimetro di azione per lo sviluppo delle nuove tecnologie. Per l'Europa le strategie digitali occupano una posizione di primo piano e il calcolo quantistico e l'intelligenza artificiale sono tra le tecnologie su cui bisognerà fondare la competitività sullo scenario globale, a condizione però di promuovere uno sviluppo all'insegna dell'etica, della sicurezza, della privacy e dell'equità sociale. ■

BIO

Nunzia Ciardi è stata la prima donna a capo della Polizia Postale italiana, duemila esperti impegnati nel contrasto al cyberterrorismo, al financial cybercrime, alla pedopornografia on-line, alla tutela delle infrastrutture critiche informatiche nazionali, all'hacking e ai crimini informatici in generale. Sempre connessa, per lavoro e per piacere, affascinata dalle infinite potenzialità del web, che difende con determinazione da chi vuole renderlo un luogo pericoloso. È membro del Comitato Scientifico dell'Osservatorio Permanente sulla Sicurezza e del Comitato Scientifico dell'Osservatorio Permanente sulle politiche educative dell'EURISPES. È componente del Consiglio del "Women4Cyber", iniziativa avviata dall'Organizzazione Europea per la Sicurezza Cibernetica (ECSO), volta a implementare il coinvolgimento delle donne nel settore della sicurezza cibernetica. Ha svolto attività di docenza presso diverse scuole di Polizia, presso la scuola Ufficiali dei Carabinieri, presso il Centro Alti Studi per la Difesa, ed è relatrice presso diverse università ed enti, sulle principali attività di competenza dell'Agenzia per la Sicurezza Cibernetica. Autrice del libro "Con lo smartphone usa la testa", Sperling & Kupfer, 2018 e di pubblicazioni a carattere scientifico in materia di cybercrime, ha collaborato alla redazione dei Rapporti Clusit. Ambasciatrice di Telefono Rosa contro la violenza sulle donne. Vincitrice del premio "Inspiring Fifty 2021 Italy", conferito da personalità del mondo imprenditoriale, del business e dell'Accademia alle donne che fanno da "role model" nel mondo della tecnologia. Vincitrice della Mela d'oro in occasione della 35esima edizione del Premio Marisa Bellisario come riconoscimento alle donne che fanno la differenza con un percorso professionale manageriale esemplare nel mondo delle istituzioni: "Un modello di donna delle istituzioni che con grande intuito e dedizione lavora ogni giorno per la nostra sicurezza".

Il quantum computing e le insidie di Ulisse, primo hacker della storia.

Intervista VIP a Francesco Marchesani.

Autore: Massimiliano Cannata

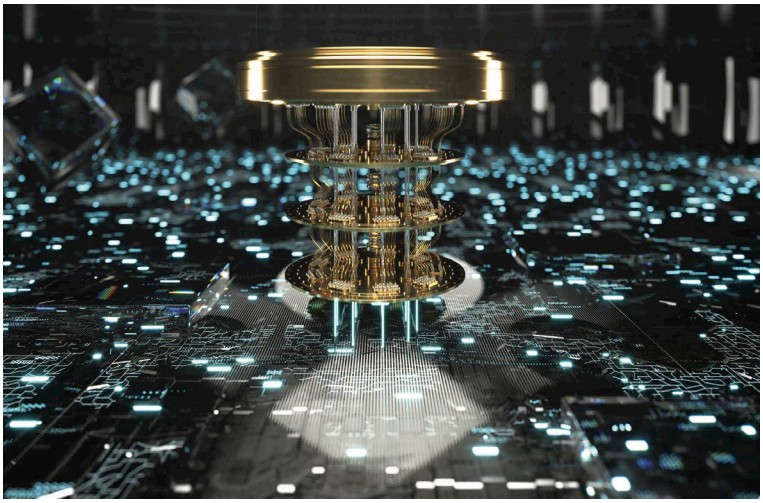
"I sistemi basati su intelligenza artificiale e sul machine learning saranno sempre più utilizzati sia per attacchi che per difese. Sviluppare competenze in queste tecnologie sarà fondamentale per rimanere al passo con le minacce e le soluzioni di sicurezza. In particolare il quantum computing si pone come una spada di Damocle sulla crittografia odierna. Investire nella ricerca di nuove tecniche quantistiche sarà una necessità imprescindibile per proteggere i nostri dati".
Francesco Marchesani, ingegnere informatico, scrittore, esperto di Cybersecurity, offre uno sguardo sinottico sulle sfide della cyber security, navigando con proprietà dialettica e chiarezza di idee, nel mare "periglioso" di Ulisse, eroe omerico evocato nel suo brillante saggio.

BIO

Francesco Marchesani è un ingegnere informatico e autore. Attualmente lavora in Google come Customer Engineer (Security) per il Public Sector in Europa, Medio Oriente e Africa (EMEA). Nei suoi libri Francesco tratta prevalentemente argomenti che riguardano piattaforme digitali, sicurezza informatica e innovazione.

Ingegnere, il primo numero dell'anno di Cybersecurity Trends è dedicato alla nuova trama di connessione che legherà lo sviluppo del Quantum Computing alle strategie di una sicurezza cyber, sollecitata a seguire i percorsi del cambiamento. Prima di affrontare le questioni che Lei solleva nel suo ultimo saggio,* Ulisse era un hacker, *può dirci che cosa comporterà questo salto evolutivo, atteso e per molti aspetti anche temuto?

Il Quantum Computing presenta una sfida significativa per la sicurezza informatica tradizionale, poiché potrebbe compromettere l'efficacia degli algoritmi crittografici attuali. Protocolli come RSA e ECC, che sono comunemente utilizzati per garantire la sicurezza delle comunicazioni online, potrebbero infatti essere messi in scacco da attacchi "lanciati" da computer quantistici. Allo stesso tempo ritengo che il Quantum Computing offra opportunità per lo sviluppo di nuovi algoritmi crittografici, come l'utilizzo di chiavi quantistiche per garantire la sicurezza delle comunicazioni. Simili

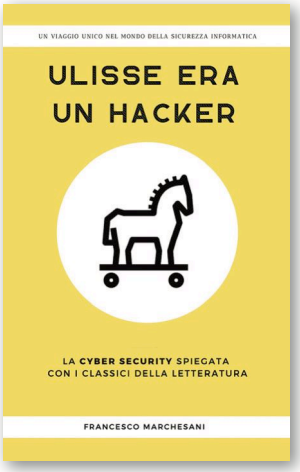


approcci, basati sui principi della meccanica quantistica, potrebbero offrire una sicurezza superiore rispetto ai metodi tradizionali. Resta fondamentale, faccio questa considerazione considerando l'evoluzione della comunità della sicurezza informatica presa nel suo complesso, mettere in atto le azioni, sul piano sia strategico che formativo, che possano abilitare le organizzazioni a gestire le sfide dell'avvenire, che non possiamo prevedere a tavolino. È una questione di metodo e di apertura mentale che va costantemente esercitata e allenata.

Il mito e la cyber security

La cyber security spiegata con i classici della letteratura. Il suo scritto ha queste finalità. Quali sono i vantaggi di un approccio certamente originale?

Rendere la cyber security accessibile a tutti. Credo sia importante promuovere una cultura della sicurezza informatica semplice, condivisibile, facilmente intellegibile. Dobbiamo tutti essere consapevoli dei pericoli che si nascondono online, dalle truffe ai ransomware, per imparare a proteggerci adeguatamente. Ricordiamo sempre che queste minacce coinvolgono non solo aziende e governi, ma tutti i cittadini. Con il mio libro voglio anche educare le nuove generazioni: i giovani di oggi saranno i cittadini e le cittadine digitali di domani; quindi, è fondamentale che essi imparino fin dai primi anni a scuola le basi della cyber security. Attraverso un linguaggio semplice e divertente, il mio obiettivo è insegnare loro come navigare nel web e usare i propri dispositivi in modo sicuro e responsabile. I vantaggi dell'approccio originale basato sui classici della letteratura sono, dal mio punto di vista, molteplici.



Possiamo fare qualche esempio?

La letteratura rende la cyber security più accessibile a un pubblico ampio. Le storie e i personaggi dei classici sono noti a tutti, e questo facilita la comprensione di concetti complessi. Inoltre, il libro diviene immediatamente coinvolgente e stimolante, invogliando il lettore ad approfondire le tematiche trattate. L'originalità dell'idea permette di esplorare la cyber security da una nuova prospettiva, creando un'esperienza di apprendimento unica e memorabile. Ulisse, ad esempio, può essere visto come un hacker ante litteram. Con il suo ingegno e la sua tenacia, supera ostacoli insormontabili e raggiunge i suoi obiettivi, agendo da vero e proprio social engineer. Teniamo presente che la letteratura è ricca di storie che possono essere interpretate in chiave moderna: lo stesso mito di Prometeo, ad esempio, ci insegna i pericoli dell'uso improprio della tecnologia. «Ulisse era un hacker» vuole essere un ponte tra la cultura letteraria e il mondo della cyber security.

Ulisse primo "hacker" dunque. Una metafora suggestiva per l'eroe omerico che mistifica l'identità operando sul camuffamento, sulla finzione, sull'inganno. Si può affermare che i cyber criminali sono tanti "Ulisse" senza scrupoli?

L'accostamento tra Ulisse e la figura dell'hacker è senza dubbio suggestivo e ricco di spunti di riflessione. Entrambi, infatti, si muovono in un mondo pieno di insidie, dove l'astuzia e l'inganno sono spesso elementi imprescindibili per sopravvivere. L'eroe di Itaca, ad esempio, si camuffa e inganna i suoi nemici per superare le sfide del suo viaggio. Allo stesso modo, i cyber criminali utilizzano tecniche di social engineering, phishing e malware sempre più avanzati per carpire informazioni e accedere a sistemi informatici. Tuttavia, credo che sia importante non abusare di questa metafora. Ulisse nell'epica greca è pur sempre un eroe che combatte dapprima una lunga guerra, per poi tornare all'agognata terra natìa dopo numerosi anni di viaggi e avventure. I cyber criminali, invece, sono mossi da avidità, motivazioni politiche o da intenti malevoli. In molti casi non hanno scrupoli e non esitano a danneggiare le persone, anche pesantemente.

Non tutti gli hacker sono "criminali". Perché lo dimentichiamo spesso?

Per superficialità di approccio. Molti hacker (gli "ethical hacker" n.d.r.) sono professionisti esperti che mettono le loro conoscenze al servizio della sicurezza informatica. Essi lavorano per proteggere i sistemi e le informazioni

da attacchi e intrusioni. Se da un lato, dunque, la metafora di Ulisse come primo hacker può essere utile per comprendere alcuni aspetti del cybercrime, dall'altro non dobbiamo dimenticare le profonde differenze che esistono tra l'eroe omerico e i criminali informatici. I parallelismi sono sempre suggestivi, ma le profonde differenze etiche, contestuali e di finalità tra l'eroe omerico e i criminali informatici non devono essere ignorate.

La centralità del fattore umano

Più ci si sofferma ad analizzare le potenzialità di strumenti e reti più emerge la fragilità del fattore umano. Esistono delle contromisure?

Sicuramente è una sfida articolata. Non si tratta di semplice disattenzione o scarsa conoscenza: la fragilità umana, nella sfera digitale, assume sfumature complesse, intrecciandosi con emozioni e debolezze insite nella nostra stessa natura. Paura, ansia, curiosità sono emozioni che possono offuscare il giudizio e renderci vulnerabili alle trappole digitali. Pensiamo a una email dal mittente

sconosciuto, un link accattivante, un messaggio che suscita timore o urgenza: ecco che la razionalità vacilla e si cede all'impulso, aprendo la porta a *malware, phishing* e intrusioni indesiderate. Spesso sottovalutiamo i rischi, convinti che le minacce informatiche non tocchino noi. Ci sentiamo al sicuro nella nostra bolla digitale, ignari del fatto che un semplice click può compromettere dati sensibili, identità e la sicurezza di interi sistemi. Spesso, poi, ci fidiamo ciecamente di ciò che vediamo online, cadendo vittima di truffe e raggiri architettati con abile ingegneria sociale. La bontà d'animo e l'inclinazione a fidarci del prossimo si trasformano in armi a doppio taglio nel mondo digitale, dove l'anonimato può celare intenzioni maligne. Oltre a rafforzare le difese tecniche con software e protocolli di sicurezza, diviene quindi fondamentale investire sulla formazione e sulla sensibilizzazione.

Lo si ripete spesso. Da dove bisognerebbe partire?

Cominciando con l'educare gli utenti a riconoscere le minacce, a gestire le emozioni online e a mettere in pratica un comportamento sicuro è un passo fondamentale

per rendere il cyberspazio un luogo più sicuro. Non si tratta certo di demonizzare la fragilità umana, ma di comprenderla e di imparare a gestirla. Emozioni e debolezze fanno parte di noi, ma non devono condurci a scelte rischiose e dense di problemi. Conoscere i propri punti deboli, essere consapevoli delle minacce e adottare un approccio cauto e responsabile sono le armi migliori per difenderci nel mondo digitale. La sicurezza informatica non è solo una questione di tecnologia, ma anche di cultura, pensiero critico e di consapevolezza. Solo comprendendo le fragilità umane e sviluppando una difesa psicologica adeguata possiamo rendere il cyberspazio un ambiente più sicuro e affidabile per tutti.

"Il futuro non è più quello di una volta"

Il libro guarda al futuro. Peccato che ci vorrebbe l'Oracolo di Delfi per capire quello che ci aspetta. Su cosa bisognerà porre l'attenzione per migliorare i livelli di protezione degli asset?

Predire il futuro della cybersecurity è un'impresa ardua. Come in un enigma sibillino, le tendenze attuali ci offrono solo frammenti di ciò che avverrà, lasciandoci con la responsabilità di interpretare e prepararci. Al contempo, possiamo comunque osservare i trend e le innovazioni emergenti, per cercare di capire in che direzione potrebbe muoversi il mondo della tecnologia e dell'informatica. Dal mio punto di vista, sistemi basati su intelligenza artificiale e machine learning saranno sempre più utilizzati sia per attacchi che per difese. Sviluppare competenze in queste tecnologie sarà fondamentale per rimanere al passo con le minacce e le soluzioni di sicurezza. Il cosiddetto *quantum computing* si pone come una spada di Damocle sulla crittografia odierna. Investire nella ricerca di nuove tecniche quantistiche sarà una necessità imprescindibile per proteggere i nostri dati. Pensiamo poi all'*Internet of Things (IoT)*: un'esplosione di dispositivi connessi comporta su base statistica un aumento progressivo di vulnerabilità sfruttabili dagli attaccanti. Rafforzare la sicurezza di questi dispositivi e delle loro reti sarà un compito arduo ma non eludibile.

Web3 se ne parla nella parte finale del lavoro. Possiamo in estrema sintesi spiegare in conclusione di che cosa si tratta?

Il Web 3.0 (o semplicemente Web3) è una visione ambiziosa che promette di cambiare significativamente il modo in cui utilizziamo internet, partendo

dalla tecnologia *blockchain*. In linea teorica, il Web 3.0 offre la possibilità di creare un internet più aperto, democratico e sicuro. La decentralizzazione del controllo del web, l'utilizzo della tecnologia blockchain e l'introduzione di token digitali potrebbero portare a una serie di vantaggi per gli utenti, come il maggiore controllo dei dati personali o nuove opportunità finanziarie. Teniamo anche presente che il Web 3.0 presenta alcune sfide che non possono essere ignorate. La complessità delle tecnologie sottostanti e la scalabilità di alcune soluzioni proposte sono solo alcuni degli ostacoli che devono essere superati prima che il Web3 possa diventare realtà. Nonostante la blockchain sia nata ormai più di 15 anni fa (Bitcoin è stato lanciato all'inizio del 2009), il Web3 è ancora un'area relativamente nuova e solo in parte regolamentata, anche se le cose stanno progressivamente cambiando su quest'ultimo fronte (si veda come esempio l'entrata in vigore della regolamentazione MiCAR 1 in Europa quest'anno, n.d.r.). Vi è, comunque, ancora terreno fertile per truffatori e schemi Ponzi che sfruttano l'hype e la complessità del Web3 per ingannare gli utenti, specie quelli meno esperti. Nel 2022, ad esempio, i crolli di FTX e del token Terra Luna hanno avuto un impatto negativo sull'intero ecosistema delle criptovalute, danneggiando la fiducia degli investitori e sollevando preoccupazioni sulla sicurezza e la stabilità del settore. Il fronte, come si può ben comprendere, è ancora tutto da esplorare e da adeguatamente presidiare. ■

Security Mind

La Cyber Security incontra La Psicologia

A cura di Veronica Patron Co-Founder di Security Mind

Alla Scoperta delle Euristiche e dei Bias Cognitivi nella Cyber Security

Le Euristiche sono delle scorciatoie mentali che il nostro cervello usa per semplificare il processo decisionale. Queste scorciatoie sono utili perché ci permettono di prendere decisioni rapide senza dover analizzare dettagliatamente ogni singola informazione che incontriamo. Ma possono condurre ad errori di giudizio.

I Bias Cognitivi sono gli errori di giudizio, provocati dal modo in cui elaboriamo informazioni e prendiamo decisioni. Possono essere visti come effetti collaterali delle euristiche.

Nel contesto della sicurezza informatica, i criminali possono sfruttare sia le euristiche che i bias cognitivi per ingannare le persone affinché compiano azioni indesiderate, come ad esempio cliccare su un link dannoso o divulgare informazioni riservate.

Ma quali sono i Bias più comuni nella Cyber Security?

1. **BIAS DI CONFERMA**
   Porta gli individui a cercare o interpretare le informazioni in modo che confermino le loro preconcezioni, ignorando i segnali di allarme o le informazioni che contraddicono le loro convinzioni esistenti.

2. **BIAS DI SCARSITA'**
   Tendiamo ad attribuire maggiore valore a ciò che è percepito come raro o in offerta limitata, induce un senso di urgenza che può spingere le vittime a compiere azioni senza la dovuta riflessione.

3. **BIAS DELL'AUTORITA'**
   Indica la tendenza a fidarsi di chi viene percepito come una figura autoritaria. I cyber criminali sfruttano questo bias impersonando figure di potere, come amministratori delegati o alti dirigenti ingannando il destinatario.

4. **BIAS DI ANCORAGGIO**
   Si riferisce alla tendenza umana di fare affidamento eccessivo su una prima informazione ricevuta quando si prendono decisioni successive.

La nostra Missone è passare dall' Informazione alla Trasformazione

www.securitymind.cloud

Italiadecide Rapporto 2023 Il Mulino

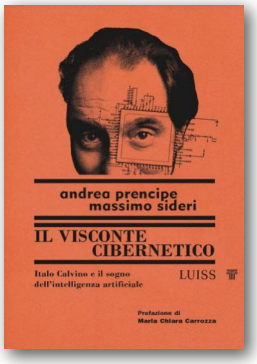
La scuola nel tempo mutante della società tecnologica

Autore: Massimiliano Cannata

Viviamo nella società della conoscenza. Se fosse vero la scuola dovrebbe godere di una centralità di fatto negata dalla scarsa attenzione dei decisori pubblici, evidente nell'attuazione reiterata della politica dei "tagli". I sistemi educativi si trovano infatti nella tenaglia di una duplice crisi. La prima, concernente le tecnologie della comunicazione, è indotta dalla rivoluzione digitale che sta trasformando repentinamente i modi di produzione, accumulazione, trasmissione e circolazione della conoscenza e dei saperi; la seconda riguarda i modelli culturali e valoriali della civiltà occidentale, così come si è sviluppata in Europa e si è diffusa nel mondo, che conduce alla confluenza di molteplici transizioni: il declino, lento ma inevitabile, del patriarcato; il declino dell'età dei combustibili fossili; il progressivo "mutamento di paradigma" che ha plasmato per secoli la nostra moderna civiltà, leggibile nel passaggio da un pensiero analitico, semplificante e tecnocratico a un pensiero sistemico, complesso ed ecologico. Questa la tesi di fondo, argomentata dall'epistemologo Mauro Ceruti, che attraversa il Rapporto Italiadecide su *"Educazione e formazione nelle democrazie del XXI secolo"*. Molto vasto l'orizzonte preso in esame dagli studiosi: la nuova alleanza tra linguaggi naturali e artificiali, l'educazione alla sostenibilità, la comunicazione e applicazione di saperi spendibili in un universo del lavoro in mutazione. Stiamo vivendo una crisi cognitiva che concerne il rapporto che l'uomo intrattiene con sé stesso e con la realtà. "Un pensiero in crisi – spiega il filosofo – che oggi appare impotente di fronte a un mondo in crisi. Affrontare una riforma del pensiero come quella che serve per uscire dal tunnel della crisi impone una riforma dell'educazione, che vede al centro proprio la scuola e l'Università". La complessità di un mondo caratterizzato da un aumento inedito e simultaneo di interdipendenza e di potenza tecnologica crea, infatti, condizioni favorevoli per adottare strategie audaci e innovative quelle pratiche e politiche educative, che presiedono alla trasmissione della conoscenza, che tanto fragili ci sono apparse nel periodo della pandemia e nel corso delle tante emergenze che ci siamo trovati a fronteggiare. Per reggere l'impatto di un mondo in trasformazione bisogna intendere l'"innovazione pedagogica" da introdurre e costruire nei prossimi anni in un senso ampio e globale, non riducibile né all'applicazione del digitale in ambito didattico, né alla ricerca di empatia e risonanze emotive nella relazione docente-allievo, pure necessarie. Bisognerà tenere conto che l'innovazione è un processo che dovrà passare attraverso una riforma dei contenuti e attraverso l'assimilazione di un paradigma culturale imperniato su un nuovo umanesimo, commisurato alla inedita condizione umana globale del nostro tempo, che ribadisco è un tempo della complessità, in cui tutto è connesso. Servirebbero investimenti mirati per rafforzare la qualità, l'innovazione, l'efficacia dell'esperienza formativa che sono leve decisive per la riduzione delle dicotomie territoriali, la diseguaglianza e la dispersione scolastica. Quest'ultimo fenomeno in Italia tocca livelli tra i più alti d'Europa eppure continuiamo a trattarlo, denuncia Santa Parrello in *"Maestri di strada di Napoli: l'esperienza educativa contro il rischio della dispersione"* come se si trattasse di una pratica burocratica da espletare. A queste condizioni risulterà impossibile togliere manovalanza alla criminalità, facendo innalzare quel capitale sociale che è la vera ricchezza di ogni nazione. "Stanno venendo meno i canoni fondamentali dello scrivere, leggere, subiamo una sorta di ipernozionismo da utenti di Google – l'analisi del filosofo Salvatore Natoli – che consegna ai giovani un sapere labile, senza fondamenti, che esula dalla argomentazione razionale, con il risultato che il paese è destinato a un irreversibile declino". Sono passati cento anni dalla riforma Gentile, e stiamo ancora annaspando nel labirinto di riforme incompiute. Dal passaggio fondamentale alla scuola media unificata, datato 1962-63, alla svolta disegnata da Luigi Berlinguer che ha introdotto il principio dell'autonomia, auspicando un bilanciamento necessario tra responsabilità decisionale e capacità progettuale non sempre messe in campo dai singoli istituti, il "cantiere educativo" è rimasto aperto. Aggiornare lo statuto delle discipline sempre più interconnesse, governare la crescita di classi multietniche che impongono una questione della lingua, riequilibrare il rapporto tra l'istruzione classica e gli istituti tecnici, decisivi nell'intercettare la domanda delle imprese, le tante questioni irrisolte non devono però far pensare che le aule siano cristallizzate nell'immobilismo. La recente rivolta del Tasso, storico liceo romano che sta vedendo i genitori rifare "la lotta di classe" al fianco dei figli fa comprendere al corpo collettivo che il *"dàimon"*, la passione dei greci per il sapere e per una scuola inclusiva non è morta, fa sentire il suo dissenso, richiedendo risposte immediate, ineludibili. ■

Andrea Prencipe, Massimo Sideri Il Visconte cibernetico Ed. LUISS University Press

Le intuizioni di Calvino e la rivoluzione tecnologica



Autore: Massimiliano Cannata

Il *Visconte cibernetico* di Andrea Prencipe Rettore della Luiss e Massimo Sideri, giornalista, conoscitore e divulgatore attento delle mirabolanti fenomenologie dell'innovazione che la tecnologia ci mette continuamente sotto gli occhi, è uno scritto denso di spunti teoretici, filosofici letterari. A partire dal "recupero" di una grande figura del Novecento, come è stato Italo Calvino, di cui

sono stati da poco celebrati i cento anni dalla nascita. L'immagine dell'uomo diviso, intuita dallo scrittore nel celebre racconto "Il Visconte dimezzato" attraversa l'analisi degli studiosi, proiettandoci su alcuni aspetti stimolanti ma anche inquietanti della contemporaneità. Il prepotente sviluppo della tecnoscienza pone interrogativi di non facile interpretazione.

L'IA, osserva in un interessante commento apparso sul Corsera il filosofo Maurizio Ferraris, non può essere lasciata a se stessa, va governata, perché non c'è nulla di più umano della tecnologia, che accompagna la civiltà fin dal suo sorgere. Calvino lo aveva scritto anticipando i tempi, facendo vedere come le dicotomie classiche, attorno a cui il pensiero filosofico ruota da secoli, sono sempre valide, ineludibili. ***Caso e necessità, responsabilità e destino, istante e decisione, uomo e macchina***, sono questioni che rimandano al rapporto tra sviluppo fisico - biologico e religione, rimandano all'etica che impone di trovare una direzione al nostro agire, alla concezione di un tempo fluttuante, post euclideo, che preme sulle nostre decisione, cambiandone verso e significato, alla tecnologia, che getta un ponte tra l'individuo e gli strumenti, protesi sofisticare che si interpongono, mediando: sentimenti, idee, parole.

I dilemmi della contemporaneità si specchiano tutti in questo agile e originale scritto, che in trasparenza rimanda alle ultime riflessioni di Edgar Morin *(Ancora un momento, Ed. Raffaello Cortina)* che mette a nudo, in pagine piene di passione e sentimento, il dramma dell'io, che vive la dimensione della "policrisi", condizione di paura e spaesamento che riassume una crisi multifattoriale: sociale, economica, politica.

"È possibile che l'umanità faccia ancora l'umanità?", l'interrogativo di Morin, è quello stesso dei nostri autori, manifestato ancora una volta da Calvino, nelle sue *Lezioni americane*. "Se la complessità del reale sfida la conoscenza non possiamo arrenderci – si legge nella lezione dedicata alla *molteplicità* - il plurale è la categoria di lettura dell'esistente, la molteplicità non ammette infatti nessuna *reductio ad unum*".

Nella società tecnologica bisogna saper tessere insieme saperi diversi, molteplici codici in una visione plurima, sfaccettata del mondo. Ricostruire i *"sentieri interrotti"*, per sanare la frattura tra l'essere e il mondo, che la post modernità ha avvertito per prima e che la "quarta rivoluzione", (per usare la nota definizione di Luciano Floridi) dettata da Internet e dalla IA ha portato a maturazione, fino alle estreme conseguenze. Di fronte alle trasformazioni epocali socio tecnologiche, l'uomo si riscopre "senza qualità", smarrito, preso da imbarazzo e angoscia, ma non può arrendersi. Prencipe e Sideri ci aiutano a ritrovare il linguaggio giusto, che è poi una questione di prospettiva, di metodo, di approccio. Servono "dosi massicce di pensiero critico" ha ragione il filosofo del linguaggio Franco Lo Piparo, non bisogna arrendersi al pensiero unico ma aprirsi a una dialogicità, necessaria dopo il naufragio delle certezze e il declino dell'epistemologia classica.

Gli autori sembrano volerci dire che sperata la fase "protagorea", di un realismo ingenuo che ci faceva pensare che l'uomo era comunque misura di tutte le cose, perché è accaduto che è la misura stessa che è saltata. Per porre rimedio nuovi parametri della conoscenza devono essere esperiti e applicati, al fine di capire il presente e intercettare il futuro. ■

Giovanni Ziccardi
Dati Avvelenati
Ed. Raffaello Cortina

Truffe, virus informatici e falso online

Autore: Giovanni Ziccardi*

In anni recenti è apparsa all'orizzonte una minaccia tecnologica che ha visto un'espansione senza precedenti durante la pandemia, la crisi economica, il conflitto Russia-Ucraina e la guerra in Medio Oriente. Da allora, ha continuato a crescere grazie alla diffusione di virus informatici che rubano, distruggono, sequestrano o divulgano dati riservati di persone e aziende, e inquinano l'ambiente digitale nel quale i cittadini vivono, comunicano e lavorano. Ad agire nel sottobosco criminale sono gruppi ben organizzati che approfittano delle vulnerabilità nei comportamenti delle vittime – e delle loro scarse, o inesistenti, competenze informatiche – per truffarle, rubare loro l'identità e commettere vari tipi di reati. I nuovi criminali informatici avvelenano il dibattito pubblico e alterano gli equilibri democratici con la diffusione di disinformazione, di espressioni che istigano all'odio e di teorie del complotto; minano, al contempo, la correttezza degli scambi tra privati sulle piattaforme di commercio elettronico e in tutte le attività che si svolgono in rete. Simili obiettivi vengono raggiunti anche falsificando contenuti audio e video, con manipolazioni digitali estremamente realistiche finalizzate a rappresentare una persona affinché dica cose che non ha mai detto, faccia cose che non ha mai fatto o, addirittura, sia collocata in luoghi, situazioni e scene dove, in realtà, non è mai stata. Sono presi di mira, indistintamente, soggetti privati, enti, professionisti, aziende, infrastrutture, utenti dei social network e, persino, ospedali e persone vulnerabili quali anziani, bambini e malati. In un quadro così critico, i temi della criminalità digitale, dei virus, della sicurezza informatica, dei sabotaggi tecnologici, dello spionaggio elettronico, delle frodi telematiche e, in generale, le attività delle organizzazioni criminali sono sempre stati visti come argomenti caratterizzati da una forte componente tecnica e, pertanto, poco interessanti per l'utente comune, nonché obiettivamente ostici da comprendere. Sono tematiche percepite come molto lontane dalle preoccupazioni tipiche di un genitore o di un insegnante; sono nozioni che possono suonare noiose anche per molti bambini e adolescenti, ormai attivi online già a partire dai cinque anni, e per intere giornate, con un alto grado di spavalderia ma, al contempo, con le difese quasi sempre abbassate. Questi argomenti attirano ancor meno le attenzioni di tutto quel mondo che ruota attorno ai professionisti, ai manager e alle aziende e, in generale, a coloro che fanno un uso della tecnologia non particolarmente raffinato – e, tendenzialmente, ripetitivo – e non si sentono direttamente coinvolti nelle questioni di sicurezza. Si pensi ad amministratori delegati e ai vertici aziendali ma, anche, al

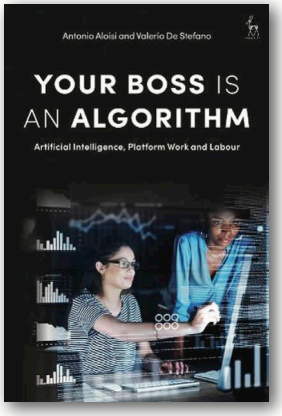
mondo della politica, ai funzionari e a quegli individui che rivestono posizioni apicali e che, pertanto, dovrebbero essere i primi a essere preparati, e a investire, su questi temi. In verità, una visione meno superficiale di queste problematiche, più moderna e adatta ai tempi, attenta al mondo che ci circonda e proiettata verso il futuro, rivelerebbe come ci si trovi di fronte a una criticità che sta colpendo le persone di tutte le età, e professioni, in ogni parte del mondo. Si tratta di una materia che, nell'era delle piattaforme, della profilazione continua degli utenti, delle fragilità comportamentali correlate al post-pandemia, alle guerre e alla crisi economica, dell'intelligenza artificiale e della corsa sfrenata alla monetizzazione e al trattamento dei dati, è diventata fondamentale. Da un lato, vi è stata l'improvvisa e profonda penetrazione delle nuove tecnologie nel tessuto sociale moderno. È, questo, un fattore che ha fornito ai cittadini una rosa di strumenti sempre più sofisticati che hanno, però, la caratteristica di contenere, raccogliere, diffondere e, in generale, trattare i dati delle persone, compresi quelli più intimi, con un'intensità mai sperimentata prima. Tale trattamento avviene anche a dispositivi spenti, sui vari servizi collocati ai quattro angoli del mondo e, in alcuni casi, persino all'insaputa dell'utente: mentre le persone dormono, le macchine continuano a generare e a diffondere dati su di loro (…)

(…) Scopo di questo libro è quello di fornire una base di conoscenza tecnica e di sicurezza personale e professionale attraverso un approccio semplice, non traumatico, appassionante, ricco di esempi, di incidenti, di sanzioni e di casi pratici, con un costante riferimento alla fiction e alla tecnologia così come è stata assorbita dalla cultura popolare. L'obiettivo è quello di riuscire, attraverso una spinta gentile, a responsabilizzare e cambiare i comportamenti di tanti lettori e lettrici nel loro modo quotidiano d'interagire con i servizi online, nelle loro abitudini di utilizzo di strumenti informatici e nelle loro prassi lavorative. L'idea è che questo libro sia letto da utenti e da professionisti, che sia preso come riferimento formativo e culturale da genitori, insegnanti, dirigenti scolastici e referenti per il cyberbullismo, nonché da minori e adolescenti, e che sia studiato anche da chi ha compreso, magari prima di altri, come la sicurezza informatica sia diventata un patrimonio di competenze oggi imprescindibile. Può essere, in tal senso, un testo da consegnare a quegli amici e conoscenti che si credono già esperti e che, pertanto, hanno la tendenza ad abbassare la guardia nella loro attività online. Il problema della sovrastima delle proprie competenze informatiche e di cybersecurity – ossia il credere di sapere di più di quanto realmente si sappia – è individuato da tempo come un fattore critico capace di generare vulnerabilità importanti soprattutto in ambito aziendale. La protezione informatica dalla criminalità attuale può, e deve, diventare popolare e democratica nel senso migliore del termine: non più un elenco di arcani segreti, di formule e di codice incomprensibile ai più che scorre su uno schermo, ma un piccolo patrimonio di conoscenza comune e alla portata di tutti. Ciò permetterà di vivere meglio, e in maniera più sicura, in una società digitale che spesso ci domina e dove, in molti casi, sono gli strumenti informatici a utilizzare noi e non viceversa. ■

**Il testo che pubblichiamo è un estratto dell'introduzione*
Gentilmente concesso dall'editore

Filmografia

Antonio Aloisi, Valerio De Stefano Your Boss Is an Algorithm (Bloomsbury Publishing PLC, 2022)



"Che effetto hanno robot, algoritmi e piattaforme online sul mondo del lavoro?"

Il libro *Your Boss Is an Algorithm: Artificial Intelligence, Platform Work and Labour* fornisce un'analisi dettagliata dell'impatto dei robot, degli algoritmi e delle piattaforme online sul mondo del lavoro. Attraverso casi di studio ed esempi tratti dall'Unione Europea, dal Regno Unito e dagli Stati Uniti, gli autori, Antonio Aloisi e Valerio De Stefano, forniscono una bussola essenziale per orientarsi in questa radicale trasformazione tecnologica.

L'opera esplora dettagliatamente come la tecnologia stia rimodellando il mercato del lavoro, dalla gig-economy all'impatto dell'intelligenza artificiale, dalla gestione algoritmica alla sorveglianza digitale sui luoghi di lavoro. Contrariamente alle previsioni di un'imminente obsolescenza del lavoro umano, gli autori dimostrano come gli strumenti digitali tendano a sostituire i ruoli manageriali e intensificare i processi organizzativi.

Attraverso l'ampia serie di casi di studio e ricerche approfondite, il libro evidenzia il crescente potere delle piattaforme digitali e degli algoritmi nel determinare la distribuzione del lavoro, i salari e le condizioni di impiego. Solleva inoltre questioni cruciali come la a ricerca di un equilibrio tra flessibilità e protezione dei lavoratori, e affronta il pervasivo potere del monitoraggio basato sull'intelligenza artificiale.

Un punto chiave del testo è l'appello a governare la tecnologia affinché garantisca un progresso equo e sostenibile per tutti. Gli autori sottolineano l'importanza di valutare la trasformazione digitale non solo in termini di convenienza economica, ma anche in termini di sostenibilità sociale e politica. Con un approccio interdisciplinare, il libro stimola il lettore a riflettere criticamente sull'equilibrio tra innovazione tecnologica, efficienza economica e diritti dei lavoratori, proponendo strategie per affrontare i rischi e massimizzare i benefici per la società.

Your Boss Is an Algorithm si distingue come un'opera essenziale per chiunque desideri comprendere il futuro del lavoro nell'era dell'intelligenza artificiale e delle piattaforme digitali. Scritto con chiarezza e competenza, rappresenta una risorsa preziosa per promuovere una discussione informata su uno dei temi più rilevanti del nostro tempo. ■

Proteggere i bambini on-line è una sfida globale che richiede un approccio globale. Mentre molti sforzi per migliorare la protezione online dei bambini sono già in corso, la loro portata finora è stata più di carattere nazionale che globale. L'ITU (Unione Internazionale delle Telecomunicazioni) ha avviato l'iniziativa Child Online Protection (COP) per creare una rete di collaborazione internazionale e promuovere la sicurezza online dei bambini in tutto il mondo. COP è stato presentato al Consiglio ITU nel 2008 e approvato dal Segretario generale dell'ONU e da capi di Stato, Ministri e capi di organizzazioni internazionali provenienti da tutto il mondo.

Poste Italiane, insieme alla propria Fondazione GCSEC e alla Polizia Postale e delle Comunicazioni ha prodotto la Versione italiana delle linee guida ITU, guida per la protezione dei bambini nell'uso di Internet e guida per genitori, Tutori ed insegnanti per la protezione dei bambini nell'uso di Internet.

Scaricatele su: www.distrettocybersecurity.it/linee-guida-itu

www.itu.int/cop

Una pubblicazione

web for business
swiss webacademy

Redazione:

Laurent Chrzanovski e Romulus Maier (†)

(tutte le edizioni)

Per l'edizione italiana:

Nicola Sotira, Elena Agresti

ISSN 2559 - 1797

ISSN-L 2559 - 1797

Indirizzi:

info@cybertrends.it

Şcoala de Înot nr.18, 550005,

Sibiu, Romania

www.swissacademy.eu

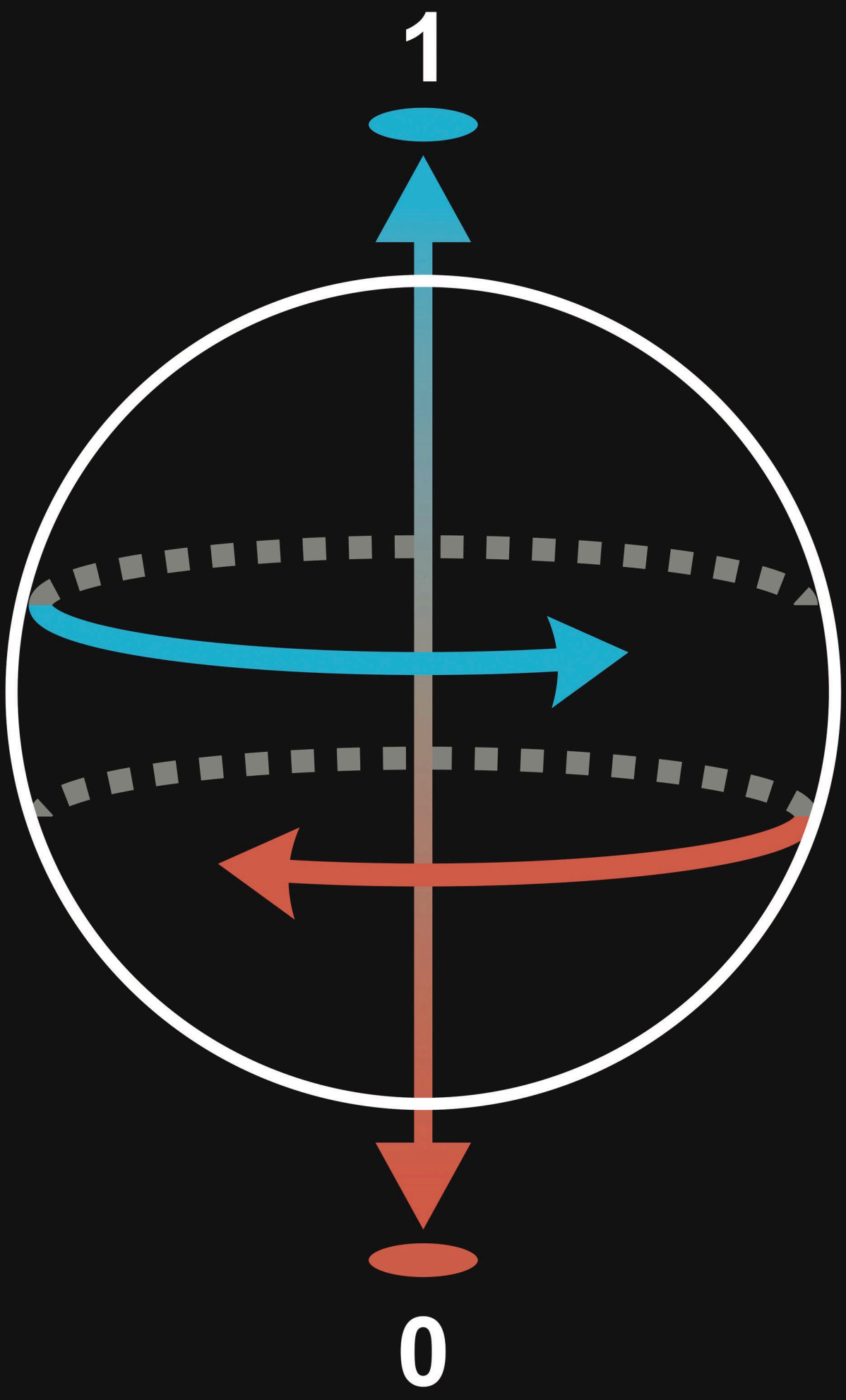
www.cybertrends.it

CYBERSECURITY TRENDS

SOSTIENI IL GIORNALISMO INDIPENDENTE

DONA ORA

Il tuo contributo è prezioso 💎
www.cybertrends.it/donate/


1
0