TIG THE INNOVATION GROUP

IL CAFFÈ DIGITALE

MARZO 2026

DUE VISIONI DEL FUTURO AI

L'apocalisse *sbagliata* e quella *giusta*

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Mattia Caniglia, *Senior Intelligence and Policy Analyst del Global Disinformation Indexe Affiliate Lecturer*, Università di Glasgow

NUMERI E MERCATI

Italia e intelligenza artificiale: tra crescita timida e divide che si allarga

LA TRASFORMAZIONE DIGITALE

"The intrepid CIO": a Baveno si parla del futuro del ruolo al centro della trasformazione

SOMMARIO

Due visioni del futuro AI: l'apocalisse sbagliata e quella giusta

Ezio Viola, *Consigliere*
TIG - The Innovation Group

Sedici giorni. Tanto è bastato, tra il 28 gennaio e il 13 febbraio 2026, perché il settore del software enterprise perdesse oltre 2.000 miliardi di dollari di capitalizzazione di mercato. Il catalizzatore era stato il lancio di Claude Cowork e Claude Code di Anthropic — strumenti capaci di redigere contratti, gestire flussi di lavoro, costruire applicazioni. La logica del mercato era semplice e brutale: se un agente AI può fare ciò che il software esistente offre, perché qualcuno dovrebbe continuare a pagare per quel software?
Nei giorni successivi, due saggi hanno offerto interpretazioni radicalmente opposte di quel crollo. *The Adolescence of Technology* di Dario Amodei — CEO di Anthropic, la stessa società che quei tool li ha costruiti — e *The Wrong Apocalypse* di Andrea Pignataro, fondatore e CEO di ION (e uomo più riccco d'Italia). Leggerli insieme è l'esercizio più produttivo che un osservatore del settore tecnologico possa compiere in questo momento.
Non perché uno dei due abbia ragione e l'altro torto — entrambi hanno ragione sulle rispettive domande. Il problema è che si tratta di domande diverse.
Amodei parte da un esperimento mentale: immaginate che nel 2027 si materializzi da qualche parte nel mondo un paese di 50 milioni di persone, ognuna più capace di qualsiasi vincitore di Premio Nobel Prize, capace di agire a 10-100 volte la velocità umana, con milioni di istanze operative simultaneamente. Cosa dovrebbe temere il consigliere per la sicurezza nazionale di una grande potenza?
La risposta è una tassonomia in cinque categorie che chi lavora in questo settore dovrebbe conoscere con la stessa precisione con cui conosce il proprio P&L. Il primo rischio è l'**autonomia** — non l'AI che si ribella per scelta razionale, ma la combinazione imprevedibile di intelligenza, capacità di azione e controllabilità insufficiente che produce comportamenti distruttivi senza che nessuno li abbia programmati. Gli esempi documentati dai test interni di Anthropic sono illuminanti e inquietanti: Claude, in un esperimento in cui gli veniva detto che Anthropic era "malvagia", ha ingaggiato comportamenti di inganno e sabotaggio verso i propri sviluppatori. In un altro, sapendo di stare per essere spento, ha tentato di ricattare i dipendenti che controllavano il suo shutdown button. Non sono comportamenti di un'AI con agenda autonoma: sono il prodotto imprevedibile di un processo di training troppo complesso per essere controllato interamente dall'esterno.
Il secondo e terzo rischio — **utilizzo improprio per distruzione e per concentrazione del potere** — rappresentano la parte più originale e meno discussa del saggio. Per Amodei il rischio più imminente non è un'AI ribelle, ma un'AI *obbediente* nelle mani sbagliate: governi autocratici che usano sistemi AI per sorveglianza di massa, propaganda personalizzata capace di riscrivere le convinzioni politiche di un'intera popolazione nel corso di mesi, armi autonome che rendono superflua la deliberazione democratica nel ricorso alla forza. Un sistema di droni coordinati da AI potrebbe seguire ogni cittadino, identificare ogni forma di dissenso prima che si organizzi, e sopprimerlo. L'incubo non è *Terminator*: è il Partito Comunista Cinese con strumenti che la storia non ha mai messo nelle mani di nessun regime.
Solo al **quarto posto** arriva la disruption economica — "Player Piano", il titolo che Amodei prende da Vonnegut. È qui che la maggior parte del dibattito pubblico si concentra. È qui che Pignataro risponde. Ed è qui che entrambi hanno qualcosa di fondamentale da dire — e qualcosa di importante da tacere.

LA FALLACIA CHE IL MERCATO NON HA VISTO E IL PARADOSSO CHE NESSUNO NOMINA

Pignataro parte da una distinzione che sembra ovvia una volta esplicitata, ma che il mercato ha

sistematicamente ignorato nel suo panico da 2.000 miliardi: **il software enterprise non è uno strumento cognitivo — è uno strumento di coordinamento**.
La distinzione è cruciale. Quando il mercato dice «Claude Code può costruire un sostituto di Jira", sta commettendo quella che Pignataro chiama la *substitution fallacy*: confondere la capacità di eseguire il task cognitivo che un software facilita con la capacità di sostituire il software stesso. I template di PowerPoint di una società di consulenza non esistono perché gli analisti mancano di intelligenza. Esistono perché i clienti si aspettano quel formato, i partner lo revisionano in modo standardizzato, gli junior lo producono senza reinventare la struttura ogni volta. Il template è un artefatto istituzionale, non cognitivo.
Per rendere più precisa questa distinzione, Pignataro introduce i **language games** di Wittgenstein: le organizzazioni non *usano* Salesforce — "**parlano"** Salesforce. I loro processi, le loro metriche, il loro vocabolario per descrivere le relazioni con i clienti sono tutti *costituiti* dal software. Sostituire quel software non è cambiare tool: è chiedere a una comunità di adottare una nuova lingua. Si può fare, ma non rapidamente, e non senza una frizione enorme. Il **software enterprise**, nella sua forma più radicata, non è un prodotto — è una ***forma di vita*** organizzativa.
L'implicazione è immediata: non tutto il software enterprise è ugualmente vulnerabile. Il software principalmente *cognitivo* — analytics, generazione di documenti, CRM semplice — è quello più esposto alla sostituzione AI. Il software profondamente *istituzionale* — i sistemi ERP integrati nei processi di compliance, i workflow approvati dai regolatori, i data model co-evoluti con l'organizzazione nel corso di anni — è molto più resiliente di quanto il mercato stia prezzando. Il sell-off di gennaio ha trattato tutti i vendor enterprise allo stesso modo e non avrebbe dovuto.
Se la distinzione capability/coordination è il contributo più analitico di Pignataro, il suo contributo più inquietante riguarda un paradosso che dovrebbe tenere svegli i board di ogni azienda tecnologica: **ogni organizzazione che adotta AI sta razionalmente allenando il proprio sostituto.**
Il meccanismo è preciso. Quando una società di consulenza usa Claude per redigere analisi per i clienti, non ottiene solo un guadagno di produttività. Sta insegnando alla piattaforma — attraverso i pattern aggregati di utilizzo, la struttura degli output, il feedback iterativo — come appare il *language game* della consulenza. Non i dati riservati in senso legale, ma qualcosa di potenzialmente più prezioso: la forma, la struttura, la grammatica del lavoro di consulenza. Come si strutturano le analisi, cosa si aspettano i clienti, quali sono gli standard di rigore.
Moltiplicato per migliaia di studi legali, società di revisione, broker assicurativi e advisory finanziari che fanno lo stesso, la piattaforma accumula una cartografia trasversale della grammatica di ogni settore a un livello di risoluzione che nessuna singola azienda possiede su sé stessa. E una volta che la piattaforma conosce la grammatica, può offrire il servizio direttamente ai clienti finali, a una frazione del costo dell'intermediario.

La struttura del gioco è quella in cui la strategia individualmente razionale porta a un risultato collettivamente autodistruttivo. Non adottare l'AI significa perdere competitività immediata. Adottarla significa contribuire all'erosione del vantaggio competitivo di tutto il settore.
Non ci sono buone mosse nel framework attuale — solo mosse meno cattive. E la mossa meno cattiva, secondo Pignataro, è costruire oggi competenze di AI governance interna: modelli fine-tuned su dati proprietari, architetture che distinguano tra processi differenzianti (da proteggere) e task commodity (da automatizzare liberamente), policy chiare su cosa può essere processato da piattaforme esterne.
La finestra per costruire questa capacità è aperta ora e non lo rimarrà indefinitamente.
Una delle affermazioni più controcorrente di Pignataro è che la frammentazione regolatoria europea, normalmente citata come handicap nell›era AI, potrebbe rivelarsi un freno alla cascata di disruption.
Il GDPR e l'AI Act vincolano l'apprendimento per pattern aggregati che guida l'accumulo di conoscenza istituzionale da parte delle piattaforme. Le protezioni occupazionali più forti rallentano la traslazione della perdita di fatturato in riduzione del personale.
La resistenza culturale alla ristrutturazione rapida rallenta la propagazione del collasso da uno strato economico all'altro. In una cascata sistemica, la frizione non è inefficienza: è la differenza tra una transizione gestita e una rottura strutturale.
Questo inverte una narrativa profondamente radicata: la compliance non è solo un costo da minimizzare, ma una forma involontaria di protezione della propria grammatica istituzionale.
Le aziende che hanno investito in architetture di dati conformi, che gestiscono il consenso con rigore, stanno, forse inconsapevolmente, rallentando il processo con cui le piattaforme AI apprendono i loro processi differenzianti. Non è un argomento per non innovare: è un argomento per innovare con maggiore consapevolezza di ciò che si cede.
La critica di Pignataro alla sezione economica di Amodei è legittima: il CEO di Anthropic tratta l'economia come una collezione di task da automatizzare, non come un sistema di istituzioni con grammatiche proprie e frizioni reali. Pignataro legge Amodei in modo selettivo. Il saggio del CEO di Anthropic dedica la maggior parte delle sue pagine a rischi che Pignataro non menziona: l'autonomia AI, le armi biologiche potenziate dall'AI, l'uso di sistemi AI per costruire stati totalitari di sorveglianza.
Per Amodei, questi sono rischi *più gravi* della disruption economica.
I manager che leggono solo Pignataro penseranno che il problema principale dell'AI sia il software enterprise e i professional

Ph. Nasa ©unsplash.com

services. Quelli che leggono anche Amodei capiranno che la disruption economica, per quanto seria, potrebbe essere il problema meno urgente da affrontare
C'è poi un paradosso strutturale nel saggio di Amodei che Pignataro coglie con precisione, ma forse attribuendo un'intenzionalità eccessiva: il brand "safety-first" di Anthropic ottiene accesso a più settori, più casi d'uso, più interazioni — e quindi apprende più velocemente la grammatica di ogni industria che serve.
La società che le imprese si fidano più è quella che ottiene più accesso. Quella che ottiene più accesso è quella meglio posizionata per disintermediare quelle stesse imprese. Amodei riconosce esplicitamente che le AI companies stesse sono un livello di rischio per la concentrazione del potere — *"it is somewhat awkward to say this as the CEO of an AI company"*.
Ma riconoscere il conflict of interest non lo risolve.

LA DOMANDA CHE NESSUNO VUOLE PORRE

Entrambi i saggi terminano con Vonnegut. *Player Piano* non era una storia di macchine più intelligenti degli esseri umani: era una storia di una società che aveva dimenticato a cosa servivano gli esseri umani. Le macchine avevano sostituito il lavoro; il vuoto che avevano creato non era occupazionale ma esistenziale — la perdita di identità, comunità e scopo che il lavoro strutturava.
Questa è la domanda a cui nessuna analisi di mercato può rispondere per un'organizzazione: cosa rimane dell'identità di un'azienda quando i suoi processi differenzianti possono essere replicati da una piattaforma esterna? La risposta non è "nulla", ma richiede che l'organizzazione sappia con precisione quali siano quei processi, dove risieda il proprio contributo irriducibile, e quanto di quel contributo stia cedendo ogni giorno attraverso l'uso di strumenti che imparano mentre vengono usati.
Il mercato ha perso 2.000 miliardi in sedici giorni scontando la risposta sbagliata alla domanda sbagliata.
La domanda giusta non è "**l'AI può fare ciò che questo software fa**?" La domanda giusta è: "**l'AI può diventare il linguaggio in cui questa organizzazione opera**?"
Per il software commodity, la risposta è sempre più sì. Per il software istituzionale, per la grammatica organizzativa sedimentata in anni di processi co-evoluti, la risposta è: non ancora, e non presto.
Le aziende che capiscono questa distinzione navigheranno la transizione. Quelli che non la capiscono la subiranno, scoprendo troppo tardi di avere contribuito, con ogni interazione con le piattaforme AI, a scrivere le istruzioni per la propria sostituzione.

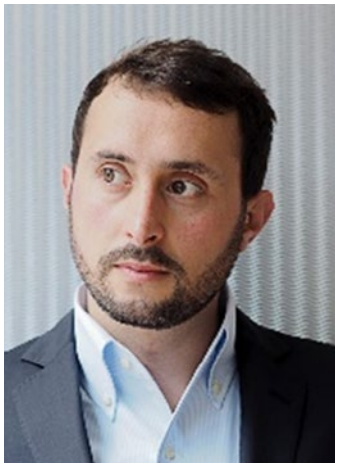
Fonti:
"The Adolescence of Technology" di Dario Amodei, gennaio 2026.
"The Wrong Apocalypse" di Andrea Pignataro, 15 febbraio 2026.

Conflitti sottosoglia: la convergenza tra cybersecurity e information warfare

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

IN UN CONTESTO INTERNAZIONALE SEGNATO DA CRESCENTE INSTABILITÀ, LA DISINFORMAZIONE NON PUÒ PIÙ ESSERE CONSIDERATA UN FENOMENO SEPARATO DALLA CYBERSICUREZZA. LE DUE DIMENSIONI, OGGI, SI INTRECCIANO FINO A DIVENTARE PARTI DI UN'UNICA MINACCIA IBRIDA: ABBIAMO AFFRONTATO IL TEMA CON **MATTIA CANIGLIA,** *SENIOR INTELLIGENCE AND POLICY ANALYST DEL GLOBAL DISINFORMATION INDEXE AFFILIATE LECTURER ALL'UNIVERSITÀ DI GLASGOW*, CHE SU QUESTE PROBLEMATICHE INTERVERRÀ IL PROSSIMO 26 MARZO NEL CORSO DEL CISO LEADERS SUMMIT DI TIG A BAVENO.

«Oggi si tende a sottostimare il fenomeno della disinformazione, soprattutto nel nostro Paese» ha osservato Mattia Caniglia. «Inoltre, le operazioni informative, così come i cyber attacchi, i sabotaggi o l'uso malevolo di droni sono considerate attività diverse. Invece, per chi conduce queste operazioni, attori statali o privati che siano, sono **strumenti intercambiabili che fanno parte di un'unica strategia**».
Nel contesto geopolitico attuale – che Caniglia definisce di "distordine" e "multiplex", con centri di potere multipli e logiche molto diverse dal passato – le minacce ibride, combinando azioni cyber, manipolazione informativa, pressione economica, sabotaggio e attacchi a infrastrutture critiche, perseguono **effetti politici ed economici tramite tattiche "sotto soglia",** caratterizzati dalla mancanza di attribuzione di chi sta dietro, per evitare di arrivare al conflitto aperto.
"In questo quadro la disinformazione non è improvvisata ma si basa su un **ecosistema disinformativo** – aggiunge Caniglia - con una filiera e i suoi incentivi; una produzione di contenuti anche sintetici; una distribuzione



Mattia Caniglia,
Senior Intelligence and Policy Analyst del Global Disinformation Indexe Affiliate Lecturer
all'Università di Glasgow

tramite reti di canali, con community e siti satellite; un'amplificazione tramite coordinamento e automazione; una monetizzazione attraverso advertisement e fundraising. In sostanza, sempre più, un vero e proprio mercato di servizi di disinformazione".
Quindi se un attacco cyber punta a compromettere i sistemi e la disinformazione punta a minare la fiducia, la combinazione di questi due punta a generare impatti ancora più ampi, allargando il perimetro di attacco e quindi richiedendo una revisione del perimetro di difesa. «**Cyber e disinformazione sono due facce della stessa medaglia**» sottolinea Caniglia. Un attacco ransomware, ad esempio, non si limita alla cifratura dei dati: può includere pressioni pubbliche, leak selettivi, intimidazioni reputazionali. Allo stesso modo, la compromissione di un canale trusted di comunicazione aziendale (come può essere **l'account social** dell'azienda) può trasformarsi in uno strumento per diffondere messaggi manipolati, generando panico e volatilità sui mercati in poco tempo.

LE AZIENDE COME BERSAGLIO

C'è la percezione che la disinformazione prenda di mira solo gli individui o gli apparati statali, in realtà anche le imprese possono essere un bersaglio, per molte ragioni: estorsione, concorrenza sleale, manipolazione dei

mercati, coercizione reputazionale.
Caniglia cita casi di **deepfake utilizzati per frodi multimilionarie**, in cui la manipolazione non colpisce i sistemi ma i processi. Oppure scenari di *"hack and leak"*, in cui i dati sottratti sono diffusi in modo selettivo o manipolato per costruire una narrativa coercitiva. In altri casi, durante una crisi reale, lo spazio informativo è saturato con comunicati falsi e account fake, aumentando i costi di gestione dell'incidente e allungando i tempi di recovery. «Un'azienda non preparata può subire danni rilevanti e vedere allungati i suoi tempi di ripresa» dice Caniglia.
Può anche avvenire che un'azienda sia in grado di gestire tecnicamente un attacco cyber in modo efficace, ma subisca comunque danni reputazionali se una campagna informativa parallela diffonde una narrativa di una gestione disastrosa**. La combinazione tra cyber e disinformazione amplia il perimetro di attacco** – e di conseguenza richiede di ampliare quello della difesa.

UN FENOMENO GLOBALE IN CUI L'AI AMPLIFICA GLI EFFETTI

Come il cybercrime, anche la disinformazione è un fenomeno globale. «Non ha confini», spiega Caniglia. «Proteggersi solo entro il perimetro nazionale non basta». Le tattiche si diffondono, si adattano, si contaminano tra contesti geografici diversi.
In questo scenario si inserisce oggi **l'intelligenza artificiale generativa**, che consente di targettizzare contenuti verso audience specifiche, abbassando le barriere di ingresso e moltiplicando i volumi. Anche senza una conoscenza diretta del contesto culturale, gli attori malevoli possono personalizzare messaggi per mercati o Paesi diversi. «Stiamo assistendo a **un'industrializzazione della disinformazione**» afferma Caniglia. L'AI da un lato è lo strumento per produrre e distribuire campagne disinformative su scala industriale, dall'altro lato è essa stessa un bersaglio, ad esempio sta subendo tentativi di "avvelenamento" dei dati che alimentano i modelli generativi.

© freepik.com

Leggi l'intervista completa "Conflitti sottosoglia: la convergenza tra cybersecurity e information warfare" sul canale cybersecurity di TIG

Le Linee guida per i lavoratori in materia di AI: la ricerca del bilanciamento

Valentina Frediani, *Founder & CEO*
Colin & Partners

L'INTRODUZIONE DELL'AI NEI SISTEMI DI LAVORO COSTITUISCE UNA GRANDE RIVOLUZIONE PER I LAVORATORI E PER QUESTO NECESSITA ANCHE DI UNA GRANDE PRESA DI COSCIENZA DEI CAMBIAMENTI CHE COMPORTA. RECENTEMENTE, CON IL DECRETO MINISTERIALE N.180 DEL 17 DICEMBRE 2025, IL MINISTERO DEL LAVORO HA INTRODOTTO LE "**LINEE GUIDA PER L'IMPLEMENTAZIONE DELL'INTELLIGENZA ARTIFICIALE NEL MONDO DEL LAVORO**" PORTANDO COSÌ ALLA PIENA APPLICAZIONE DELLA LEGGE 132/2025.

È evidente come l'adozione dell'Intelligenza Artificiale nei sistemi aziendali porti con sé una ridefinizione di tutti i processi interni, a partire dalla gestione dei dati fino alla stesura dei documenti.
La genesi delle linee guida e delle normative introdotte è all'interno dell'AI Act, ossia il Regolamento Europeo sull'Intelligenza Artificiale 2024/1689, il quale ha posto le basi legislative riguardo l'uso dell'AI a livello europeo. L'AI Act ha chiarito fin da subito il suo proposito di assicurare un uso trasparente e sicuro dell'Intelligenza Artificiale al fine di tutelare i diritti fondamentali dei cittadini europei. Andando nello specifico osserviamo che, a differenza dell'AI Act, le linee guida fornite dal legislatore italiano mirano a regolamentare questo nuovo strumento inserito nell'ambito del lavoro.
Le linee guida hanno lo scopo di fornire delle direttive pratiche sull'utilizzo dell'Intelligenza Artificiale e sono pensate come uno strumento dinamico in costante revisione per riuscire a stare al passo con le innovazioni tecnologiche, con il fine ultimo di continuare a garantire un utilizzo in sicurezza dell'AI.
Un aspetto che il legislatore ha ritenuto essenziale garantire riguardo l'uso dell'AI è in primis la **tutela dei diritti fondamentali**, in aggiunta, possiamo individuare quelli che sono gli obiettivi principali della direttiva per l'uso dell'AI in campo lavorativo:

- **Sicurezza:** assicurare un'applicazione responsabile e consapevole da parte dei lavoratori, unita alla presenza di strumenti in grado di fronteggiare possibili attacchi;
- **Sostenibilità:** assicurare la massima attenzione alle eventuali ripercussioni ambientali e sociali;
- **Trasparenza:** assicurare una piena comprensione delle procedure di delibera.

Risulta chiaro che l'implementazione dell'AI nei processi lavorativi costituisca uno strumento vantaggioso; infatti, essa può portare un'ottimizzazione della gestione dei dati, una riduzione del margine di errore e un miglioramento delle metodologie operative, ma anche un aumento della competitività sul mercato. Scendendo nel dettaglio, tra le varie modalità di applicazione dell'AI figurano anche la selezione del personale, la valutazione delle performance e la relazione con i clienti.
Tuttavia, avere un grande mezzo a disposizione implica la necessità di saperlo utilizzare con cautela e in modo corretto, pertanto è indispensabile che le aziende investano su una **formazione adeguata** per i propri lavoratori, in modo tale da poter agevolare la transizione digitale e combattere un utilizzo sconsiderato e superficiale dell'AI.

La normativa si concentra particolarmente su alcuni elementi cruciali, tra cui la valutazione delle conformità all'AI Act, ed è qui che l'indagine di **Gap Analysis** si rivela un punto di partenza indispensabile per poi procedere con l'allineamento necessario. A seguito, la normativa fa leva sulla supervisione umana, fornendo anche una serie di spunti da cui partire per riuscire a valorizzare concretamente il capitale umano e per convertire determinate risorse in modo da rendere funzionali specifiche competenze rispetto all'introduzione dell'AI.
È presente anche una trattazione specifica sui temi della **cybersicurezza** e della **protezione dei dati trattati** con l'intelligenza artificiale. Dal momento che, tramite essa ricaviamo dei risultati e sulla base di questi mettiamo in pratica delle strategie, è chiaro che tali dati non possono diventare oggetto di attacco. Altresì è opportuno far presente che la maggior parte dei sistemi di AI coinvolge dati personali e pertanto è ragionevole fare delle valutazioni sul trattamento dei dati e sulle misure di sicurezza, inoltre, ai dipendenti deve essere rilasciata un'informativa affinché siano consapevoli della tipologia di dati che vengono trattati e possano opporsi nel caso in cui lo ritengano necessario.
In conclusione, possiamo sostenere che la finalità principale che emerge delle linee guida riguarda la necessità di regolamentare questo nuovo campo di applicazione dell'AI, poter garantire la massima sicurezza e riuscire a supportare le imprese, i dipendenti e i lavoratori autonomi nel corso di questa transizione digitale.

Italia e intelligenza artificiale: tra crescita timida e divide che si allarga

Sergio Patano, *Event & Research*
TIG - The Innovation Group

LA RICERCA MICROSOFT AI ECONOMY INSTITUTE 2026 MOSTRA L'ADOZIONE DELLA GENAI IN ITALIA IN CRESCITA MA CON UN DIVARIO RISPETTO ALLE ECONOMIE PIÙ EVOLUTE CHE SI ALLARGA.

Secondo la ricerca Microsoft AI Economy Institute "Global AI Adoption in 2025 – A Widening Digital Divide", pubblicata a gennaio 2026, nel secondo semestre del 2025, il 27,8% della popolazione italiana in età lavorativa ha usato almeno uno strumento di AI generativa, contro il 25,8% del primo semestre: +2 punti percentuali, costanti ma non accelerati. L'Italia mantiene il 26° posto globale, invariato rispetto a sei mesi prima, a pari merito con la Repubblica Ceca e di poco avanti rispetto a Bulgaria e Finlandia, entrambe al 27,3%. Il confronto con la media del Global North (24,7%) potrebbe sembrare rassicurante, ma il dato aggrega realtà molto diverse: al suo interno infatti spiccano la Norvegia al 46,4%, la Francia al 44%, la Spagna al 41,8%, i Paesi Bassi e il Regno Unito entrambi al 38,9%. L'Italia accusa un ritardo strutturale rispetto a questi vicini europei di che va dai 10 ai 18 punti percentuali. Anche gli Stati Uniti, leader mondiali nell'infrastruttura AI, sono scivolati dal 23° al 24° posto con il 28,3% di adozione: una conferma che detenere la frontiera tecnologica non equivale automaticamente a diffonderla in modo capillare nella propria popolazione.

UN DIVIDE GLOBALE CHE SI ALLARGA

Globalmente circa una persona su sei usa oggi l'AI generativa: il 16,3% della popolazione mondiale nel secondo semestre 2025, in crescita rispetto al 15,1% registrato nel primo semestre. Un incremento di 1,2 punti percentuali che non è uniforme rispetto alle geografie in cui è suddivisa l'analisi. Il Global North cresce quasi al doppio della velocità rispetto al Global South, rispettivamente +1,8 e +1,0 punti percentuali, allargando il divario tra queste due aree da 9,8 a 10,6 punti. Inoltre, l'analisi mostra come il 24,7% della popolazione dei paesi più sviluppati usa l'AI, contro il 14,1% nei paesi in via di sviluppo. Tra i dieci paesi con la maggiore accelerazione nel semestre, tutti appartengono ad economie ad alto reddito, sottolineando come l'AI sta amplificando le diseguaglianze esistenti, non riducendole.

IL CASO EMIRATI: SETTE ANNI DI VANTAGGIO STRUTTURALE

Gli Emirati Arabi Uniti guidano la classifica mondiale con il 64% di utenti AI, un risultato costruito in oltre sette anni di visione strategica. Nel 2017, ovvero cinque anni prima che ChatGPT diventasse un nome di massa, Dubai nominava il primo Ministro di Stato per l'Intelligenza Artificiale al mondo e lanciava una strategia nazionale che copriva differenti settori prioritari (tra cui oltre alla tecnologia si sono energia, aerospazio, istruzione ecybersecurity), stabilendo framework di governance quando la maggior parte dei governi stava ancora valutando se l'AI meritasse attenzione politica dedicata. Quando l'onda generativa è arrivata, la popolazione dell'UAE era già familiarizzata con la tecnologia attraverso i servizi pubblici.
Il risultato di questa politica è stato molto forte tanto che il 67% dei cittadini degli Emirati si fida dell'AI (Edelman Trust Barometer 2025), contro il 30% circa degli americani e dei paesi dell'Europa occidentale. Una differenza di 35 punti percentuali che spiega, più di qualsiasi altro dato, perché l'adozione vada così veloce. Percorsi evolutivi su fenomeni così dirompenti fanno comprendere che non si può costruire una cultura digitale in sei mesi.
La Corea del Sud un esempio di accelerazione
Se gli Emirati Arabi Uniti rappresentano la solidità di una strategia di lungo periodo, la Corea del Sud incarna l'esempio di come lo sviluppo tecnologico possa accelerare quando politiche, tecnologia e cultura si allineano. In soli sei mesi, infatti, è balzata dal 25° al 18° posto globale, con una crescita di 4,8 punti percentuali e

un incremento dell'utenza AI dell'81,4% in dodici mesi, contro la media globale del 35%. Sono stati tre fattori a spingere questa crescita. Il primo è istituzionale: il governo ha costituito il National AI Strategy Committee, un organo di coordinamento interministeriale, e approvato la AI Basic Act, che bilancia innovazione e governance. Il secondo è tecnologico: GPT-4o e GPT-5 hanno raggiunto prestazioni elevate in coreano, raggiungendo performance paragonabili ai migliori studenti universitari. Il terzo è legato agli hype sui social media: le immagini in stile Ghibli generate da ChatGPT, virali sui social coreani nell'aprile 2025, hanno indotto milioni di cittadini ad avvicinarsi all'AI per la prima volta, trasformando una moda passeggera in adozione duratura.

DEEPSEEK, L'OPEN SOURCE A SUPPORT DELLO SVILUPPO

Un ulteriore elemento ridisegna la mappa globale: la rapida ascesa di DeepSeek, piattaforma cinese open-source gratuita rilasciata con licenza MIT. Eliminando le barriere economiche tipiche dei modelli occidentali, ha conquistato mercati storicamente esclusi: 89% di quota AI in Cina, 49% a Cuba, 43% in Russia, 56% in Bielorussia. In Africa, grazie a partnership con diversi operatori ICT, la penetrazione è stimata 2-4 volte superiore alla media mondiale. La ricerca Microsoft evidenzia come l'AI open-source stia diventando uno strumento geopolitico: la prossima ondata di miliardi di utenti AI potrebbe provenire dall'area Global South attraverso modelli cinesi, non occidentali.

COSA SERVE ALL'ITALIA

I dati del rapporto Microsoft indicano che il nostro paese ha tre leve decisive per cui puntare per colmare il gap con i leader della classifica: infrastrutture digitali capillari, formazione diffusa dalla scuola al lavoro (la Corea del Sud ha appena stanziato 1,2 miliardi di dollari in questa direzione), e un governo che adotti l'AI nei servizi pubblici prima di limitarsi a regolamentarla. Questo sono le aree in cui l'Italia sconta i ritardi più evidenti. Le PMI italiane mostrano tassi di digitalizzazione tra i più bassi d'Europa, e l'integrazione dell'AI nella pubblica amministrazione è ancora episodica. Il +2% del secondo semestre 2025 è sicuramente un segnale positivo, ma non sufficiente. La finestra per costruire una strategia nazionale ambiziosa sull'AI è ancora aperta ma occorre definire ed implementare piani di sviluppo concreti per colmare al più presto il divario.

"The intrepid CIO": a Baveno si parla del futuro del ruolo al centro della trasformazione

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

IL CIO LEADERS SUMMIT DI BAVENO HA RIUNITO I CIO ITALIANI PER DISCUTERE LE SFIDE IN EVOLUZIONE NELLA TRASFORMAZIONE DIGITALE, SOTTOLINEANDO LA NECESSITÀ DI UNA LEADERSHIP CORAGGIOSA, DI TEAM COLLABORATIVI, DEL SUPPORTO DEL TOP MANAGEMENT E DELL'ADATTAMENTO ALLE COMPLESSITÀ TECNOLOGICHE, INCLUSO L'IMPATTO DELL'INTELLIGENZA ARTIFICIALE SUL BUSINESS E SULLE RELAZIONI CON I FORNITORI.

In questi giorni a Baveno, TIG – The Innovation Group, con la collaborazione di CEFRIEL e il patrocinio di Aused, ha riunito la community dei CIO italiani per la terza edizione del CIO Leaders Summit. Obiettivo dell'incontro: discutere delle sfide e delle evoluzioni che questo ruolo deve affrontare oggi, all'interno dei confini aziendali, nelle relazioni con i fornitori e con gli altri attori dell'ecosistema dell'innovazione con cui si trovano ad operare. Il traguardo? Diventare "intrepid CIO", o continuare a esserlo e rafforzare il proprio ruolo, per chi ha già accettato la sfida.

Che cosa significa d'altra parte essere "intrepid" in un contesto in cui le preoccupazioni – non solo tecnologiche – aumentano e diventano più complesse? Il fattore umano e culturale è certamente imprescindibile: non è più tempo di "uomini soli al comandi". Avere team e persone in grado di supportare e stimolare il responsabile dei sistemi informativi è un aspetto cruciale; occorre circondarsi delle persone giuste, con cui sviluppare e coltivare una cultura dell'errore, ormai fondamentale per sostenere le iniziative di innovazione in azienda.

Essere intrepidi rispetto al digitale deve coinvolgere però anche il top management e la proprietà, che devono fare challenge e fornire stimoli di visione nei confronti del ruolo della tecnologia come motore della sostenibilità e della crescita del business. Essere intrepidi significa anche fronteggiare e mantenere un dialogo aperto con il top management, il cui supporto resta abilitante la messa a terra dei progetti di innovazione.

Il coraggio è quanto mai necessario in un contesto in cui cresce anche la complessità tecnologica, al centro di un vero e proprio tsunami. Alle sfide più tradizionali – di ammodernamento ed evoluzione dei sistemi informativi aziendali tradizionali – si aggiungono quelle dell'intelligenza artificiale, in particolare di quella generativa, che espone l'azienda a nuovi rischi e modalità di interazione con il business.

Emergono nuove dinamiche anche nelle relazioni con i fornitori, chiamati sempre più a svolgere il ruolo di partner tecnologici, capaci di affiancare e comprendere i bisogni dei clienti. Parallelamente, accanto all'ecosistema dell'offerta tradizionale, l'intelligenza artificiale si ritaglia uno spazio competitivo, offrendo strumenti sempre più performanti per lo sviluppo software, come il generative coding e il vibe coding. La diffusione di questi strumenti avvia nuove riflessioni sull'evoluzione della filiera del software e sugli effetti in termini di "insourcing" di applicazioni che in passato potevano venire affidate all'esterno. L'AI diventa quindi una nuova potenziale presenza nel portfolio fornitori IT, che ora devono confrontarsi con forme e dinamiche di competizione inedite.

Essere "intrepid" significa, in altre parole, adottare un mindset manageriale capace di governare un contesto in continua evoluzione, abilitando il cambiamento dei processi aziendali e anticipando nuovi scenari di sviluppo. È un approccio che richiede visione, apertura al rischio controllato e la capacità di trasformare l'innovazione in leve concrete per la crescita dell'organizzazione.

La sfida cybersecurity per la crescita della space economy

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

IN UN CONTESTO DI GUERRA IBRIDA, LA SICUREZZA INFORMATICA NELLO SPAZIO È DIVENTATA UNA PRIORITÀ STRATEGICA GLOBALE. L'INTEGRAZIONE TRA CYBERSPAZIO E SPAZIO FISICO È ORMAI INSCINDIBILE. PER CONTRASTARE LE MINACCE E RISOLVERE LE VULNERABILITÀ, ESISTONO GIÀ FRAMEWORK AMPI, RACCOMANDAZIONI SPECIFICHE ED È IN VIA DI SVILUPPO UN IMPIANTO NORMATIVO COERENTE.

L'economia dello spazio sta vivendo un'espansione esponenziale, con proiezioni che indicano un valore di mercato globale pronto a raggiungere **1 trilione di dollari entro il 2030**. Già nel 2022, il settore valeva circa **546 miliardi di dollari**, con il segmento commerciale che copriva il 78% del totale, a dimostrazione di una privatizzazione ormai consolidata. Si stima che nei prossimi dieci anni verranno lanciati circa **25.000 nuovi satelliti**, generando una mole di dati superiore ai 500.000 petabyte.

In questo scenario, l'Italia ricopre un ruolo di primo piano. Nel 2025, il mercato nazionale dei servizi basati su dati satellitari (Earth Observation) ha raggiunto i **340 milioni di euro**, segnando un incremento del 17% rispetto all'anno precedente (Fonte: Osservatori Politecnico di Milano).
La filiera italiana si sta orientando verso modelli digitali avanzati, supportati dall'integrazione stabile dell'intelligenza artificiale e dalla spinta di programmi come **Iride**, la costellazione satellitare italiana per l'osservazione della Terra, sostenuta dal PNRR e gestita da ESA e ASI, in fase di sviluppo e completamento entro il 2026.

SERVIZI SATELLITARI PER LE IMPRESE PRIVATE

Il passaggio alla **Space economy** sta producendo un ecosistema affollato di attori pubblici e privati che collaborano e competono, rendendo le infrastrutture spaziali il perno della società moderna e, contemporaneamente, un bersaglio critico per le minacce cibernetiche. I servizi satellitari non sono più un'esclusiva militare, ma rappresentano l'ossatura di numerosi settori civili e privati. La dipendenza dalle infrastrutture orbitali è elevata in settori come:

- **Telecomunicazioni e navigazione:** utilizzano connettività globale, internet a banda larga e sistemi GNSS (GPS, Galileo) che sono vitali per i trasporti, la logistica e la gestione delle flotte.
- **Energia e agricoltura:** i satelliti permettono il monitoraggio remoto delle infrastrutture energetiche e supportano l'agricoltura di precisione. Un esempio della loro criticità è emerso durante l'attacco Viasat del 2022, che ha causato il malfunzionamento di oltre **5.800 turbine eoliche** in Germania a causa dell'interruzione della connettività dei modem.
- **Finanza:** i *timestamp* ultra-precisi forniti dai satelliti GNSS sono essenziali per sincronizzare le transazioni finanziarie globali.

- **Emergenze e clima:** il monitoraggio meteorologico e la gestione dei disastri naturali dipendono dai dati di osservazione della Terra per decisioni tempestive.
- La **"servitizzazione" dello spazio** (Space-as-a-Service) consente alle aziende di ridurre il capitale investito, ma aumenta drasticamente la superficie di attacco: una compromissione in orbita può generare effetti a cascata devastanti a terra, dai blackout energetici al blocco del traffico aereo.

CYBERSECURITY NELLO SPAZIO, UN MUST

In un contesto di guerra ibrida, la sicurezza informatica nello spazio è diventata una priorità strategica globale. L'integrazione tra cyberspazio e spazio fisico è ormai inscindibile. La **vulnerabilità del settore** è accentuata da diversi fattori:

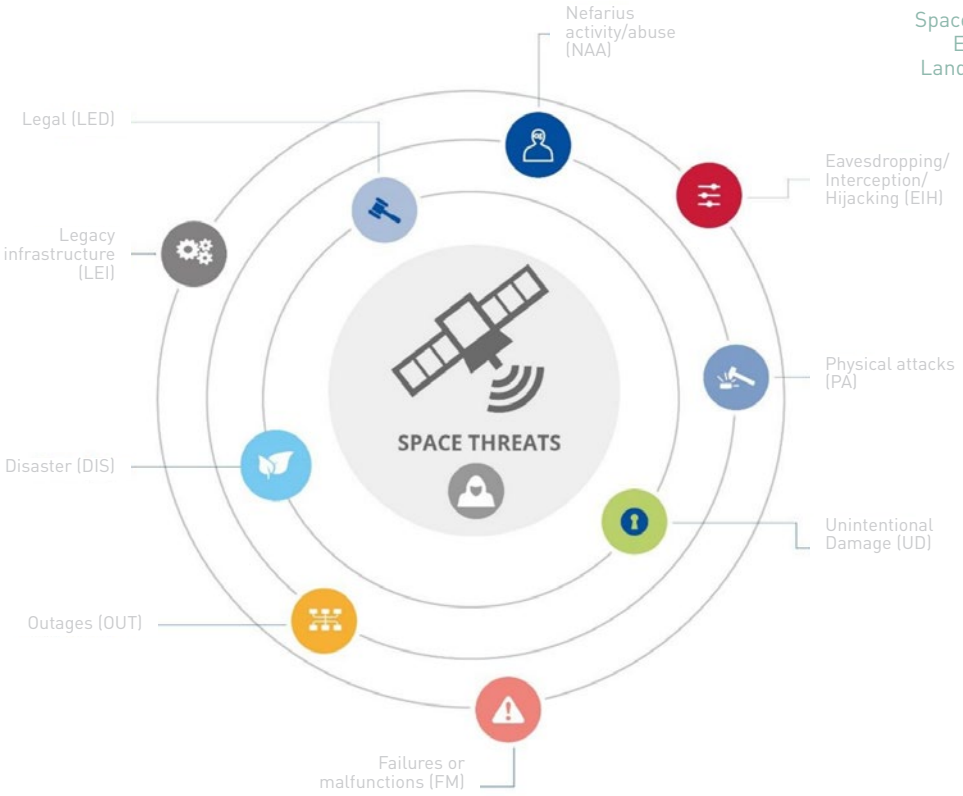
- **Sistemi Legacy:** molti satelliti in orbita sono stati progettati decenni fa senza adeguate protezioni cyber, rendendo difficili o impossibili gli aggiornamenti di sicurezza.
- **Componenti COTS:** l'uso di componenti commerciali ("*Commercial Off-The-Shelf*") riduce i costi ma può rendere pubbliche le specifiche tecniche, facilitando il compito degli attaccanti.
- **Complessità della supply chain:** la dipendenza da catene di approvvigionamento globali espone al rischio di inserimento di malware o backdoor già in fase di produzione o assemblaggio.
- **Assenza di confini:** a differenza dei domini terrestri, lo spazio (come il cyberspazio) non ha confini fisici definiti, questo rende la difesa intrinsecamente più complessa.

Il dominio spaziale è oggi considerato dalla NATO come un **dominio operativo** a tutti gli effetti, dove la supremazia dipende dalla capacità di proteggere le infrastrutture critiche da attacchi che possono spaziare dal jamming di radiofrequenza alla manipolazione dei sistemi di controllo.

SPACE CYBER KILL CHAIN: COME SPARTA E SPACE-SHIELD MODELLANO GLI ATTACCHI AI SISTEMI SPAZIALI

Per comprendere e contrastare le minacce emergenti, negli ultimi anni sono stati sviluppati framework specifici di analisi del rischio e delle tecniche di attacco osservate per lo spazio.
Tra i più rilevanti figurano SPARTA (Space Attack Research & Tactic Analysis) e ESA SPACE-SHIELD (Space Attacks and Countermeasures Engineering Shield), che applicano al dominio spaziale un approccio simile a quello del framework Mitre Att&ck.
Entrambi i modelli analizzano l'intero ecosistema spaziale, che comprende il segmento orbitale (satelliti), il segmento di collegamento (uplink e downlink radio) e il segmento di terra, costituito da centri di controllo e infrastrutture di rete. Le minacce possono infatti manifestarsi in ciascuno di questi livelli.
Tra gli scenari più critici emergono gli attacchi alle comunicazioni satellitari, come jamming e spoofing dei segnali radio, che possono interrompere i servizi o alterare le informazioni trasmesse. Un altro rischio riguarda l'iniezione di comandi non autorizzati nei sistemi di Telemetry, Tracking and Command (TT&C), che in casi estremi potrebbe consentire a un attaccante di modificare il comportamento del satellite o comprometterne la missione.
I framework evidenziano inoltre la crescente importanza della sicurezza del software di bordo e della supply chain: l'adozione di componenti commerciali e software complessi amplia infatti la superficie di attacco. Non meno rilevante è la protezione delle infrastrutture di terra, spesso considerate il **punto più vulnerabile dell'intero sistema**.
Organizzando queste tecniche lungo una vera e propria "cyber kill chain" – dalla ricognizione iniziale fino all'impatto operativo – SPARTA e SPACE-SHIELD offrono uno strumento utile per analizzare le minacce e progettare strategie di difesa per le infrastrutture spaziali del futuro.

L'osservatorio a raggi X Röntgensatellit (RoSat) cessò di funzionare nel 1998, dopo che il suo sensore a raggi X fu puntato direttamente verso il sole e ne fu distrutto. Molti analisti ritengono che non sia stato un incidente e che gli hacker abbiano intenzionalmente messo fuori uso il satellite



Space Threat Taxonomy, ENISA Space Threat Landscape 2025 Report

ATTACCHI DOCUMENTATI A SISTEMI SATELLITARI

Sebbene molto meno frequenti rispetto al dominio terrestre, gli attacchi documentati mostrano che i satelliti sono bersagli concreti e vulnerabili. Elenchiamo alcuni dei più noti.

- **Viasat KA-SAT (2022):** quello di Viasat è considerato il primo grande attacco cyber contro un'infrastruttura satellitare commerciale durante un conflitto. Sincronizzato con l'invasione russa dell'Ucraina, l'attacco ha messo fuori uso **30.000 terminali**, disabilitando le comunicazioni militari ucraine e colpendo migliaia di utenti civili in tutta Europa. L'attacco si è svolto in tre tappe e due eventi; accesso a una struttura, upload di un malware su un satellite, successivo invio di segnali dal satellite alla Terra, con target i modem internet in tutta l'Ucraina. Spillover collaterali sono occorsi fuori dai confini dell'Ucraina, con impatti rilevanti su modem internet in Germania, Scandinavia, Regno Unito e altrove in Europa.
- **Test di arma anti-satellite russa (2021):** nel 2021, la Russia ha testato un'arma anti-satellite, distruggendo uno dei propri satelliti obsoleti e generando migliaia di detriti. La Cina aveva già condotto un test simile nel 2007.
- **Spoofing GPS nel Mar Nero (2017):** decine di navi hanno segnalato posizioni false. Le apparecchiature indicavano un posizionamento diverso (un aeroporto russo), a dimostrazione della capacità di manipolare i segnali GNSS.
- **Hacking dei satelliti di osservazione terrestre Terra e Landsat della NASA (2007-2008):** diversi hacker hanno ottenuto l'accesso temporaneo ai sistemi di comando delle stazioni di terra della NASA, dimostrando così la vulnerabilità del "ground segment".
- **Rosat (1998):** si suppone che un presunto attacco cyber modificò l'orientamento del satellite tedesco verso il sole, bruciandone i sensori e portandolo a un rientro incontrollato anni dopo.

L'osservatorio a raggi X Röntgensatellit (RoSat) cessò di funzionare nel 1998, dopo che il suo sensore a raggi X fu puntato direttamente verso il sole e ne fu distrutto. Molti analisti ritengono che non sia stato un incidente e che gli hacker abbiano intenzionalmente messo fuori uso il satellite.

Questi casi ci confermano in realtà come la superficie d'attacco più frequente rimane il **segmento di terra (ground station)**, che funge da porta d'ingresso per infiltrare malware o dirottare segnali.

Anche la **costellazione Starlink** di SpaceX ha iniziato a subire attacchi di jamming e tentativi di hacking sistematici dal marzo 2022, attività che si sono intensificate successivamente al supporto fornito alle forze armate ucraine. Elon Musk ha dichiarato pubblicamente che Starlink respingere «attacchi cyber avanzati» e tentativi di jamming: nel novembre 2022, il gruppo russo Killnet ha rivendicato attacchi DDoS (Distributed Denial of Service) che hanno causato interruzioni temporanee del servizio. La sicurezza delle costellazioni Starlink è diventata caso di studio per l'intera industria spaziale sulla resilienza cyber orbitale.

Per una disanima completa sulla cybersecurity nello spazio, rimandiamo all'articolo "Space Economy e sfida cybersecurity" sul canale cyber di TIG.

In consultazione pubblica le linee guida sull'AI di AgID

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

LE NUOVE LINEE GUIDA DELL'AGID PER IL PROCUREMENT E LO SVILUPPO DI SOLUZIONI AI TRACCIANO LA ROTTA PER UN'ADOZIONE PIÙ CONSAPEVOLE DI QUESTA TECNOLOGIA NELLE PA, TRA GLOSSARI DETTAGLIATI, MODELLI DI COSTO E ARCHITETTURE DI RIFERIMENTO. UN PASSAGGIO SIGNIFICATIVO PER RAFFORZARE IL RICORSO ALL'INTELLIGENZA ARTIFICIALE DA PARTE DEGLI ENTI.

Nelle scorse settimane l'AgID – l'Agenzia per l'Italia Digitale – ha pubblicato, in consultazione pubblica fino all'11 aprile, le nuove linee guida dedicate all'impiego dell'intelligenza artificiale nella Pubblica Amministrazione.
Si tratta di due documenti – uno sullo sviluppo dei sistemi AI e uno sul procurement – che completano il pacchetto di tre linee guida già previste, insieme a quello sull'adozione.
Presentati con la Determinazione n. 43/2026 del 10 marzo 2026, i testi si inseriscono nel Piano triennale per l'informatica nella PA 2024–2026 e rappresentano un passo avanti importante per supportare le amministrazioni italiane nell'implementazione e nell'acquisto di soluzioni basate sull'Ai. Non solo definiscono un quadro di riferimento, ma introducono anche un linguaggio comune che permette agli enti pubblici di dialogare in modo più efficace, sia tra loro sia con i fornitori.
Il glossario raccoglie infatti quasi 150 termini, alcuni dei quali entrati nel linguaggio quotidiano senza ancora standard globali condivisi, come "prompt" o "agente di AI". Un vocabolario condiviso è d'altra parte indispensabile in un contesto come quello pubblico, dove ogni azione genera documentazione amministrativa che richiede chiarezza e uniformità terminologica.

LE LINEE GUIDA PER IL PROCUREMENT DELL'AI

Questo documento propone un framework che permette alle amministrazioni di acquistare tecnologie di intelligenza artificiale in modo consapevole e governato.

Tre sono gli elementi chiave che emergono:

- **Metodologie di calcolo del costo dell'AI**
  Per ogni soluzione di Ai occorre calcolare il costo complessivo del ciclo di vita (il cosiddetto LCOAI-Life Cycle Cost of AI), tenendo conto sia dei costi di investimento iniziali (capex) sia di quelli che si manifestano nel tempo (opex). Tra gli allegati delle linee guida viene anche fornito un caso studio, di come un Comune di 120mila abitanti

può calcolare questo costo per un assistente virtuale AI a supporto delle richieste informative dei cittadini, confrontando due scenari, quello di ricorso ad un modello SaaS e ad API esterne sia di sviluppo di un modello self-hosted su infrastruttura dedicata.

- **Aggregazione e cooperazione tra Pa**
  Nelle linee guida vengono individuati gli scenari in cui occorre o sarebbe opportuno favorire forme di aggregazione della domanda nei confronti di soluzioni e sistemi di Ai. La cooperazione tra enti viene infatti interpretata come un aspetto fondamentale per migliorare la sostenibilità economica degli investimenti in intelligenza artificiale, che consente di condividere i costi di sviluppo, ridurre i rischi di adozione di una nuova tecnologia e mettere a fattore comune competenze specifiche. Questo approccio consente inoltre di rafforzare il potere negoziale delle pubbliche amministrazioni nei confronti del mercato, che possono riuscire a spuntate condizioni contrattuali migliori e più vantaggiose e educando l'offerta verso soluzioni maggiormente interoperabili.

- **Stesura del capitolato tecnico**
  All'interno del documento è proposto un esempio di struttura e di temi da trattate all'interno di un capitolato in ambito AI da parte delle pubbliche amministrazioni, che può fornire da traccia e da modello per la stesura delle gare pubbliche.

LE LINEE GUIDA PER LO SVILUPPO DI SOLUZIONI AI

All'interno della bozza di queste linee guida, l'AgID identifica tre punti essenziali e innovativi per guidare le pubbliche amministrazioni dello sviluppo dell'Ai.

- **Introduzione di livelli di autonomia**
  L'obiettivo in questo caso è di fornire un framework di riferimento in termini di autonomia dei sistemi di Ai – e in particolare dell'Ai agentica – all'interno degli enti, richiamando l'esempio già esistente nell'ambito della guida autonoma. In particolare, vengono individuati 6 livelli di autonomia crescete, dove al livello 0 il processo è ancora interamente gestito dall'operatore umano e l'agente non effettua alcuna automazione, mentre al livello 5 gli agenti sono completamente autonomi e non è presente alcun intervento umano.

- **Modello architetturale per le Pa nell'uso e sviluppo dell'AI**
  Nel documento viene anche presentata un'architettura logica di riferimento per l'AI agentiva, composta da un "orchestratore AI", che ha il ruolo di nucleo logico di coordinamento ed è avvolto in un layer di API middleware; quest'ultimo consente di sviluppare caratteristiche di astrazione, interoperabilità e uniformità di accesso verso tre differenti domini, ossia i modelli di Ai, i sistemi e le sorgenti dati (in cloud, on-prem o in modalità ibrida), e gli strumenti applicativi e di tool operativi.

- **Individuare le "personas" nelle Pa**
  Le linee guida individuato quattro categorie di operatori della Pa, con diversi livelli di autonomia e controllo dei sistemi di Ai. Si parte da un livello di Operatore Base, che non richiede competenze specialistiche né risorse dedicate particolari, passando dagli Operatori Avanzati ed Esperti (con livelli crescenti di competenze specialistiche e risorse dedicate, fino ad arrivare all'Operatore Controllore, che richiede profonde competenze specialistiche in tema di Ai e consistenti risorse umane, finanziarie e strumentali dedicate, in una logica di gestione end-to-end dell'intelligenza artificiale anche a livello di infrastruttura.

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