TIG THE INNOVATION GROUP

IL CAFFÈ DIGITALE

NOVEMBRE 2025

AI e cloud spingono il mercato digitale

LE NUOVE SFIDE PER **IMPRESE** E **PA**

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Alec Ross, *Autore & Professore, Bologna Business School*

LA TRASFORMAZIONE DIGITALE

Cavi sottomarini: un asset strategico per la competitività e la sicurezza europee

CYBERSEC E DINTORNI

I robot con le scarpe da tennis sono un rischio serio

SOMMARIO

AI E CLOUD SPINGONO IL MERCATO DIGITALE: LE NUOVE SFIDE PER IMPRESE E PA

Camilla Bellini, *Research and Content Manager*
TIG - The Innovation Group

L'ITALIA DIGITALE CONTINUA A CORRERE, MA L'INTELLIGENZA ARTIFICIALE RESTA UNA SFIDA PER IMPRESE E PA. È QUESTO IL QUADRO CHE EMERGE DALL'ANALISI DEL MERCATO DIGITALE PRESENTATA DA TIG ALL'INTERNO DELLA NUOVA EDIZIONE DEL SUO RAPPORTO ANNUALE.

Entro fine 2025, *secondo le stime di TIG – The Innovation Group*, il mercato digitale italiano raggiungerà un valore di 83,4 miliardi di euro, crescendo del +3,9% rispetto al 2024, e toccherà i 86,6 miliardi nel 2026.
È una fotografia di un mercato in crescita, dove le componenti più innovative trainano le prospettive di crescita della spesa: cloud computing, intelligenza artificiale, sicurezza informatica diventano voci di spesa che pesano sui budget ICT, soprattutto nelle grandi imprese, richiedendo un attendo monitoraggio.

UNA CRESCITA DIVERSIFICATA PER IL MERCATO ITALIANO

Più in generale, guardando alle macro-voci del mercato, lo sviluppo è trainato principalmente dai **servizi IT** con i servizi **cloud** infrastrutturali (IaaS e PaaS), i servizi di **cybersicurezza** e per lo sviluppo e la formazione in ambito AI. Continuano a crescere d'altra parte il mercato del software e dei contenuti digitali, mentre per l'**hardware** è prevista nei prossimi anni una timida ripresa, favorita dall'espansione dell'intelligenza artificiale e dalla connessa necessità di infrastrutture sempre più sicure e performanti.
A rallentare la performance del mercato della Penisola sono d'altra parte soprattutto la **componente consumer**, che maggiormente ha risentito negli ultimi anni dell'incertezza economica e del "caro vita", e i servizi di telecomunicazione, con le aziende del settore che affrontano una fase turbolenta di ripensamento e riorganizzazione: l'obiettivo è quello di "migrare" verso un **modello TechCo**, dove infrastrutture e connettività diventano piattaforme abilitanti per lo sviluppo di servizi digitali verso le imprese e i cittadini.

L'INTELLIGENZA ARTIFICIALE ALL'INTERNO DI ENTI E IMPRESE

Per quanto riguarda la diffusione dell'AI nelle imprese italiane, questa è d'altra parte ancora agli inizi. È infatti solo il 14% delle aziende coinvolte nella


© Parna Gohil / pexels.com

Digital Business Transformation Survey 2025 di TIG – The Innovation Group che dichiara di aver integrato l'intelligenza artificiale nei propri processi, frenate soprattutto dalla **carenza di competenze interne** (44%) e dagli **elevati costi** di investimento (23%).
Molte imprese stanno invece ancora esplorando o studiando l'adozione di queste soluzioni, con un 27% in fase di valutazione e un 17% che prevede di implementarla in futuro. Gli ostacoli all'adozione citati richiamano anche la difficoltà di dimostrare il valore concreto e di business delle soluzioni di intelligenza artificiale (31%) e di identificare **casi d'uso** efficaci (28%).
Questi risultati, raccolti principalmente tra aziende e organizzazioni private, si ritrovano anche tra gli enti della pubblica amministrazione, in particolare locale: se il 96% degli enti intervistati da TIG – Gruppo Maggioli nell'*Indagine sulla transizione digitale della PAL* di quest'anno ha infatti sviluppato progetti digitali nell'ultimo anno, puntando soprattutto su piattaforme digitali pubbliche e migrazione al cloud, tuttavia "solo" 18% degli enti utilizza – in modo sperimentale o più consolidato – strumenti di **AI generativa**, l'11% sfrutta assistenti e agenti AI per **automatizzare i processi** e il 9% ricorre a strumenti e modelli di AI per **l'analisi avanzata dei dati**.
Tra i principali benefici attesi dall'adozione dell'AI emerge poi in particolare la possibilità di automatizzare attività complesse e ripetitive – lo afferma il 43% dei rispondenti pubblici – seguita dalla ricerca di una **migliore interazione con i cittadini** (23%) e un incremento nella produttività personale dei dipendenti (22%); al contrario, tra gli ostacoli emergono ancora una volta la **mancanza di competenze interne** (59%) e fattori culturali come la resistenza al cambiamento (45%) e la preparazione ancora limitata della dirigenza su questi temi (36%).

LA TRASFORMAZIONE DIGITALE COME LEVA COMPETITIVA PER IL PAESE

In questo scenario, d'altra parte, la trasformazione digitale non è più soltanto un obiettivo strategico per enti e imprese, ma una leva competitiva decisiva per la **crescita del sistema Paese**. L'evoluzione continua delle tecnologie – dall'ascesa dell'intelligenza artificiale alle prospettive del calcolo quantistico e dell'high performance computing – richiede a imprese e istituzioni di **ripensare modelli, processi e infrastrutture** con una visione di medio-lungo periodo. La dinamica espansiva del mercato digitale italiano, che entro il 2025 è prevista superare gli 83 miliardi di euro, conferma la direzione che sarà necessario seguire: investire in soluzioni ICT, infrastrutture moderne e aggiornate e nell'accesso a servizi e contenuti digitali è la condizione per **supportare l'innovazione**, garantendo sicurezza, efficienza e la generazione di nuovo valore.

Investimenti e visione, per una sovranità tecnologica europea

Gianluca Dotti, *Giornalista*
TIG - The Innovation Group

LA DISCUSSIONE SULLA **SOVRANITÀ DIGITALE EUROPEA** EVIDENZIA UNA CONTRADDIZIONE ANCORA IRRISOLTA: LA CAPACITÀ DI **REGOLAMENTARE** CRESCE, MENTRE QUELLA DI **COSTRUIRE TECNOLOGIE AUTONOME** RIMANE LIMITATA. LA DISTANZA TRA AMBIZIONE E CAPACITÀ INDUSTRIALE EMERGE IN CAMPI COME L'INTELLIGENZA ARTIFICIALE, IL CLOUD E LE TECNOLOGIE DI FRONTIERA COME IL QUANTUM COMPUTING, DOVE LA COMPETIZIONE GLOBALE RICHIEDE INVESTIMENTI COSTANTI E INFRASTRUTTURE PROPRIE.

A margine del suo intervento sul palco del Digital Italy Summit 2025, a metà novembre, abbiamo incontrato **Alec Ross** nelle sale monumentali dell'Acquario Romano. Nato e cresciuto a Charleston negli Stati Uniti, ma con una famiglia di origini italiane, Ross è analista di mercato e autore di bestseller sui temi della tecnologia, noto in tutto il mondo attraverso i suoi libri e oggi anche professore alla Bologna Business School. Il punto di partenza della chiacchierata è stato il messaggio centrale del suo keynote speech: l'Europa dispone di molti talenti e di idee solide, ma fatica a trasformarli in sistemi tecnologici scalabili. Ed è proprio in questo divario tra visione e capacità produttiva che si gioca la possibilità di un ruolo del nostro continente nelle tecnologie emergenti.

Alec Ross, *Autore e Professore*, Bologna Business School

Alec Ross, quando si parla di sovranità digitale, spesso in Europa si insiste sulla regolamentazione. Secondo lei, cosa servirebbe per avere un controllo reale su dati e infrastrutture?

La regolazione non basta, anzi rischia di diventare un esercizio burocratico che dà l'illusione di proteggere i dati senza cambiare nulla nella sostanza. Tutti quei banner sui cookie fanno sorridere noi statunitensi: sembrano proteggere la privacy, ma in realtà non determinano alcun effetto. Se l'Europa vuole la sovranità digitale, credo la via sia una sola: smettere di usare gli strumenti degli altri e cominciare a costruire i propri. Significa investire in piattaforme e infrastrutture europee, non limitarsi a conferenze stampa, report o post sui social. Negli ultimi 10-15 anni l'approccio è stato troppo formale e poco concreto: molta retorica, pochi investimenti veri. La sovranità si conquista creando tecnologie, non regolando quelle altrui.

L'iniziativa Gaia-X per un'infrastruttura dati europea è stata per anni presentata come un progetto strategico. Come mai, dal suo punto di vista, non ha portato ai risultati attesi?

Il progetto Gaia-X è stato soprattutto un grande esercizio comunicativo. C'erano conferenze stampa, rapporti, tavoli di lavoro, ma non la spinta economica e politica necessaria a costruire davvero un'infrastruttura europea. È mancata la sostanza: nessuno ha investito con la determinazione che serve quando si vuole creare un'alternativa alle big tech globali. Il progetto avrebbe potuto diventare un pilastro della sovranità europea, ma si è fermato a livello teorico. È l'esempio tipico di un approccio generale: tanta narrativa, poca ingegneria e pochi capitali. Se si vuole competere, bisogna accettare

Alec Ross, Autore e Professore, Bologna Business School al Digital Italy Summit 2025 di TIG – The Innovation Group

che tecnologia significa investimenti massicci, continuità e rischi. Senza queste tre condizioni Gaia-X non aveva alcuna possibilità di trasformarsi da progetto politico a infrastruttura reale, ed era inevitabile che rimanesse un'iniziativa incompiuta.

Guardando all'intelligenza artificiale, quali filoni della competizione globale ritiene ormai persi per l'Europa, e quali invece restano ancora aperti?

L'Europa ha certamente perso terreno nell'AI legata alla raccolta dati e in quella generativa, settori ormai dominati da colossi statunitensi e cinesi capaci di investire in modo massiccio e continuativo. Ma questo non significa che tutto sia compromesso. Esistono ancora due ambiti fondamentali, l'intelligenza artificiale agentica e l'AI fisica, che uniscono software e capacità d'azione nel mondo reale e che si trovano ancora in una fase iniziale di sviluppo. È proprio qui che l'Europa potrebbe ritagliarsi un ruolo da protagonista, a condizione però di avere il coraggio di investire con serietà e di farlo senza esitazioni. Il talento, infatti, non manca: lo vedo nei giovani, nei ricercatori, nelle università con cui collaboro quando mi trovo in Italia o altrove nel continente. Ciò che oggi manca davvero è un impegno strutturale, fatto di continuità, risorse adeguate e una visione che vada oltre i documenti programmatici e le dichiarazioni di intenti. La partita, insomma, non è affatto chiusa, ma va affrontata adesso, con determinazione e con investimenti che abbiano un peso reale.

Un'altra tecnologia sulla cresta dell'onda è il quantum computing, su cui vediamo molti annunci – soprattutto dalle big tech – ma un po' meno investimenti europei. Cosa serve per restare davvero in questa partita?

Il quantum computing è un settore in cui gli annunci, se non sono accompagnati da investimenti veri e consistenti, finiscono per non avere alcun valore. Negli Stati Uniti, in Cina, in India o nei Paesi del Golfo, ogni dichiarazione pubblica viene seguita da un impegno economico enorme, che permette ai progetti di crescere e consolidarsi. So di ripetermi, ma in Europa invece troppo spesso dopo la conferenza stampa non accade praticamente nulla, e questo rivela un limite culturale prima ancora che finanziario, perché si tende a confondere la comunicazione con l'azione. Serve un cambio di mentalità, meno orientato al rituale e più all'efficacia, perché l'innovazione non è un momento da celebrare, ma un lavoro costante che va sostenuto giorno dopo giorno.

Lei ha un legame profondo con l'Italia e sostiene molte iniziative nel nostro Paese. Cosa la convince del nostro potenziale?

Il mio legame con l'Italia è fortissimo, personale e professionale. Amo questo Paese senza condizioni: la cultura, le persone e persino le sue contraddizioni. Negli anni ho sostenuto il più grande investimento di un fondo statunitense in una startup digitale italiana, e ogni giorno mi chiedo cosa posso fare per contribuire a fare crescere questo ecosistema. Qui c'è un potenziale straordinario: talenti brillanti, creatività, capacità tecnica, ma manca quel senso di autodeterminazione che spinge a non aspettare Roma o Bruxelles per risolvere i problemi. Per dirla con una battuta, credo servirebbe meno cultura del notaio e più cultura del cowboy, ossia più coraggio nel rischiare, sperimentare, costruire. L'Italia ha tutto per diventare un modello: deve solo imparare a fidarsi del proprio potenziale e a liberare l'energia che già possiede. È una delle ragioni per cui il mio prossimo libro, che si chiamerà *The Italian Dream* e uscirà nella primavera 2026, è tutto dedicato a questo Paese.

Cavi sottomarini: un asset strategico per la competitività e la sicurezza europee

Camilla Bellini, *Research and Content Manager*
TIG - The Innovation Group

UN RECENTE RAPPORTO DELLA COMMISSIONE EUROPEA METTE L'ACCENTO SUL RUOLO STRATEGICO DEI CAVI SOTTOMARINI NEL DIBATTITO PIÙ GENERALE DELL'INDIPENDENZA E DELLA SICUREZZA DIGITALE DEL CONTINENTE. SE LE COMPETENZE TECNICHE ESISTONO, MANCANO HYPERSCALER EUROPEI CHE TRAININO LA CRESCITA ED EMERGONO DIPENDENZE DA COMPONENTI NON-UE.

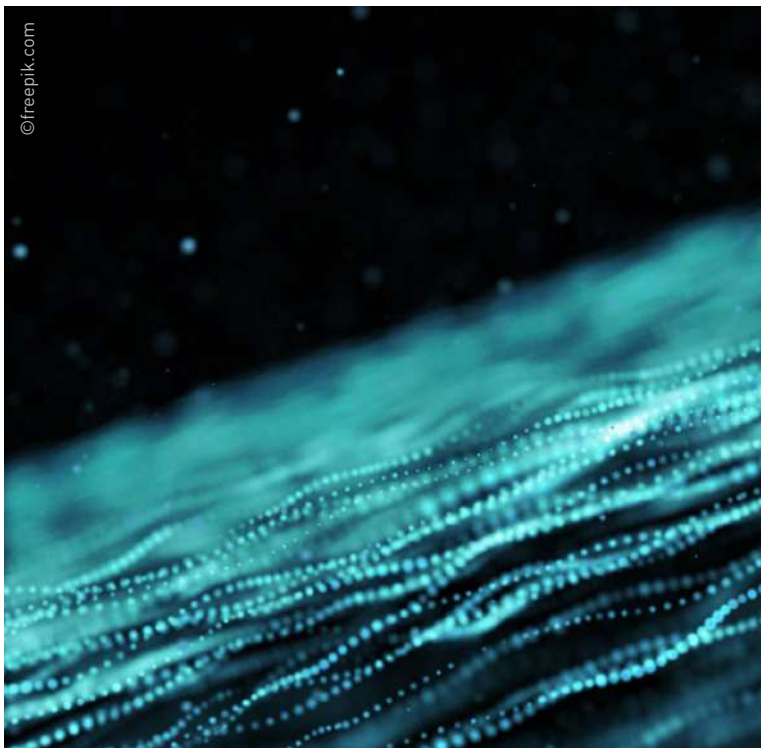
Negli ultimi dieci anni l'industria dei cavi sottomarini ha affrontato una trasformazione significativa. A guidarla non sono stati però tanto gli operatori tradizionali delle telecomunicazioni, ma piuttosto i **grandi hyperscaler statunitensi**, il cui bisogno di collegare data center e cloud region su scala globale ha spinto in modo importante la crescita della capacità dei cavi. Basti pensare che, se nel complesso la capacità dei cavi che connettono l'Unione Europea al resto del mondo è passata da 318 Tbit/s nel 2010 a 3.755 Tbit/s nel 2024, oggi gli hyperscaler rappresentano il 71% di questa capacità internazionale, contro il 10% controllato solo dieci anni prima. A riguardo, per meglio comprendere e approfondire le dinamiche relative all'**infrastruttura europea dei cavi sottomarini**, dei suoi rischi e della sua resilienza, recentemente la Commissione Europea ha pubblicato un rapporto sul tema, di cui di seguito vengono ripresi alcuni spunti, dati e riflessioni.

LA GEOGRAFIA DELLA CONNETTIVITÀ SOTTOMARINA SI TRASFORMA

Sulla rotta che collega Stati Uniti ed Europa gli hyperscaler detengono ormai buona parte della capacità dei cavi sottomarini. La corsa a interconnettere data center e cloud region su entrambe le sponde dell'Atlantico ha fatto in modo che la presenza di questi player diventasse dominante, mentre il contributo europeo, e in particolare delle aziende tradizionali di telecomunicazioni, diventava marginale. D'altra parte, attualmente non esiste in Europa un hyperscaler "nativo" paragonabile per dimensione a realtà come Amazon, Meta, AWS o Google, e gli operatori telco nazionali non generano volumi di traffico tali da giustificare l'investimento in nuovi sistemi transcontinentali. Anche al di fuori dell'asse UE – USA, lo scenario sta rapidamente evolvendo: benché attualmente nell'area del Mar Rosso e dell'Oceano Indiano la capacità controllata dagli hyperscaler sia ancora limitata, anche a fronte di un'infrastruttura cloud regionale meno sviluppata e di investimenti ancora lenti nell'area, **tre nuovi cavi ad alta capacità** – il Blue-Raman, l'India-Europe-Xpress (IEX) e il SEA-ME-WE 6 (South East Asia-Middle East-West Europe 6, o SMW6) – supporteranno gli hyperscaler nell'accesso anche a queste rotte emergenti.

CRESCE LA DIPENDENZA EUROPEA DAGLI HYPERSCALER

Circa il 97–98% del traffico Internet globale passa oggi attraverso cavi sottomarini, che emergono come



un'infrastruttura critica per le economie digitalmente più avanzate. La crescente dipendenza dell'Europa da risorse non-UE – in particolare dagli hyperscaler americani – assume anche una valenza una questione strategica. Gli hyperscaler controllano infatti già il 90% della capacità complessiva dei cavi sulla rotta USA–Europa e hanno quote in crescita sulle rotte Europa–Africa e Europa–Asia. Se queste tendenze continueranno, gli Stati membri diventeranno ancora più **dipendenti da attori extraeuropei** per i collegamenti verso Nord America, Asia e Africa, con implicazioni dirette per la sicurezza e l'indipendenza dell'UE.

CAVI NUOVI E VECCHI: UN CAMBIO GENERAZIONALE

Un cavo sottomarino ha in genere una vita utile di 25 anni, ma il vero limite non è solo tecnico, ma economico: l'arrivo di nuove generazioni di cavi a capacità molto più elevata rende infatti spesso antieconomica la gestione delle **vecchie infrastrutture**. Basti pensare che, tra i cavi oggi a disposizione, i 33 più recenti forniscono il 74% della capacità totale verso l'Unione Europea, mentre gli 89 più vecchi contribuiscono solo per il 2%; senza contare che questi ultimi trasportano soprattutto **traffico pubblico** e sono utilizzati dagli operatori di telecomunicazioni, mentre molti cavi di nuova generazione sono di proprietà degli hyperscaler e sono pensati per uso privato. Questo significa che, man mano che i cavi tradizionali si avvicineranno al fine vita, gli operatori telco europei dovranno acquistare capacità dai nuovi sistemi, spesso controllati da attori privati stranieri.

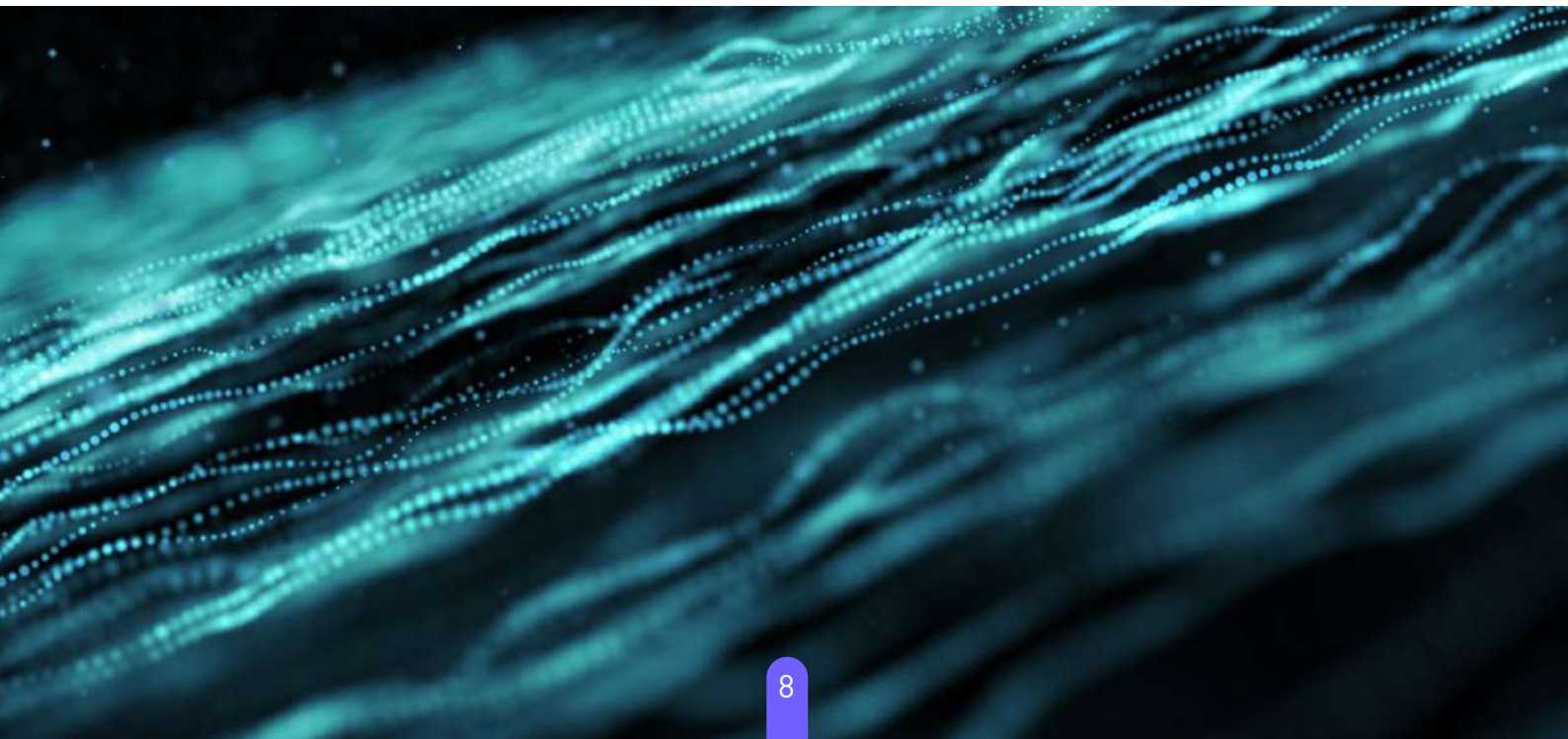
IL NODO CRITICO DELLA MANUTENZIONE

Anche la pressione sulla capacità di manutenzione e riparazione sta aumentando. Questo è dovuto soprattutto all'invecchiamento della flotta dedicata a queste attività, all'aumento della lunghezza totale dei cavi installati dagli hyperscaler che assorbe risorse crescenti, la conversione di navi di riparazione in navi di installazione, per far fronte al boom nella richiesta di nuovi sviluppi, e la possibilità che gli hyperscaler sviluppino flotte di riparazione proprie, alterando ulteriormente gli equilibri di mercato.

D'altra parte, in quest'ambito anche l'Unione Europea possiede **competenze industriali importanti**: ad esempio, la francese Alcatel Submarine Networks (ASN) è una delle principali aziende attive nell'installazione e manutenzione dei cavi, insieme alla giapponese NEC, alla cinese HMN Technologies Co. e all'americana SubCom. Tuttavia, la catena del valore europea resta vulnerabile, soprattutto per quello che riguarda la **dipendenza da fornitori non europei per componenti critici** come i microchip, con le necessarie partnership con colossi asiatici come TSMC (Taiwan) o Samsung (Corea del Sud) e con aziende statunitensi, e della fragilità rispetto a scenari geopolitici in evoluzione.

UNA VULNERABILITÀ STRATEGICA DA AFFRONTARE

La fotografia complessiva mostra un'Europa ben posizionata dal punto di vista di competenze tecniche, ma più debole per quello che riguarda **l'indipendenza e la sovranità tecnologica**. La crescente capacità dei cavi controllata da attori non-UE – soprattutto gli hyperscaler americani – e la dipendenza da componenti non europei espongono infatti l'Unione Europea a rischi. Per rafforzare la propria sovranità digitale, l'Europa dovrà pertanto **aumentare gli investimenti in cavi sottomarini** di nuova generazione, sostenendo gli operatori europei e i data center regionali, sviluppare una filiera più autonoma per i componenti critici, e garantire capacità di manutenzione e riparazione resilienti. In un'economia sempre più basata sulla connettività globale, i cavi sottomarini non sono infatti più solamente un'infrastruttura "tecnica", ma diventano un asset strategico per la competitività e la sicurezza del Vecchio Continente.



La figura del CISO evolve verso un ruolo di leadership strategica

Elena Vaciago, *Research Manager*
TIG - The Innovation Group

IL RUOLO DEL CISO (CHIEF INFORMATION SECURITY OFFICER) SI STA CONSOLIDANDO MA CON DIFFERENZE DI MATURITÀ E RICONOSCIMENTO. È QUANTO EMERGE DALLA SURVEY "IL RUOLO DEL CISO SURVEY 2025" DI TIG E ASSOCISO

Quella del Chief Information Security Officer (CISO) o Responsabile Cybersecurity è una figura sempre più matura, che oggi è chiamata non solo a proteggere l'impresa, i suoi dati e le sue persone, anche a guidare il cambiamento, a tradurre la sicurezza in **valore per l'impresa**. Il percorso professionale del CISO si apre a ruoli di vertice. È quanto emerge dall'indagine "Il Ruolo del CISO Survey 2025", realizzata tra luglio e settembre 2025 da TIG – The Innovation Group e AssoCISO, su un campione di 172 organizzazioni italiane in prevalenza di grande dimensione, per investigare appunto le evoluzioni di questo ruolo alla luce dei cambiamenti tecnologici, normativi e geopolitici. **Il risultato è che il ruolo del CISO si sta consolidando ma con differenze di maturità e riconoscimento:** ad esempio, è presente **solo nel 61%** delle aziende intervistate (che già dispongono di una strategia formale di cybersecurity) mentre negli altri casi la responsabilità sulla cybersecurity ricade su altre funzioni (CIO, CTO, CSO). Con riferimento alla collocazione aziendale del Responsabile Cybersecurity, si osserva una **situazione molto disomogenea**: nel 30% dei casi riporta al CIO e nel 29% al vertice.

Inoltre, solo la metà delle aziende prevede un **flusso strutturato di comunicazione del CISO verso il CdA,** mentre altrove il dialogo resta sporadico o intermediato. Questo limita la capacità del CISO di influenzare le decisioni strategiche.

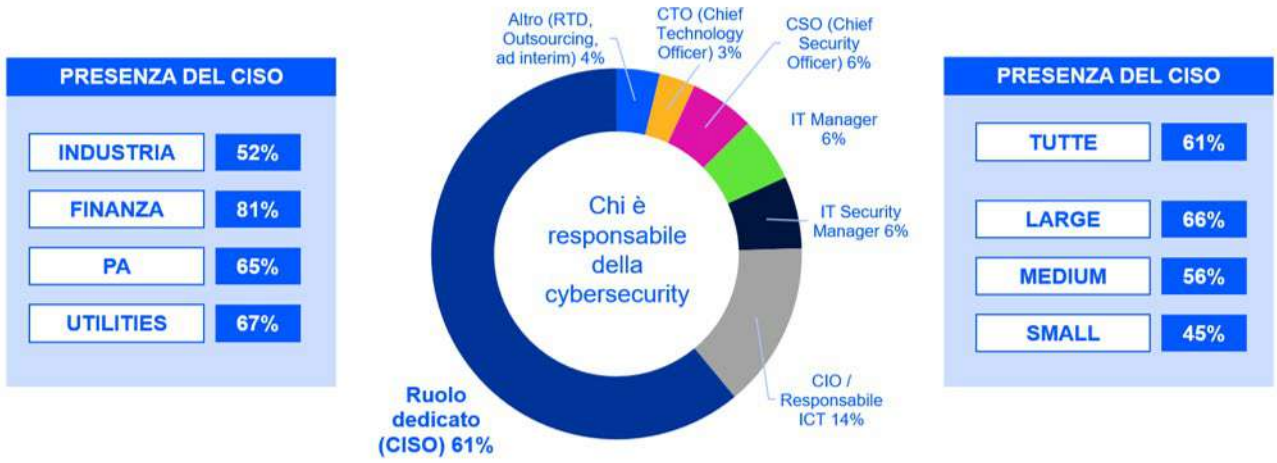
RESPONSABILITÀ E RELAZIONI CON IL VERTICE AZIENDALE

Nelle organizzazioni più strutturate, il CISO gestisce un portafoglio di attività ampio — dalla threat intelligence alla cloud security — mentre nelle realtà più piccole può trovarsi a coprire responsabilità afferenti tipicamente ad altri ruoli, come le funzioni di compliance. La comunicazione verso il CdA avviene in modo strutturato (su base trimestrale, semestrale o annuale) solo in 1 azienda su 2 (il 48% delle risposte). Negli altri casi, avviene solo su richiesta, in situazioni particolari oppure è disintermediata dal Comitato rischi, dal CIO o dal CSO, o anche non avviene mai.

LE PRINCIPALI CRITICITÀ PER IL CISO

Il reperimento di personale qualificato rappresenta oggi la difficoltà più sentita, indicata dal 57% dei rispondenti. Seguono la difficoltà di far comprendere il valore della cybersecurity (39%) e la scarsa valorizzazione del ruolo all'interno dell'organizzazione (38%). Solo al quarto posto, rispetto al passato, si colloca la mancanza di fondi adeguati (36%), segno di una maggiore attenzione al tema. Tra le richieste ricorrenti per lavorare meglio, i CISO indicano appunto la necessità di ampliare e strutturare il team di sicurezza, ottenere maggior supporto dal top management, avere chiarezza su ruoli e responsabilità, budget adeguati e strumenti di

PRESENZA DI UN RUOLO DEDICATO (CISO) PER LA CYBERSECURITY



D. Chi è il Responsabile della Cybersecurity nella Sua organizzazione?
Base: tutti i rispondenti (159)

automazione per ridurre il carico operativo. Rilevante anche la domanda di una maggiore integrazione con le altre funzioni aziendali. La comunicazione con il CdA è importante, ma comporta molte sfide (come mostra la figura successiva).

TRASFORMAZIONE DIGITALE E NUOVI TREND TECNOLOGICI

Le aziende italiane sono oggi impegnate in profondi processi di trasformazione digitale, che portano con sé anche la necessità di ripensare la cybersecurity. Secondo gli intervistati, il trend tecnologico destinato ad avere maggiore impatto in cybersecurity è **l'intelligenza artificiale**, seguita da migrazione al cloud, evoluzione dell'identity management e connettività degli oggetti. Il livello di automazione delle difese cyber — sia nei Security Operations Center (SOC) sia a livello architetturale — è giudicato buono: il 61% delle organizzazioni dichiara un grado di automazione "abbastanza o molto elevato".

FATTORI GEOPOLITICI E SCELTE TECNOLOGICHE

In un contesto internazionale sempre più instabile, gli aspetti geopolitici influenzano in modo crescente le valutazioni su tecnologie e fornitori di cybersecurity.

PRINCIPALI CRITICITÀ NELLA COMUNICAZIONE CON IL BOARD

D. Quali sono le principali difficoltà che il CISO incontra nel comunicare efficacemente con il Board / Altro Comitato sulla cybersecurity?
Base: tutti i rispondenti (144)

Le principali preoccupazioni riguardano le normative che impongono vincoli di scelta, la sovranità e localizzazione dei dati, le tensioni nelle aree chiave della supply chain, la dipendenza da tecnologie extra-UE, i rischi di backdoor o ingerenze statali e le sanzioni verso determinati vendor o Paesi. Ben il 39% delle organizzazioni dichiara di aver rivalutato o modificato le proprie scelte tecnologiche (vendor, servizi cloud, soluzioni di sicurezza) a causa di dinamiche geopolitiche, e il 63% prevede che questa influenza crescerà nei prossimi anni.

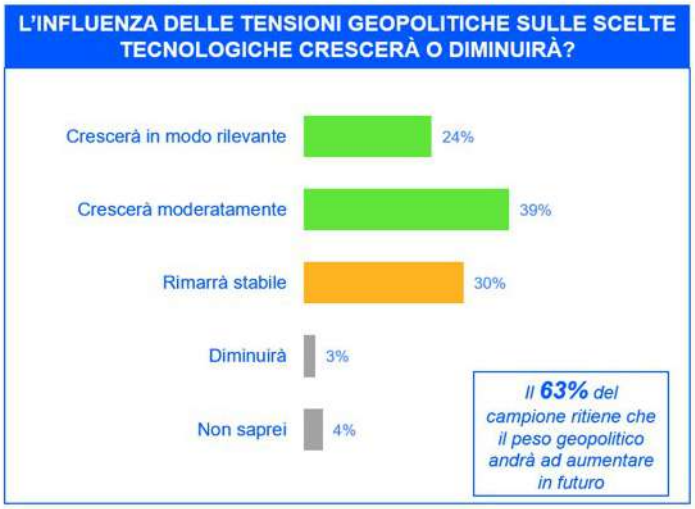
UN RUOLO SEMPRE PIÙ STRATEGICO E COMPLESSO

La ricerca, condotta tra luglio e settembre 2025, ha raccolto 172 risposte da professionisti del settore, in prevalenza CISO e manager della cybersecurity.

La maggior parte dei rispondenti appartiene a organizzazioni di grande dimensione (60% con oltre 1.000 addetti) e, in misura minore, a realtà medie (24%) e piccole (16%). I settori più rappresentati sono Industria e Finanza, confermando la rilevanza del tema per i comparti più esposti ai rischi cyber.
I risultati dell'indagine "**Il Ruolo del CISO Survey 2025**" delineano una figura professionale in forte evoluzione: più matura, più integrata nei processi decisionali, ma ancora alle prese con sfide legate a risorse, competenze e riconoscimento interno. Con la cybersecurity ormai divenuta parte integrante del business, il ruolo del CISO è sempre più strategico e trasversale. Alle competenze tecniche si affiancano oggi abilità manageriali e comunicative, fondamentali per dialogare con il top management, guidare il cambiamento e tradurre la sicurezza in valore per l'impresa.

VALUTAZIONI GEOPOLITICHE NELLE SCELTE TECNOLOGICHE

D. La Sua organizzazione ha recentemente rivalutato o modificato le scelte tecnologiche (vendor, servizi, cloud, etc.) a causa di dinamiche geopolitiche?
Base: tutti i rispondenti (152)



D. Ritiene che nei prossimi 12-24 mesi l'influenza delle tensioni geopolitiche sulle scelte tecnologiche crescerà o diminuirà?
Base: tutti i rispondenti (152)

I robot con le scarpe da tennis sono un rischio serio

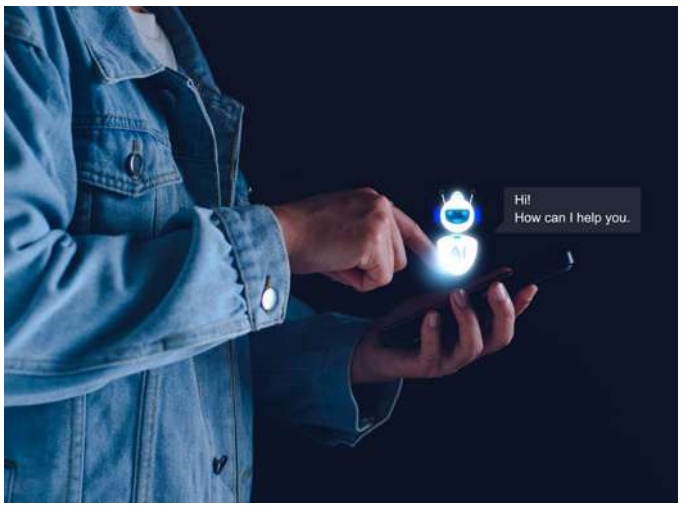
Giancarlo Calzetta, *Research and Content Manager*
TIG - The Innovation Group

I ROBOT, ANCHE QUELLI SENZA LE GAMBE, AMANO LE SCARPE DA TENNIS. PIÙ PRECISAMENTE, QUELLE DA RUNNING E DA BASKET.

Può sembrare un'affermazione curiosa, ma c'è di più. I Bot, programmi che navigano per la rete e compiono azioni in autonomia (un po' come gli agenti AI, ma senza AI), amano anche i concerti, le collezioni limitate, i memorabilia, le merci vendute con forti sconti e tutto quello di esclusivo che può essere comprato sul Web per essere rivenduto a un prezzo più alto. Con l'avvicinarsi delle stagioni di punta per il commercio elettronico, come il Black Friday e il Natale, il fenomeno dei bot-scalper, come vengono definiti quelli specializzati nello shopping, assume dimensioni sempre più rilevanti. Il recente blog post di Akamai intitolato *"Put Your Best Foot Forward: The Impact of Sneaker Bots on Holiday Shopping"* punta i riflettori su questo fenomeno e spiega come i bot progettati per accaparrarsi oggetti in edizione limitata abbiano un effetto distorsivo sul mercato e, parallelamente, vadano di pari passo con campagne massive di credential stuffing.

COSA SONO I "SNEAKER BOTS" E PERCHÉ RAPPRESENTANO UN RISCHIO

Nel linguaggio tecnico i sneaker bots sono programmi malevoli (o comunque strumenti di abuso) ideati per automatizzare la prenotazione o l'acquisto di beni in edizione limitata. Il nome nasce dal settore delle sneaker di lusso, ma l'applicazione si estende ben oltre. Tali bot possono partecipare a lanci "flash" di prodotti, restock di merci particolarmente richieste o semplici campagne promozionali con disponibilità ristretta.
L'utilizzo di questi bot oltre a generare un danno immediato al consumatore che non riesce ad accedere alle merci in disponibilità ridotta, crea per il rivenditore diversi problemi. Si parte dalla *customer experience* potenzialmente disastrosa perché i sistemi rallentano



sotto la pressione delle centinaia di operazioni al secondo compiute dai bot, ai costi per fronteggiare questa improvvisa richiesta di potenza elaborativa per arrivare, infine, alla perdita di fiducia da parte dei clienti in carne e ossa che etichettano il servizio come poco affidabile o addirittura "truffaldino". In aggiunta, l'intervento dei bot favorisce la rivendita a prezzi notevolmente maggiorati (con margini che possono raggiungere anche migliaia di percentuale) acclimatando un mercato secondario fortemente speculativo.
Ma è legale tutto ciò? Da questo punto di vista, non esista un divieto generalizzato per tutti i contesti di utilizzo, Ci sono molti bot che fanno cose utili, primi tra tutti i crawler dei motori di ricerca che permettono ai siti di esser trovati facilmente dagli utenti, ma se lo scopo del bot è quello di ottenere vantaggi ingiusti o illeciti, allora si configura un reato, come andremo a vedere di seguito. Un reato molto difficile da perseguire, però.

CREDENTIAL STUFFING: L'ALTRA FACCIA DELL'ABUSO AUTOMATIZZATO

Parallelamente al fenomeno dei bot per acquisti privilegiati, un'altra pratica rilevante nell'uso dei bot è quello che viene definito **credential stuffing**: quell'attività in cui credenziali (username + password)

già compromesse vengono riutilizzate automaticamente su altri siti, grazie alla capacità dei bot di testare migliaia di combinazioni in pochi minuti.
La ragione per la quale tale strategia risulta così efficace è la persistente abitudine degli utenti a **riutilizzare le stesse credenziali** su più servizi. Quando un attaccante ottiene username/password grazie a una violazioe informatica, può lanciare un attacco automatico verso altri servizi tentando l'autenticazione con le vecchie credenziali. Se va a segno, il criminale può avere accesso a conti sensibili, dati personali o sistemi di pagamento. L'automazione di questo processo – ossia l'uso dei bot – amplifica la scala dell'attacco rendendolo economicamente vantaggioso per l'attaccante.
Dal punto di vista delle aziende, tale rischio va interpretato non solo come compromissione di account, ma anche come possibile effetto collaterale su infrastrutture legacy, credenziali mal gestite, o sistemi di registrazione poco protetti.

PRODUCT SCRAPING: COME LA CONCORRENZA CI SPIA A SPESE NOSTRE

Un altro utilizzo molto comune dei bot è quello del controllo della concorrenza. Un'azienda può creare, o pagare qualcuno per farlo, un bot che raccolga l'elenco dei prodotti della concorrenza e tenga sotto controllo i prezzi applicati per poter regolare di conseguenza i propri. Apparire nelle liste di acquisto di Google a qualche euro in meno rispetto ai concorrenti, e a volte bastano anche pochi spiccioli, garantisce un ritorno di attenzione costante e ben mirato. Inoltre, un sistema simile basato su bot permette di controbattere in tempi brevissimi alle offerte speciali dei concorrenti, limitandone l'efficacia e, anzi, sfruttando il loro marketing per guadagnare visibilità.

COSA FARE, QUINDI, CONTRO QUESTI ROBOT IN SCARPE DA TENNIS?

Abbiamo ovviamente giocato un po' con l'immagine del robot in scarpe da tennis per parlare di questo problema ancora poco conosciuto, ma dalle implicazioni molto serie. Come abbiamo visto, le implicazioni per chi fornisce servizi o prodotti online sono molteplici e tutte comportano una componente finanziaria, diretta o indiretta, che può diventare importante: dai costi per gestire il traffico in più (si stima che oltre il 70% del traffico internet oggi sia creato dai bot), alla perdita di fiducia dei clienti fino ai casi di vero e proprio spionaggio, è ovvio che sia sensato cercare una soluzione al problema.
Il rimedio più immediato è una soluzione "anti-bot", un sistema che riesce a distinguere gli utenti umani da quelli artificiali e che agisce di conseguenza. Un sistema anti-bot, per esempio, può lasciare campo libero ai bot leciti come quelli dei motori di ricerca e bloccare quelli sconosciuti o che compiono operazioni dannose. Per di più, una volta riconosciuto un bot "malevolo", si può decidere di alimentarlo con informazioni false, danneggiando i piani di spionaggio del mandante, magari portandolo a compiere azioni che gli si ritorceranno contro.
Ma se queste soluzioni costano troppo? Si ricorre a piccoli accorgimenti che bisogna discutere con chi fornisce l'infrastruttura tecnologica. Si va dall'autenticazione a due fattori per combattere il credential stuffing fino all'implementazione di captcha variabili per bloccare i bot che mirano ad acquisti indiscriminati, passando per il mascheramento di prezzi e disponibilità per trarre in inganno i bot che spiano le nostre mosse. E se facessimo finta di niente? Rischiamo di perdere dei soldi. Ne vale la pena?

La migrazione quantistica: una strategia integrale e un piano d'azione per la resilienza criptografica

Gian Fabio Palmerini, *Ciso*
Webuild

UNA ROADMAP STRATEGICA PER LA MIGRAZIONE QUANTISTICA

La transizione alla crittografia post-quantistica non è un singolo evento, ma un percorso complesso che richiede un'attenta pianificazione e un'esecuzione metodica che si estende per un decennio. La roadmap presentata si ispira al modello a tre fasi delineato dall'NCSC del Regno Unito e offre un piano d'azione chiaro per i leader aziendali.

FASE I: SCOPERTA E PIANIFICAZIONE (ENTRO IL 2028)

Questa fase iniziale è la più critica e getta le basi per l'intera migrazione.

- **Ottenere il Consenso dei Dirigenti:** La migrazione PQC non è solo un problema tecnico, ma anche un problema di gestione del cambiamento e del ciclo di vita dei sistemi. È fondamentale ottenere il supporto e la sponsorizzazione dei dirigenti per garantire il budget e l'allineamento di tutti i dipartimenti. Un modo per ottenere questo supporto è presentare la questione come una mitigazione del rischio aziendale e non solo come un aggiornamento tecnologico.
- **Conduzione di un Inventario Criptografico:** Questo è il primo passo non negoziabile. Le organizzazioni devono mappare ogni risorsa che utilizza la crittografia, identificando algoritmi, dimensioni delle chiavi, protocolli (come TLS, SSH, VPN) e metodi di gestione delle chiavi e dei certificati. Il Post-Quantum Cryptography Coalition (PQCC) ha rilasciato uno strumento pratico, il **PQC Inventory Workbook**, progettato per aiutare le organizzazioni di tutte le dimensioni a costruire un inventario centralizzato e a dare il via alla pianificazione della migrazione.
- **Esecuzione di una Valutazione del Rischio Quantistico (QRA):** Una QRA è una valutazione completa delle risorse e dei sistemi informativi di un'organizzazione per identificare le vulnerabilità specifiche alle minacce quantistiche. Tale processo si basa su un approccio standardizzato del NIST e si concentra sull'identificazione di sistemi critici e dati sensibili con la più alta esposizione, nonché sul ciclo di vita della riservatezza dei dati. L'obiettivo è stabilire una linea di base per l'intera organizzazione, consentendo di concentrarsi sulle attività ad alto impatto.

FASE II: SPERIMENTAZIONE E IMPLEMENTAZIONE PRIORITARIA (2028-2031)

Con una chiara comprensione del panorama criptografico, le organizzazioni possono passare all'implementazione.

- **Abbracciare l'Agilità Criptografica:** L'agilità crittografica (o "crypto-agility") è la capacità di un sistema di adattare e sostituire rapidamente gli algoritmi crittografici in risposta a nuove minacce. Questo è un principio di progettazione fondamentale, non un semplice aggiornamento, che consente di proteggersi dalle vulnerabilità scoperte in futuro.
- **Impegno con Fornitori e Catena di Approvvigionamento:** Un elemento critico della migrazione è l'impegno con i fornitori di tecnologia. Molti fornitori di servizi cloud, come Amazon Web Services, offrono già opzioni resistenti al quantum, ma è fondamentale che le organizzazioni collaborino proattivamente con tutti i loro fornitori per comprendere le loro roadmap e i loro piani per il supporto PQC, specialmente per le applicazioni e i dispositivi legacy.
- **Esecuzione di Prova di Concetto (PoC) e Implementazioni Ibride:** Le organizzazioni dovrebbero eseguire PoC in ambienti di laboratorio per comprendere l'impatto degli algoritmi PQC sulle prestazioni e sulla compatibilità. L'approccio ibrido, che combina algoritmi classici con algoritmi PQC, fornisce un ulteriore livello di sicurezza e funge da misura provvisoria per facilitare la transizione,

consentendo la retro-compatibilità e offrendo una difesa contro attacchi che mirano a entrambi gli algoritmi.

FASE III: MIGRAZIONE COMPLETA E AGILITÀ SOSTENUTA (2031-2035)

Questa fase si concentra sull'implementazione su larga scala e sul completamento della migrazione.

- **Sprint Finale:** L'obiettivo è completare la migrazione di tutti i sistemi, i servizi e i prodotti entro il 2035. Per le organizzazioni che non hanno iniziato la pianificazione, questo rappresenta un percorso molto più complesso e rischioso.
- **Conformità Normativa:** Rispettare le scadenze del 2035 fissate da agenzie come il NIST e l'NCSC non è solo un requisito tecnico, ma anche una necessità di conformità normativa.
- **Mantenimento di un Ecosistema Pronto per il Quantum:** La migrazione non è un evento una tantum. Le organizzazioni devono mantenere un inventario criptografico "vivo", monitorando e adattando continuamente i propri sistemi ai nuovi standard e all'evoluzione del panorama delle minacce.

CONSIDERAZIONI TECNICHE E OPERATIVE

La transizione alla crittografia post-quantistica impone considerazioni tecniche e operative che vanno oltre la semplice sostituzione degli algoritmi.
E' da tenere in considerazione l'impatto sulla rete e infrastruttura in particolare al riguardo de:

- **Larghezza di Banda e Latenza:** Gli algoritmi PQC producono generalmente chiavi più grandi e firme più lunghe rispetto ai loro predecessori classici. Ad esempio, le chiavi pubbliche di CRYSTALS-Kyber (6.000 bit) e CRYSTALS-Dilithium (10.000 bit) sono molte volte più grandi delle chiavi RSA (2.000 bit). Questo aumento delle dimensioni può gravare sulla larghezza di banda e causare un aumento della latenza, il che può avere un impatto significativo sulle applicazioni sensibili, come la voce e il video. Le organizzazioni devono valutare la loro infrastruttura di rete e considerare gli aggiornamenti per supportare questo carico aggiuntivo.
- **Archiviazione:** Le dimensioni maggiori delle chiavi si traducono in certificati PQC che richiedono più spazio di archiviazione. I sistemi di gestione dei certificati e le soluzioni di backup e ripristino dei dati dovranno essere in grado di gestire questo volume di dati aggiuntivo in modo efficiente.

Oltre a tenere conto degli aggiornamenti Software e Hardware come ad esempio:

- **TLS 1.3 come Prerequisito:** L'aggiornamento al protocollo TLS 1.3 è un passo fondamentale e non negoziabile per la prontezza quantistica. L'IETF (Internet Engineering Task Force) ha esplicitamente dichiarato che non supporterà gli algoritmi PQC nelle versioni precedenti a TLS 1.3. Oltre a essere un requisito per la PQC, TLS 1.3 offre già il Perfect Forward Secrecy (PFS) e le chiavi effimere, che aumentano la sicurezza contro i rischi attuali e futuri.
- **Moduli di Sicurezza Hardware (HSM):** Molte organizzazioni si affidano a moduli di sicurezza hardware (HSM) per proteggere le chiavi crittografiche. Per la migrazione, sarà necessario aggiornare o sostituire questi HSM con modelli che supportano i nuovi algoritmi PQC, un processo costoso ma essenziale per mantenere l'integrità del sistema.

Le organizzazioni che dipendono da fornitori di terze parti e servizi cloud devono affrontare la sfida di garantire che anche questi partner siano pronti per il quantum. È fondamentale che le aziende dialoghino con i propri fornitori per comprendere le loro roadmap PQC e per assicurarsi che siano in grado di fornire prodotti e servizi aggiornati, compresi gli aggiornamenti del firmware per dispositivi legacy.
L'assenza di un piano di migrazione chiaro da parte di un fornitore rappresenta un rischio significativo per il cliente.

PQC, QKD E QRNG

Il dibattito sulla sicurezza quantistica spesso genera confusione tra PQC e Quantum Key Distribution (QKD), portando alcuni a considerare queste tecnologie come alternative dirette. In realtà, sono soluzioni distinte che servono a scopi complementari.
La PQC è una soluzione basata su software per un problema matematico, progettata per sostituire gli algoritmi vulnerabili e funzionare sulla nostra infrastruttura Internet esistente. È scalabile, supporta firme digitali e scambio di chiavi, ed è l'unico percorso pratico per una migrazione di massa.
Al contrario, la QKD è una tecnologia basata sulla fisica che utilizza i principi della meccanica quantistica per distribuire chiavi di crittografia. Sebbene offra una sicurezza "a prova di teoria dell'informazione" (il che significa che la sua sicurezza è garantita dalle leggi della fisica e non si basa su assunzioni matematiche), presenta limitazioni significative:

- **Hardware Specializzato:** La QKD richiede hardware specializzato e nodi fidati, che non sono compatibili con l'infrastruttura esistente.
- **Limitazioni di Distanza:** Funziona su distanze limitate, tipicamente pochi chilometri nelle fibre ottiche senza l'uso di nodi fidati per il "salto di chiave".
- **Nessuna Firma Digitale:** La QKD non fornisce soluzioni per le firme digitali o l'autenticazione, richiedendo un canale classico che deve essere a sua volta protetto, spesso da algoritmi PQC.

Tabella II: PQC vs. QKD - Un'Analisi Comparativa

CARATTERISTICA	PQC (CRITTOGRAFIA POST-QUANTISTICA)	QKD (DISTRIBUZIONE DI CHIAVI QUANTISTICHE)
Principio di Sicurezza	Difficoltà computazionale di problemi matematici (reticoli, hash, ecc.)	Leggi della meccanica quantistica (non clonabilità)
Implementazione	Software e firmware, su infrastruttura esistente	Hardware specializzato (fotoni, rilevatori, ecc.)
Funzionalità	Scambio di chiavi e firme digitali	Distribuzione di chiavi simmetriche
Scalabilità	Scalabile a livello globale su Internet	Limitata dalla distanza e dalla necessità di nodi fidati
Casi d'Uso Tipici	Migrazione di massa (es. TLS, VPN), firme codice	Comunicazioni ad altissima sicurezza punto-punto (es. tra data center)

Piuttosto che competere, PQC e QKD possono complementarsi in un approccio ibrido per una sicurezza "in profondità". In questo modello, la QKD viene utilizzata per generare e distribuire chiavi di sessione simmetriche su collegamenti ultra-sicuri, mentre le firme PQC autenticano le parti e garantiscono l'integrità in un'infrastruttura scalabile. Questo approccio offre un'ulteriore garanzia, proteggendo sia da potenziali vulnerabilità matematiche nella PQC sia da attacchi di implementazione sulla QKD. Le applicazioni di QKD nel mondo reale si trovano in ambienti di alta sicurezza, come banche, governi e infrastrutture critiche, dove i requisiti di riservatezza sono massimi.
Indipendentemente dalla scelta tra PQC e QKD, la qualità della casualità è un requisito fondamentale per tutta la crittografia. I generatori di numeri casuali quantistici (QRNG) sfruttano la casualità inerente alla meccanica quantistica per produrre numeri veramente casuali. Questi generatori forniscono la base per chiavi di crittografia e firme digitali più forti, e sono un componente critico nella generazione di chiavi resistenti ai computer quantistici. Le applicazioni dei QRNG sono già diffuse in diversi settori, dai telefoni cellulari e i sistemi bancari all'IoT e alle comunicazioni satellitari, dove la generazione di chiavi robuste è la pietra angolare della sicurezza.

CONCLUSIONI: IL PERCORSO DA SEGUIRE

Il tempo per l'azione è adesso. Le scadenze fissate dalle agenzie governative non sono previsioni sulla minaccia quantistica, ma piuttosto una realistica ammissione della complessità e della durata di una migrazione completa. La PQC fornisce un percorso pratico e scalabile per mitigare questa minaccia, e i recenti standard del NIST offrono un chiaro punto di partenza. Le organizzazioni devono smettere di "aspettare e vedere" e intraprendere una serie di passi immediati e non negoziabili.
TAKEAWAY:

- **Avviare il Percorso di Migrazione con Urgenza:** Ottenere il consenso dei dirigenti e dare priorità alla sicurezza quantistica come problema di rischio aziendale.
- **Mappare il Paesaggio Criptografico:** Eseguire un inventario completo di tutti gli asset crittografici e condurre una valutazione del rischio quantistico per identificare le aree più vulnerabili.
- **Abbracciare l'Agilità Criptografica:** Costruire sistemi che possano facilmente passare da un algoritmo all'altro in caso di nuove vulnerabilità.
- **Aggiornare le Fondamenta:** Assicurarsi che i protocolli e l'infrastruttura (in particolare TLS 1.3) siano pronti a supportare i nuovi standard PQC.
- **Collaborare con i Fornitori:** Dialogare attivamente con l'intera catena di approvvigionamento per comprendere e allineare i loro piani di migrazione PQC.

La migrazione quantistica è un viaggio pluriennale che richiederà un impegno sostenuto, ma intraprendere questi passi oggi non solo proteggerà l'organizzazione dalle minacce future, ma rafforzerà anche la sua resilienza informatica complessiva nel presente.

AI: come regolamentarne l'uso da parte dei dipendenti in azienda

Giulia Rizza, *Consultant & PM*
Colin & Partners

L'ADOZIONE DELL'INTELLIGENZA ARTIFICIALE GENERATIVA STA ACCELERANDO IN MODO ESPONENZIALE ALL'INTERNO DELLE ORGANIZZAZIONI. TUTTAVIA, L'UTILIZZO SPONTANEO DI QUESTI STRUMENTI DA PARTE DEI DIPENDENTI PUÒ ESPORRE L'AZIENDA A RISCHI SIGNIFICATIVI, SOPRATTUTTO IN RELAZIONE AGLI OBBLIGHI NORMATIVI EMERGENTI.

Il quadro di riferimento oggi è rappresentato principalmente dall'**AI Act** (Regolamento del Parlamento europeo e del Consiglio che disciplina i sistemi di intelligenza artificiale), dal **GDPR** per la protezione dei dati personali, dal D.Lgs. 231/2001 sui modelli organizzativi.
La prima criticità riguarda l'uso non controllato di strumenti di AI generativa: al pari di qualsiasi altro strumento aziendale, è opportuno disciplinarne adeguatamente l'utilizzo. Ad esempio, quando un dipendente inserisce dati sensibili o aziendali in piattaforme esterne, può violare gli artt. 5, 6, 32 e 44 del GDPR, relativi ai principi di minimizzazione, base giuridica, sicurezza del trattamento e trasferimenti extra UE. Anche l'AI Act pone obblighi di trasparenza e gestione dei dati, in particolare per i sistemi classificati come ad "alto rischio". Ciò implica che le aziende non possono ignorare l'esistenza di questi strumenti: devono adottare misure di governance proporzionate ai rischi.
Per questo diventa essenziale una Policy aziendale dedicata. Tale policy dovrebbe indicare quali strumenti sono consentiti, per quali finalità e con quali cautele.
L'AI Act richiede che tutti i sistemi ad alto rischio siano utilizzati sotto un regime di risk management documentato (art. 9) e con human oversight (art. 14), mentre anche i sistemi a rischio limitato devono rispettare obblighi di trasparenza (art. 52). Una due diligence tecnologica dovrebbe verificare aspetti come le funzionalità dello strumento, gli impatti e i rischi sui diritti delle persone fisiche, il trattamento dei dati, i flussi internazionali, la conservazione dei log e il possibile riutilizzo dei prompt per addestramento.
Un altro pilastro regolatorio riguarda la classificazione dei dati. I dipendenti devono sapere quali categorie possono essere trattate tramite AI, in conformità con gli artt. 5 e 32 GDPR, e quali invece devono rimanere confinate in spazi controllati. Le aziende dovrebbero integrare la policy AI con la DPIA (Data Protection Impact Assessment – art. 35 GDPR) quando l'introduzione di sistemi di AI comporta trattamenti potenzialmente ad alto rischio.
La supervisione umana è un requisito centrale, obbligatoria per i sistemi ad alto rischio. L'AI Act ribadisce che il controllo umano non è opzionale ma parte integrante della governance dei sistemi

automatizzati. L'output generato dall'AI non può essere utilizzato senza verifica, soprattutto quando potenzialmente incide su decisioni lavorative, finanziarie o reputazionali. Anche il framework 231 può essere rilevante: una cattiva gestione dei rischi tecnologici, se collegata a possibili reati presupposto (come violazioni privacy, frodi informatiche o sicurezza informatica), può chiamare in causa la responsabilità dell'ente.
Inoltre, le imprese devono definire chiaramente ruoli e responsabilità. Molte realtà adottano un AI Governance Board, utile per garantire allineamento con gli obblighi dell'AI Act, coordinare le funzioni compliance, IT, legal e data protection, e assicurare un aggiornamento continuo delle policy.
Infine, è bene ricordare che l'**articolo 4 impone ai fornitori ed utilizzatori di sistemi di AI l'obbligo di garantire un adeguato livello di alfabetizzazione all'AI** per il personale coinvolto nell'utilizzo dei sistemi di AI nonché per qualsiasi altra persona che si occupa, per loro conto, dell'utilizzo e del funzionamento di tali sistemi. Adeguatezza che deve tenere conto di vari elementi, quali le conoscenze tecniche, esperienza, istruzione e formazione di tali soggetti; il contesto in cui i sistemi di IA devono essere utilizzati; le persone o i gruppi di persone su cui i sistemi di IA saranno utilizzati.
In sintesi, regolamentare l'uso dell'intelligenza artificiale da parte dei dipendenti non significa limitare l'innovazione, ma creare un **quadro di sicurezza conforme alle normative europee e alle best practice internazionali**. Le aziende che sapranno governare in modo proattivo questi strumenti saranno le più attrezzate per sfruttarne appieno il potenziale, evitando rischi legali e reputazionali in un contesto regolatorio sempre più rigoroso.

notes

IL CAFFÈ DIGITALE

Ricevi gli articoli degli analisti
di **TIG - The Innovation Group**
e resta aggiornato sui temi
del mercato digitale in Italia!

ISCRIVITI ALLA NEWSLETTER MENSILE!

TIG | THE INNOVATION GROUP