AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Newsletter

ANNO 2026 | **n. 7/ 2026** | **luglio-agosto 2026**

Cari soci,
quest'estate lo si sente ripetere spesso: "non era così anche l'anno scorso?". Sì, era così. E probabilmente anche il prossimo anno. Ondate di calore sempre più frequenti, con temperature che restano alte anche di notte, anticicloni africani che non se ne vanno più dopo qualche giorno ma si installano per settimane. Il punto è che continuiamo a trattare tutto questo come un'emergenza stagionale da attraversare, quando è diventato il contesto operativo ordinario con cui fare i conti tutto l'anno.

Parliamo di cose concrete. Quando le temperature restano oltre i 40 gradi per più giorni consecutivi, le reti di distribuzione elettrica entrano in una zona di stress che i loro progettisti non avevano previsto. Il calore accumulato nel sottosuolo impedisce la dissipazione termica dei cavi interrati; quando le soglie di sicurezza vengono superate, scattano le protezioni automatiche, con blackout localizzati e guasti ravvicinati. Al tempo stesso, la domanda di energia impenna: ogni condizionatore acceso è un ulteriore carico su una rete già sotto pressione. Il Summer Outlook 2026 di ENTSO-E dice che l'Italia ha capacità di generazione adeguata, e va bene, ma la disponibilità complessiva di energia è un tema diverso dalla resilienza delle reti di distribuzione nei momenti di picco. E i momenti di picco, quest'estate, sono diventati la norma.

E non è solo la rete elettrica; le infrastrutture idriche subiscono pressioni crescenti: la siccità, specialmente al sud, riduce la disponibilità di acqua grezza per i potabilizzatori, mentre i consumi aumentano. Le interdipendenze tra questi sistemi producono effetti a cascata che nessuna analisi di rischio condotta in un'estate "normale" riesce ad anticipare. È qui che entra in gioco la CER, con il suo "approccio a tutti i rischi". I soggetti critici individuati dal DPCM di luglio sono tenuti, nei mesi successivi alla notifica, a valutare i rischi che possono compromettere la fornitura di servizi essenziali, e i rischi di origine naturale, inclusi quelli climatici, sono esplicitamente in perimetro, sullo stesso piano di un attacco cyber o di un sabotaggio fisico. Il problema è che molte organizzazioni non sono ancora attrezzate per farlo davvero. La valutazione del rischio climatico richiede competenze diverse da quelle tradizionali della sicurezza: modelli di scenario basati sulle proiezioni climatiche, analisi delle dipendenze infrastrutturali su scala regionale, mappatura delle soglie di rottura dei componenti critici in condizioni di stress termico prolungato.
Non basta aggiungere una riga al piano di continuità operativa. C'è poi una questione di percezione culturale da correggere. Per anni, il dibattito italiano sulla sicurezza energetica si è concentrato quasi esclusivamente sull'inverno: gas, riscaldamento, stoccaggi. L'estate era stagione di manutenzione, non di emergenza. Le infrastrutture critiche italiane sono state in gran parte progettate per un clima che non esiste più. La CER, in questo senso, arriva al momento giusto. Obbliga a trattare il rischio climatico non come un tema ambientale da delegare ad altri, ma come una variabile operativa centrale. Il caldo di queste settimane è un promemoria di ciò che dobbiamo imparare a gestire in modo strutturale. Il momento per attrezzarsi è adesso, i dieci mesi successivi alla notifica passano in fretta.
Buona estate a tutti, per quanto possibile.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Maria Beatrice Versaci
Intelligence Senior Analyst presso Hermes Bay srl. Ha conseguito una laurea magistrale in Lingue e Civiltà Orientali (Arabo) presso l'Università La Sapienza di Roma, successivamente si è specializzata in Protezione Strategica del Sistema Paese (Cyber Intelligence, Big Data e Sicurezza delle Infrastrutture Critiche) presso la Società Italiana per l'Organizzazione Internazionale (SIOI).

ATTIVITA' DELL'ASSOCIAZIONE

RINNOVO ASSOCIATIVO ANNO 2026

Il 31 dicembre 2025 è scaduto il periodo associativo. Invitiamo pertanto i signori soci a rinnovare per tempo l'iscrizione alla nostra associazione versando il relativo contributo.
La quota per il rinnovo individuale è di euro 50 e può essere versata con bonifico sul conto corrente presso Banca Intesa Business, IBAN IT17B0306909606100000114955, intestato a AIIC Associazione Italiana esperti in Infrastrutture Critiche, indicando come causale "rinnovo socio ordinario, nome e cognome, anno 2026".
Le quote e le modalità di rinnovo per i soci collettivi sono contenute nel sito AIIC www.infrastrutturecritiche.it. La nostra segreteria è a disposizione, per ogni informazione, alla mail segreteria@infrastrutturecritiche.it.

Ricordiamo agli associati che non hanno ancora rinnovato la quota: il socio rimane iscritto nel libro soci per tre mesi ma perde il diritto di partecipare alla vita sociale e il diritto di voto e viene cancellato dalle mailing list di distribuzione soci. Scaduti i tre mesi il socio decade per morosità e deve effettuare di nuovo l'iscrizione pagando anche la relativa quota una tantum.

PUBBLICAZIONE DI ARTICOLI DA PARTE DI SOCI E PARTECIPAZIONE AD EVENTI

Ricordiamo ai soci che nella pubblicazione di un articolo o di un libro **non è possibile** firmarsi qualificandosi come "Associazione Italiana esperti in Infrastrutture Critiche", in quanto solo chi ha la rappresentanza legale dell'Associazione può esprimersi a nome AIIC.
La stessa regola vale anche se si partecipa ad un evento in qualità di organizzatore, relatore o chairman.

La possibilità di pubblicare o partecipare ad eventi a nome AIIC deve essere approvata dal Consiglio Direttivo dell'Associazione su richiesta del socio che, pertanto, è pregato di contattare il CD con ragionevole anticipo.

È invece raccomandato indicare, nel proprio profilo professionale, l'appartenenza ad AIIC, Associazione Italiana esperti in Infrastrutture Critiche, in qualità di socio.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

Vi ricordiamo che il sito web www.infrastrutturecritiche.it rappresenta la **fonte ufficiale dell'Associazione Italiana esperti in Infrastrutture Critiche**: è accessibile a tutti, e contiene tutte le informazioni necessarie per un corretto svolgimento della vita associativa. Vi invitiamo a consultarlo e anche a farci pervenire le vostre osservazioni: i vostri suggerimenti sono sempre preziosi e ci aiutano a migliorare il prodotto.

COLLABORAZIONE ALLE ATTIVITA' AIIC

Si invitano tutti i soci a partecipare alle attività sociali (newsletter, webinar, ecc.) inviando articoli, segnalazioni o dando la disponibilità a tenere webinar o seminari o a partecipare alla stesura e redazione della newsletter mensile.
La mail cui scrivere è segreteria@infrastrutturecritiche.it

NEWS E AVVENIMENTI

Iran, Russia, China Target Water Systems for Sabotage
Nation-state attackers breach water systems through weak passwords, exposed PLCs, and poor segmentation — not sophisticated malware.
Nation-state threat actors continue to attack systems that regulate, distribute, and protect water, but adversary objectives in these attacks can be more complex than they might first appear.
That's according to threat intelligence provider DomainTools, which on June 25 published research concerning recent nation-state targeting of water systems as far back as 2024. The research carried particular focus on how and why cyber adversaries are going after the infrastructure.
The intersection of "cyberattacks" and "water systems" is inherently alarming, as it calls to mind "cyber Pearl Harbor" scenarios where criminals attempt to stop the flow of, or poison, a community's water supply. Causing civilian casualties is usually not a direct aim of these attacks and many modern water systems have safeguards to ensure tainted water never reaches a community's populace. That, of course, doesn't mean it can't happen, nor that cyberattacks can't have an impact on human mortality.
DomainTools' report reinforces that nation-state attacks on water systems, like all critical infrastructure, continues apace. For example, in 2025 the head of Norway's counter-intelligence agency blamed Russia for an attack on a floodgate that dumped 400 liters of water per second for four hours.
The Water-Targeting Tactics of Iran, Russia, China
The research primarily focused on attacks attributed to three countries: Iran, Russia, and China.
Iranian threat actors, such as CyberAv3ngers and other IRGC-linked groups, have been observed exploiting exposed PLCs and water control systems in countries including the US and Israel. While there was one thwarted attack in 2020 against Israel systems that could have disrupted water supply during

a heat wave, researchers described Iran's targeting overall as opportunistic and propagandistic — a vehicle to stoke public fear and media attention.
"State and state-aligned actors treat water and wastewater infrastructure as strategic pressure points. The value is primarily psychological and political rather than kinetic," researchers said. "Even limited access or brief disruptions can trigger disproportionate reactions because water is tied directly to public health, trust, and government competence."
Organizations should consider Iranian APTs high risk for smaller, internet-exposed utilities and moderate risk for mature segmented OT environments.
Compared to Iran, DomainTools said Russia-aligned actors are more willing to manipulate water control systems directly. Researchers cited an attack in Muleshoe, Texas, in January 2024 when state-backed attackers "accessed a remote industrial interface and caused a municipal water tank to overflow for roughly 30–45 minutes."
"The Cyber Army of Russia Reborn claimed responsibility, and Mandiant linked the group to Sandworm, Russia's GRU-associated destructive cyber unit," researchers said. Overall, "Russian-linked activity is more sabotage-oriented than Iranian activity. The pattern fits Moscow's broader hybrid campaign: low-cost disruptive access, public fear generation, and probing of Western infrastructure resilience."
In other words, Russia is interested in the same public fear outcomes as Iran, as well as the additional benefit of potentially gaining insight into Western infrastructure. Risk is considered high for targeting in Europe and NATO-adjacent states, as well as moderate-to-high in exposed US municipal water systems.
China's activity against water systems meanwhile centers around prolific group Volt Typhoon. CISA, the NSA, the FBI, and other agencies warned in February 2024 that Volt Typhoon had compromised critical infrastructure in the US including water and wastewater. The EPA later that year alerted more than 60,000 water and wastewater systems to the threat of the advanced persistent threat. (continua..)
https://www.darkreading.com/ics-ot-security/iran-russia-china-target-water-systems-sabotage
***DARKREADING** - Alexander Culafi, -June 29, 2026*

Il futuro dell'ACN passa dall'evoluzione del sistema: i 10 punti chiave
Il riassetto della cybersicurezza italiana non può ridursi a una contesa tra competenze civili, Difesa e intelligence. L'ACN deve evolvere senza perdere funzioni tecniche, rafforzando fiducia del mercato, prossimità alle imprese e capacità di risposta concreta alle minacce diffuse
La recente nomina ai vertici dell'**Agenzia per la cybersicurezza nazionale (ACN)** segna un punto di svolta non solo gestionale, ma profondamente strategico per il **futuro digitale del Paese**.
Dopo la stagione fondativa guidata da un **professore ordinario**, necessaria per disegnare l'architettura scientifica e normativa dell'ente, e una successiva fase di consolidamento istituzionale e amministrativo affidata a un **prefetto**, l'arrivo di un manager di chiara estrazione industriale e tecnologica come Andrea Quacivi traccia una rotta precisa.
Questa **transizione** verso una guida aziendale coincide con un vivace dibattito attorno a un possibile riassetto del comparto cyber italiano. Il rischio concreto, tuttavia, è che il confronto si polarizzi attorno a una logica di pura redistribuzione di competenze e confini di potere tra il comparto civile, il ministero della Difesa e l'intelligence.
La **cybersicurezza** moderna non può essere trattata come una torta da spartire: essa richiede un **ecosistema integrato** in cui ogni attore agisca come moltiplicatore di forza e nessuno venga indebolito. Per ispirare la nuova fase evolutiva dell'ACN, è dunque fondamentale superare i conflitti di attribuzione e guardare alle migliori pratiche internazionali, estraendone gli elementi più adatti al nostro tessuto economico e costituzionale.

Indice degli argomenti

- ACN e cybersicurezza nazionale nel confronto tra modelli
- Il modello italiano dell'ACN tra percezione e riassetto
- Cybersicurezza nazionale, NIS2 e rischio burocratico
- Compliance cyber tra rischio e sostenibilità industriale
- Il futuro dell'ACN in dieci azioni strategiche
    - Core tecnico-civile dell'ACN
    - Compliance industriale e CVCN
    - Protezione di territorio, cittadini e PMI
    - Rete territoriale dell'Agenzia
    - Cooperazione ACN, DIS e difesa
    - Comunicazione istituzionale e cultura cyber
    - Dialogo con mercato ed esperti indipendenti

ACN e cybersicurezza nazionale nel confronto tra modelli

Nel **panorama occidentale** si osserva una netta linea di demarcazione tra la filosofia continentale e l'approccio anglosassone. L'asse formato da Francia e Germania ha blindato un modello civile e iper-tecnico, rigorosamente indipendente dalle forze armate e dai servizi segreti per quanto concerne la **resilienza domestica**.

Agenzie come **l'ANSSI francese o il BSI tedesco** garantiscono la massima trasparenza con il mercato privato, poiché le aziende sanno di poter collaborare e notificare gli incidenti senza il timore che i propri log aziendali o segreti industriali vengano assorbiti da logiche di segretezza militare o di intelligence. In questi paesi, la difesa delle reti militari e le operazioni offensive sono nettamente separate e affidate a comandi specifici, quali il COMCYBER francese e il comando CIR tedesco, operanti prevalentemente in contesti internazionali o bellici.

Al contrario, il **Regno Unito** ha adottato un modello totalmente integrato e guidato dall'intelligence, in cui il **National Cyber Security Centre (NCSC)** è una branca del GCHQ, l'agenzia di spionaggio elettronico.

Sebbene questo consenta una straordinaria reattività tecnica, si tratta di un approccio difficilmente mutuabile nel contesto italiano, poiché la fusione tra supporto civile e apparati di sicurezza interna (oltre ad essere un passo indietro di anni) solleverebbe alcuni punti di attenzione, tra cui la fiducia da parte del mercato privato. Esiste però un pilastro del modello britannico da cui è possibile attingere, ovvero il programma di Active Cyber Defence.

Mentre in Italia ci siamo concentrati sul calcio e sul filtering delle partite, in UK, attraverso collaborazioni automatizzate con i provider di telecomunicazioni, lo Stato blocca le **minacce come phishing e malware** direttamente alla radice, proteggendo capillarmente cittadini e piccole e medie imprese senza intasare l'agenzia centrale.

Negli Stati Uniti, questo dualismo viene specializzato affiancando alla **CISA**, agenzia civile per la protezione delle infrastrutture commerciali, la potenza estera della **NSA** e del **Cyber Command,** i quali declassificano costantemente i dati d'intelligence per metterli a disposizione del sistema civile.

Il modello italiano dell'ACN tra percezione e riassetto

L'attuale modello italiano si ispira parzialmente alla linea transalpina, avendo originariamente istituito l'ACN proprio per separare la prima linea della **resilienza cibernetica** dalle attività propriamente informative degli apparati di intelligence. Tuttavia, l'architettura nazionale sconta ancora evidenti elementi di immaturità strutturale. Il rischio paventato da alcune ipotesi di riassetto è quello di accentrare la componente tecnico-operativa sotto stringenti regimi di segretezza e a ridosso del

comparto militare, riducendo l'ACN a una grande autorità di regolazione, vigilanza, sanzioni e produzione di carte bollate.
Un simile scenario finirebbe per **indebolire il Paese** a causa di un profondo cortocircuito tra percezione, comunicazione e politica.
All'esterno, l'Agenzia si trova oggi intrappolata in un delicato **paradosso** d'immagine: l'opinione pubblica e i media tendono spesso a metterne in discussione l'efficacia in occasione di incidenti informatici che colpiscono realtà locali o periferiche (come l'attacco ai danni degli Uffizi di Firenze), addebitandone la colpa alla struttura centrale.
Si tratta di un **fraintendimento** evidente, poiché l'ACN nasce con il mandato chiaro e circoscritto di proteggere il perimetro di sicurezza nazionale cibernetica e le infrastrutture critiche vitali per lo Stato, e non come presidio di pronto intervento per ogni singola entità del territorio. Questa distorsione dimostra che lo storytelling istituzionale è stato finora gestito in modo non ottimale, alimentando un'aspettativa errata sulle reali competenze dell'ente e lasciando l'Agenzia esposta a critiche improprie.
A questa **asimmetria comunicativa** si aggiunge il fatto che l'ente è stato talvolta percepito più per le sue eccezionali condizioni di trattamento economico e di reclutamento che per la sua effettiva vicinanza operativa al territorio, laddove strutture preesistenti come il CERT-AGID venivano vissute dagli operatori come molto più prossime alle esigenze concrete delle amministrazioni locali e del tessuto produttivo.
Inoltre, concentrarsi sulle sole faide interne non risolve il nodo della reale **sovranità digitale**. Senza una forte autonomia tecnologica e industriale, l'Italia rimarrà comunque dipendente dallo schema globale di diffusione e dalle lenti strategiche di partner esteri come la CISA statunitense.

Cybersicurezza nazionale, NIS2 e rischio burocratico

Questo quadro di tensione si riflette direttamente sul tessuto industriale. All'interno dei Consigli di Amministrazione delle aziende italiane si lamenta da tempo una crescente ed eccessiva **burocratizzazione (e ipernormazione) della sicurezza informatica**. Il rischio di questa deriva diventa evidente analizzando la genesi tecnica delle recenti determine dell'Agenzia in materia di misure di sicurezza.
Il recepimento normativo degli obblighi legati alla direttiva **NIS2** ha visto l'adozione del **Framework nazionale per la cyber security e la data protection** (sviluppato dal CINI e dal Centro di ricerca cyber della Sapienza nella sua versione del 2025), il quale a sua volta traspone l'architettura del NIST CSF 2.0 statunitense.
Sebbene il Framework nazionale nasca con un'alta valenza scientifica e di orientamento, la sua conversione pressoché testuale in obblighi regolamentari rigidi e vincolanti rappresenta, a parere di chi scrive, un cortocircuito metodologico complesso.
Un paradigma indirettamente volontaristico e flessibile, progettato come modello di maturità a cui tendere per step incrementali, viene così trasformato in **un precetto di legge sanzionabile e di fatto "binario"**. Si fissa in questo modo un'asticella talmente alta da risultare, per gran parte del tessuto produttivo e delle PMI, quasi utopistica.
La distanza da altri modelli europei appare netta: il **GDPR**, ad esempio, fonda la sua intera architettura sul principio del rischio e sulla flessibilità dell'accountability, lasciando alle singole aziende la scelta delle misure più idonee sulla base del proprio contesto, dello stato dell'arte e dei costi di implementazione.
Tra l'altro, il GDPR consente un approccio europeo più equilibrato, mentre per la NIS2 il rischio di avere in Europa livelli di sicurezza diversi, per via del differente approccio nazionale, è molto elevato e porta l'Italia ad una scelta formalmente corretta ma pressoché irrealizzabile in poco tempo.
Scegliere per la cybersecurity una via rigidamente prescrittiva, difatti, costringe i CdA a una difesa puramente formale a fini legali, allontanando l'obiettivo della sicurezza reale. (continua……)

https://www.agendadigitale.eu/sicurezza/il-futuro-dellacn-passa-dallevoluzione-del-sistema-i-10-punti-chiave/
AgendaDigitale - *Gerardo Costabile -7 lug 2026*

AI Agents Are a New Kind of Identity — and Most Organizations Aren't Ready
If you're handling AI agents like a service account or API token, consider yourself behind. AI agents need a fundamentally different approach.
COMMENTARY
I recently read an opinion piece on TechTarget by Todd Thiemann, a principal analyst at Omdia, on identity security for AI agents. It is one of the clearest articles I have read on this topic. But it also made me think about something that I want to dig into further because it's the most important factor in enterprise security right now, and it's not getting the attention it deserves: the development environment.
Thiemann makes a point that I have been making for a while now, and it's worth repeating loudly: AI agents are not just another type of nonhuman identity. They are fundamentally different. If you're still treating them like a service account or an API token, you are already behind.
A Distinction That Changes Everything
Think about every nonhuman identity you have ever had to manage. A service account. An API token. A bot. They all have one thing in common: You tell them what to do, and they do it. Consistently, predictably, and within defined boundaries.
AI agents don't work that way. They are given a goal, and they figure out how to get there. They make decisions along the way. They adapt. And they don't stop at 5 p.m. They are running while your team is asleep, touching repositories, triggering pipelines, opening pull requests, and, in some cases, merging and deploying code, all without a human watching or audit trail that tells you what happened.
That is not a variation of the service account problem; it's a fundamentally different class of risk. And it requires a fundamentally different approach to governance.
AI agents are identities. They need to be provisioned, monitored, governed, and deprovisioned just like any human or nonhuman developer identity. The difference is that they operate at a speed and scale that breaks every governance model we have built to date. That isn't a reason to treat them differently. It's a reason to govern them better.
AI agents are nonhuman identities with superhuman capabilities. That combination requires a governance approach that borrows from what we do for humans and what we do for machines, and then goes further than both.
The governance models we built for human developers assumed human speed and human judgment. The models we built for nonhuman identities assumed deterministic, bounded behavior. AI agents break both assumptions simultaneously. That's why most security tools were simply not built to see them, let alone govern them.
The SDLC Blind Spot
The research is clear: Every organization has an average of 22 distinct AI agent projects, spanning IT, legal, compliance, sales, and more. That's a lot of autonomous activity with a lot of unanswered questions about who is governing it.
And while AI agents are showing up everywhere across the enterprise, the development environment is where they are most embedded, most autonomous, and, in my view, most ungoverned right now. That is the conversation I want to have.
We need to be clear about what is really happening inside engineering teams today because there are two very different types of AI in play, and they carry very different risk profiles.

Most organizations are now in the coding-assistant phase. GitHub Copilot, Cursor, and Claude help developers write faster, suggest better code, and catch issues earlier. Humans are still in the loop. The developer writes, the AI suggests, and the developer decides. That is one risk profile, and most security teams are at least beginning to think about the implications.
Autonomous agents are a different story entirely. These agents write code, run tests, open pull requests, approve merges, and trigger pipeline deployments, sometimes without a single human reviewing what they did. Not every organization is here yet, but this is where we are heading, and it's happening faster than most security and governance teams are prepared for.
Here is what I find most striking about both scenarios: Security teams are worried about vulnerable code getting through, which is a legitimate concern. But the questions most organizations cannot answer are more fundamental: Which AI agent introduced the code? What did it have access to? Was there a human anywhere in that loop? The code is the symptom. The ungoverned AI identity behind it is the cause. And without knowing the cause, you are patching symptoms forever.
The gap is not just about malicious activity. In most environments we look at, what we find is not malicious. It's just ungoverned, and being ungoverned is the risk. (continua…)
https://www.darkreading.com/identity-access-management-security/ai-agents-new-kind-identity-most-organizations-not-ready
DARKREADING *- Mora Gozani, -July 9, 2026*

Passwork, il password manager europeo con radici russe che preoccupa gli esperti
Un'inchiesta di Occrp ricostruisce i legami tecnici tra il password manager commercializzato in Europa e l'omonimo prodotto russo certificato da Fstec e Fsb. Non sono emerse prove di violazioni, codici malevoli o accessi ai dati dei clienti. Ma il passaggio degli aggiornamenti attraverso una società degli Emirati, gestita da uno dei fondatori russi, apre una questione di trasparenza e sicurezza della catena di fornitura
Passwork si presenta come un password manager europeo, con sede in Spagna e clienti tra amministrazioni pubbliche, università e grandi aziende. Ma un'inchiesta di Organized Crime and Corruption Reporting Project ricostruisce una storia più complessa: il software nasce in Russia, condivide ancora elementi tecnici con una versione certificata dalle autorità di Mosca e riceve aggiornamenti attraverso una società degli Emirati legata a uno dei fondatori originari. Non ci sono prove di violazioni o codici malevoli. Restano però aperte domande sulla trasparenza della filiera e sul controllo effettivo di un prodotto che custodisce alcune delle credenziali più sensibili delle organizzazioni che lo utilizzano.
Dalla Russia alla Finlandia, passando per gli Emirati
Il software Passwork venne sviluppato nel 2014 ad Arkhangelsk, città portuale della Russia settentrionale, dai programmatori **Ilya Garakh** e **Andrey Pyankov**. Nel 2017 l'attività europea fu trasferita in Finlandia attraverso Passwork Oy, partecipata dai due fondatori russi e dall'imprenditore finlandese **Pekka Viljakainen**.
Dopo l'invasione russa dell'Ucraina, la struttura societaria cominciò a cambiare. Garakh e Pyankov cedettero le proprie quote nella società finlandese nel maggio 2022. Due mesi dopo venne costituita negli Emirati Arabi Uniti Passwork FZ-LLC, con Pyankov indicato nei registri locali come manager. Nello stesso anno i due fondatori aprirono in Russia Passwork Llc, società che utilizza lo stesso marchio e che presenta tra i propri clienti anche aziende russe del comparto missilistico e spaziale sottoposte a sanzioni occidentali.
La società finlandese fu liquidata nel 2024. Nell'agosto dello stesso anno **Alexander Muntyan** registrò a Barcellona Passwork Europe S.L., di cui è amministratore delegato e unico azionista. Muntyan sostiene

di avere acquistato dalla società emiratina i diritti necessari per sviluppare, distribuire e assistere la versione internazionale del programma.
Il passaggio, però, non è ancora concluso. In una dichiarazione sulla trasparenza pubblicata dopo le domande dei giornalisti, la stessa Passwork Europe ha confermato che fino al 30 agosto 2026 la società degli Emirati continuerà a fornire aggiornamenti del codice sorgente e trasferimento di competenze tecniche. L'azienda spagnola definisce l'accordo una normale fase transitoria nell'acquisizione di un prodotto software già operativo.
Il punto sollevato dall'inchiesta riguarda proprio la natura di questo ponte emiratino. I beneficiari effettivi della società non sono pubblicamente identificabili, mentre uno dei fondatori russi figura come manager e l'altro è collegato al relativo dominio internet. Occrp non è riuscita a stabilire con certezza chi controlli materialmente la produzione e la distribuzione degli aggiornamenti.
Due prodotti ancora molto simili
La società spagnola nega qualsiasi legame societario, amministrativo o commerciale con Passwork Llc, l'impresa che opera sul mercato russo. Muntyan ha dichiarato che le due aziende non condividono clienti, server, sistemi di assistenza, registri, accessi amministrativi o ambienti informatici.
Passwork Europe riconosce, però, che le due versioni derivano dallo stesso codice originario. Questa eredità, secondo l'azienda, spiegherebbe le somiglianze riscontrate dai giornalisti: manuali pressoché identici, funzionalità sovrapponibili e aggiornamenti pubblicati con tempistiche molto vicine.
Il 6 aprile 2026, per esempio, il sito russo annunciò la versione 7.6. Il giorno seguente, il sito europeo presentò la stessa versione con una descrizione quasi identica delle nuove funzionalità. Gli esperti consultati da Occrp hanno inoltre individuato centinaia di righe sostanzialmente uguali negli script utilizzati per installare il programma. Il ricercatore **Lukasz Olejnik** ha descritto la separazione tecnica tra le due versioni come ancora poco profonda e meritevole di una verifica più accurata. (continua…)
https://formiche.net/2026/07/passwork-radici-russe/#content
***FORMICHE** - Mario Bentivoglio - 18/07/2026*

Kimi K3: l'AI cinese che mette alla prova prezzi, chip e sovranità dell'occidente
Moonshot AI presenta Kimi K3, modello multimodale da 2,8 trilioni di parametri annunciato come open-weight. Il sistema avvicina la Cina alla fascia alta dell'AI globale, ma restano da verificare licenza, costi reali, benchmark, requisiti hardware e impatto regolatorio
Moonshot AI ha presentato Kimi K3, un modello multimodale da 2,8 trilioni di parametri progettato per la programmazione di lunga durata, il ragionamento e l'automazione del lavoro intellettuale.
L'azienda cinese lo descrive come **il primo modello aperto** della classe dei tre trilioni di parametri e ha annunciato la pubblicazione dei pesi entro il 27 luglio 2026. Al momento del lancio, tuttavia, K3 è utilizzabile attraverso Kimi.com, Kimi Work, Kimi Code e le API dell'azienda. La sua effettiva natura open-weight potrà essere valutata soltanto quando saranno disponibili licenza, file e documentazione tecnica completa.
Indice degli argomenti

- Kimi K3 e modelli open-weight cinesi nella competizione globale
- La scala di Kimi K3 tra sparsità e inferenza efficiente
  - Finestra contestuale e conversazioni multi-turn
- Prestazioni di frontiera e limiti dei confronti su Kimi K3
  - Casi di studio scelti da Moonshot
- Modelli open-weight cinesi e pressione sul mercato dell'AI
  - Costi API, caching e infrastruttura

- Stati Uniti, chip e vantaggio tecnologico davanti a Kimi K3
- Europa, Kimi K3 e sovranità operativa nell'AI
- Bibliografia

Kimi K3 e modelli open-weight cinesi nella competizione globale

La notizia non riguarda semplicemente la costruzione di un sistema più grande. Kimi K3 segnala che il divario tra i laboratori cinesi e i leader statunitensi non può più essere descritto come un ritardo stabile di diversi mesi.

Lo Stanford AI Index 2026 documenta una distanza ormai ridotta nelle prestazioni. A marzo, il migliore modello statunitense conservava un vantaggio del 2,7 per cento sul migliore sistema cinese, mentre dal 2025 i due Paesi si erano alternati più volte al vertice. Gli Stati Uniti mantengono una netta superiorità negli investimenti privati, nella capacità dei data center e nel numero di modelli di rilievo, ma il primato tecnico dei singoli prodotti è diventato più contenuto e intermittente.

La scala di Kimi K3 tra sparsità e inferenza efficiente

K3 utilizza un'**architettura Mixture of Experts**. I 2,8 trilioni di parametri rappresentano la dimensione complessiva del sistema, ma soltanto 16 dei 896 esperti vengono attivati per ciascun token. Questa selezione riduce il calcolo necessario rispetto a un modello denso della stessa scala. Moonshot combina Stable LatentMoE con Kimi Delta Attention, un meccanismo ibrido di attenzione lineare, e con Attention Residuals, una tecnica che permette agli strati di recuperare in modo selettivo le rappresentazioni precedenti invece di accumularle uniformemente.

Secondo l'azienda, queste soluzioni migliorano di circa **2,5 volte** l'efficienza di scaling rispetto a Kimi K2. Si tratta ancora di una stima interna, non verificabile in modo indipendente finché non saranno pubblicati dati completi sull'addestramento, sul calcolo impiegato e sulla composizione dei dataset.

La documentazione cita anche Quantile Balancing, Per-Head Muon, SiTU e Gated Multi-Head Latent Attention. K3 sarebbe inoltre stato sottoposto ad addestramento **quantization-aware** già dalla fase di supervised fine-tuning, con pesi MXFP4 e attivazioni MXFP8. Queste scelte puntano a rendere più efficiente l'inferenza di un sistema le cui dimensioni restano comunque proibitive per la maggior parte delle organizzazioni.

Finestra contestuale e conversazioni multi-turn

La finestra contestuale dichiarata raggiunge **un milione di token**, sufficiente a contenere vaste raccolte documentali o grandi basi di codice. Una capacità nominale così ampia non dimostra, però, che il sistema sappia recuperare con la stessa precisione ogni informazione presente nella sequenza. Moonshot segnala inoltre che la cronologia del ragionamento deve essere conservata integralmente nelle conversazioni successive. Nelle conversazioni multi-turn e nelle chiamate agli strumenti, la documentazione API richiede di reinviare senza modifiche l'intero messaggio dell'assistente, non soltanto il contenuto della risposta finale.

Prestazioni di frontiera e limiti dei confronti su Kimi K3

Moonshot riconosce che le prestazioni complessive di K3 restano inferiori a quelle di Claude Fable 5 e GPT-5.6 Sol, pur dichiarando risultati competitivi nella programmazione, nell'uso di strumenti e nel lavoro professionale. Artificial Analysis gli assegna **57 punti** nel proprio Intelligence Index, una valutazione comparabile a GPT-5.5 e Claude Opus 4.8, ma inferiore ai sistemi più avanzati presenti nella stessa classifica.

I benchmark non permettono comunque di decretare un vincitore generale. Moonshot ha utilizzato, a seconda della prova, ambienti agentici differenti come Kimi Code, Claude Code e Codex. Alcuni punteggi dei concorrenti provengono da valutazioni esterne, altri da test condotti direttamente dall'azienda. **Budget di ragionamento**, strumenti disponibili, configurazione dell'hardware e criteri di completamento possono modificare sensibilmente il risultato. (continua…)

https://www.agendadigitale.eu/mercati-digitali/kimi-k3-lai-cinese-che-mette-alla-prova-prezzi-chip-e-sovranita-delloccidente/
Agenda Digitale - *Giovanni Masi - 20 lug 2026*

Dutch Intelligence Warns Russia Uses Hacked IP Cameras for Military Espionage
Dutch intelligence says Russia hacks IP cameras to monitor NATO military logistics and weapons shipments to Ukraine.
The Netherlands' AIVD and MIVD, the civilian and military intelligence services, published a joint advisory on July 10 confirming that at least one Russian intelligence service is systematically compromising internet-connected IP cameras across the Netherlands, other EU and NATO member states, and Ukraine to collect military intelligence.
The operation is ongoing. The advisory is based on intelligence gathered by both services and covers a campaign that has escalated since Russia's full-scale invasion of Ukraine.
The immediate military application in Ukraine is the most direct part of the finding.
"The information obtained by the Russian state actor via digital espionage operations targeting IP cameras provides insight into relevant military data, such as EU and NATO military transport routes and weapon deliveries to Ukraine. The Russian state actor uses image recognition software to conduct targeted searches for military vehicles and the military cargo they are transporting. In some cases, the access to IP cameras gained by the Russian state actor in Ukraine is used to identify the locations of Ukrainian military personnel." reads the advisory. "Intelligence reveals that this information is subsequently used to neutralise Ukrainian military personnel and military materiel in use by the Ukrainian armed forces. Furthermore, the Dutch services have determined that the Russian service is using the access to IP cameras to acquire relevant military intelligence in EU and NATO member states, including information that is not directly relevant to the war in Ukraine."
A roadside camera or a business camera overlooking a loading area becomes a targeting asset. That's the direct line from a default password left unchanged to a strike on Ukrainian forces.
The surveillance operation in EU and NATO member states serves a different but related purpose.
"Furthermore, the Dutch services have determined that the Russian service is using the access to IP cameras to acquire relevant military intelligence in EU and NATO member states, including information that is not directly relevant to the war in Ukraine." confirms the advisory. "To date, the Dutch services have not observed the Russian state actor using such information for military attacks outside Ukraine."
The intelligence collected includes EU and NATO military transport routes and weapons deliveries bound for Kyiv. The Dutch services separately confirmed they caught a small number of cameras breached directly on military logistics routes inside the Netherlands, and warned the organizations running them so they could act.(continua…)
https://securityaffairs.com/195708/intelligence/dutch-intelligence-warns-russia-uses-hacked-ip-cameras-for-military-espionage.html
Security Affairs -*Pierluigi Paganini - July 20, 2026*

Data center in Italia, la guida completa: quanti, quali e dove sono
Data center, tutti li cercano, tutti li vogliono. Ma dove sono, in Italia? E quanti sono? Soprattutto, quanto consumano, costano e come funzionano? Ecco tutto quello che bisogna sapere su queste **infrastrutture fondamentali per lo sviluppo e l'innovazione del Paese**, ma spesso poco conosciute e a volte contrastate.
Abbiamo fatto un'indagine per fare chiarezza su un mercato la cui rilevanza, economica (investimenti) e sociale (impatto sui territori), è in forte crescita, anche in Italia.

La fonte principale della seguente analisi è **Data Center Map**, un'organizzazione alla quale molti operatori del mercato segnalano i propri DC attivi, in corso di realizzazione e in programmazione, ricevendo in cambio l'opportunità di proporre i propri servizi a chi visita il sito.
I dati, forniti ad Agendadigitale.eu dal fondatore Sune Christesen, sono aggiornati a maggio 2026.
Indice degli argomenti

- Quanti sono i data center in Italia
- Dove si trovano i Data center in Italia
- Tipologie di data center in Italia
  - Colocation, soprattutto "neutra"
  - La variante "schierata": colocation delle Telco
  - Hyperscale
  - Svolta tecnica nell'evoluzione dell'offerta hyperscale: come gestire i servizi AI
  - Edge data center e infrastrutture della pubblica amministrazione locale
  - Cable Landing Station (CLS) e Digital Hub
  - High Performance Computing e ricerca
  - Centri Elaborazione Dati (CED) tradizionali
  - Gli altri data center
- Quadro sinottico degli operatori e infrastrutture identificati
- La linea di sviluppo "in grande": le gigafactory in Italia e cosa le frena davvero
- La linea di evoluzione "in piccolo": l'Edge per capillarità e sovranità, e il bivio dei CED

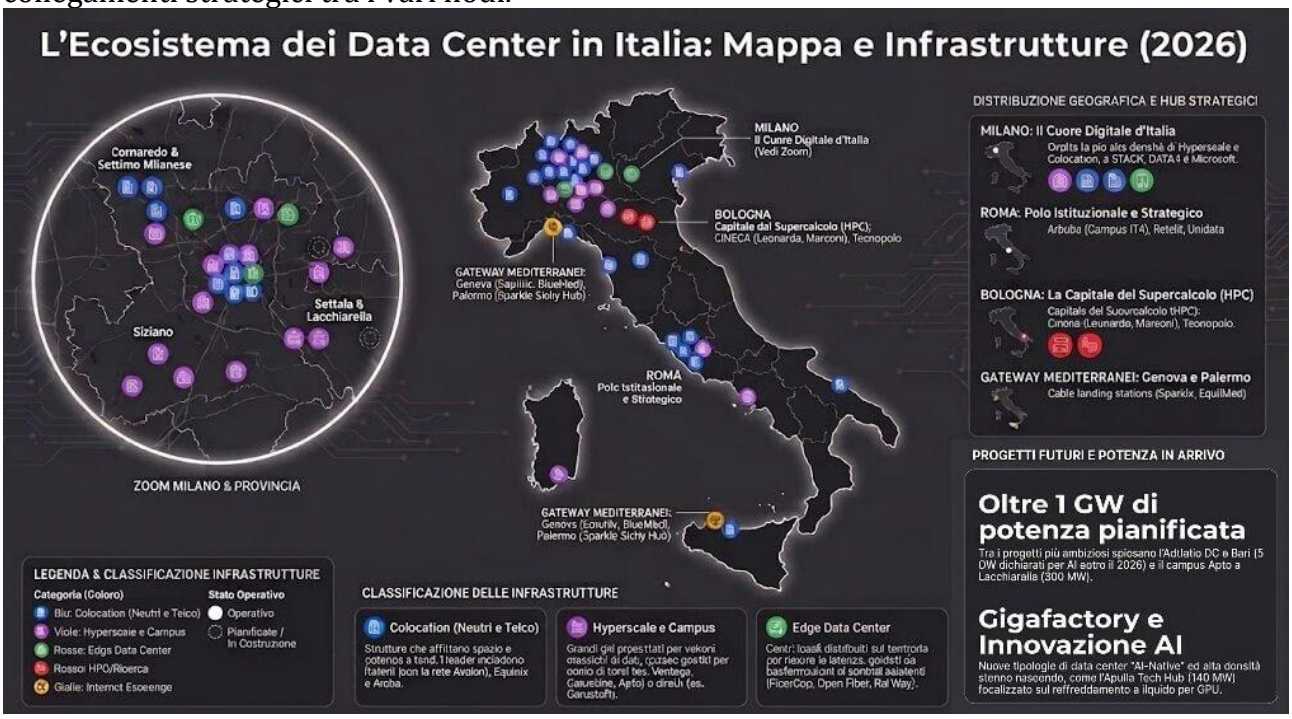
Quanti sono i data center in Italia
In Italia ci sono circa **250 impianti** (*Facility*).
Tra questi 250 impianti circa, secondo Data Center Map, circa 190 sono attivi (*Operational*), 20 in costruzione e **più di 30 "previsti"** (*Planned*). Tra questi, quelli che dichiarano una potenza obiettivo citano valori molto superiori alla media attuale, da 50 MW IT a 120-140 per impianto, fino a 240 per un campus di 5 moduli da 48 MW ciascuno. Basterebbero questi "previsti" a dimostrare che il mercato italiano attuale è **in crescita forte ma incerto**: alcuni sono verosimilmente solo annunciati, in attesa di autorizzazioni e forniture di elettricità che potrebbero non venire mai o… non trovare più nessuno ad aspettarle, quando arriveranno! Alcuni sono intestati a costruttori che non gestiscono le infrastrutture ma le cedono ad altri operatori appena pronte e che, per questi progetti, non sono ancora disposti a nominare i propri clienti; riserbo o incertezza?
Quanto è rappresentativa, se non completa, Data Center Map? **Copre in maniera adeguata i data center sul mercato**, quelli che offrono a vario titolo servizi a pagamento, mentre **ignora i data center ad uso esclusivo di una singola organizzazione**. Questa categoria, la forma tradizionale dei Centri di Elaborazione Dati (CED) negli scorsi decenni, ancora oggi conta **migliaia di siti** pubblici e privati, tutti fuori da inventari come Data Center Map. In questo paragrafo ci concentriamo su quelli di mercato; dei CED descriveremo le prospettive, e il bivio di fronte al quale l'evoluzione del mercato li pone.
Abbiamo considerato anche alcune decine di altri data center non citati da Data Center Map – presumibilmente perché meno interessati a comparirvi. Alcuni sono del tutto confrontabili a quelli citati, mentre la maggior parte appartiene a una categoria piccola ma significativa per il ruolo che sta cominciando a giocare su due temi già oggi chiave, sui quali si orienterà gran parte del futuro del settore: **edge computing** e **sovranità digitale**.
Si tratta di molti delle decine di data center che servono **pubbliche amministrazioni locali** gestiti dai membri di **Assinter**, l'associazione degli in-house di servizi informatici e di acquisto delle diverse regioni, o di ambiti territoriali più specifici. La **razionalizzazione delle infrastrutture digitali della**

pubblica amministrazione avviata da AgID alla fine degli anni Dieci e culminata in Polo Strategico Nazionale pone tutte queste infrastrutture e i loro gestori di fronte a un bivio: rimanere CED tradizionali, perdere tutti i dati "critici" oltre a quelli "strategici", svuotarsi e venire progressivamente dismessi, oppure trasformarsi in erogatori di **servizi infrastrutturali Edge sovrani italiani**, magari federandosi e collaborando con Polo Strategico Nazionale da una parte, e dall'altra sviluppando ulteriormente la collaborazione con grandi operatori cloud globali e sovrani europei privati.

Dove si trovano i Data center in Italia

In questa sezione, analizziamo la mappa dei data center per capire, anche graficamente, come sono distribuiti in tutta Italia.

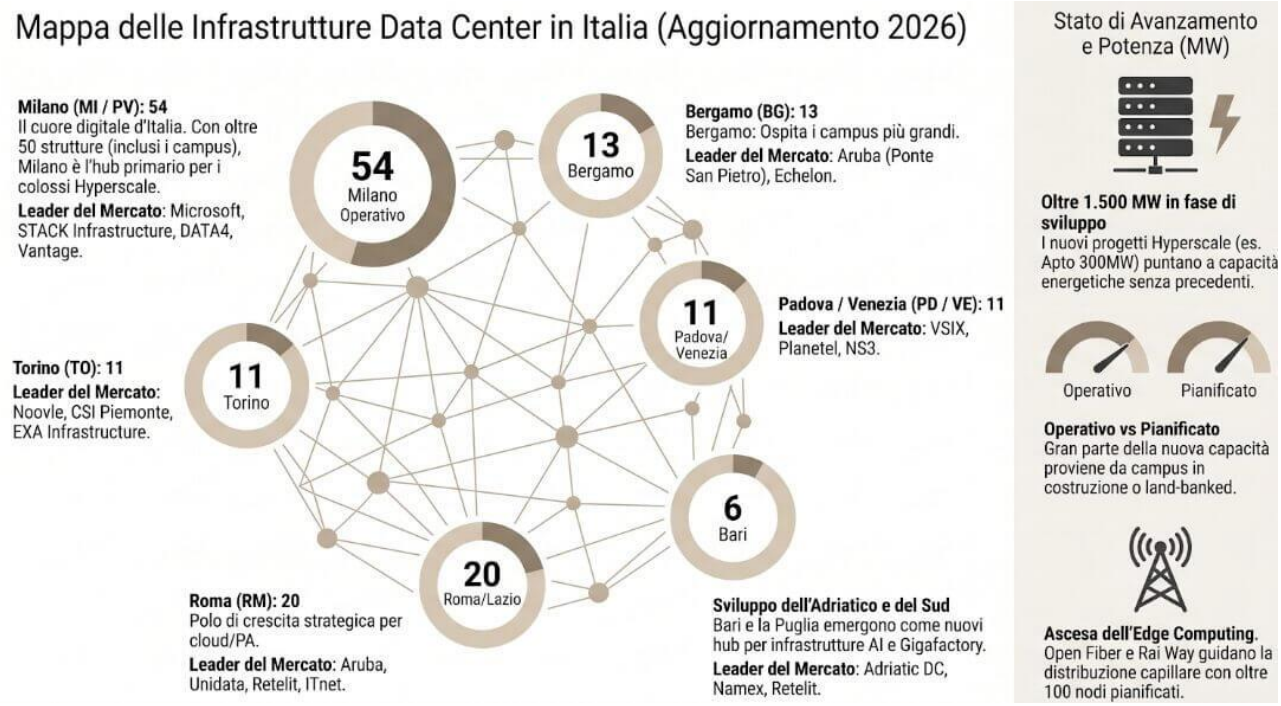
Per seguire meglio lo sviluppo della rete sopra illustrata, l'immagine riportata di seguito mostra i collegamenti strategici tra i vari nodi.



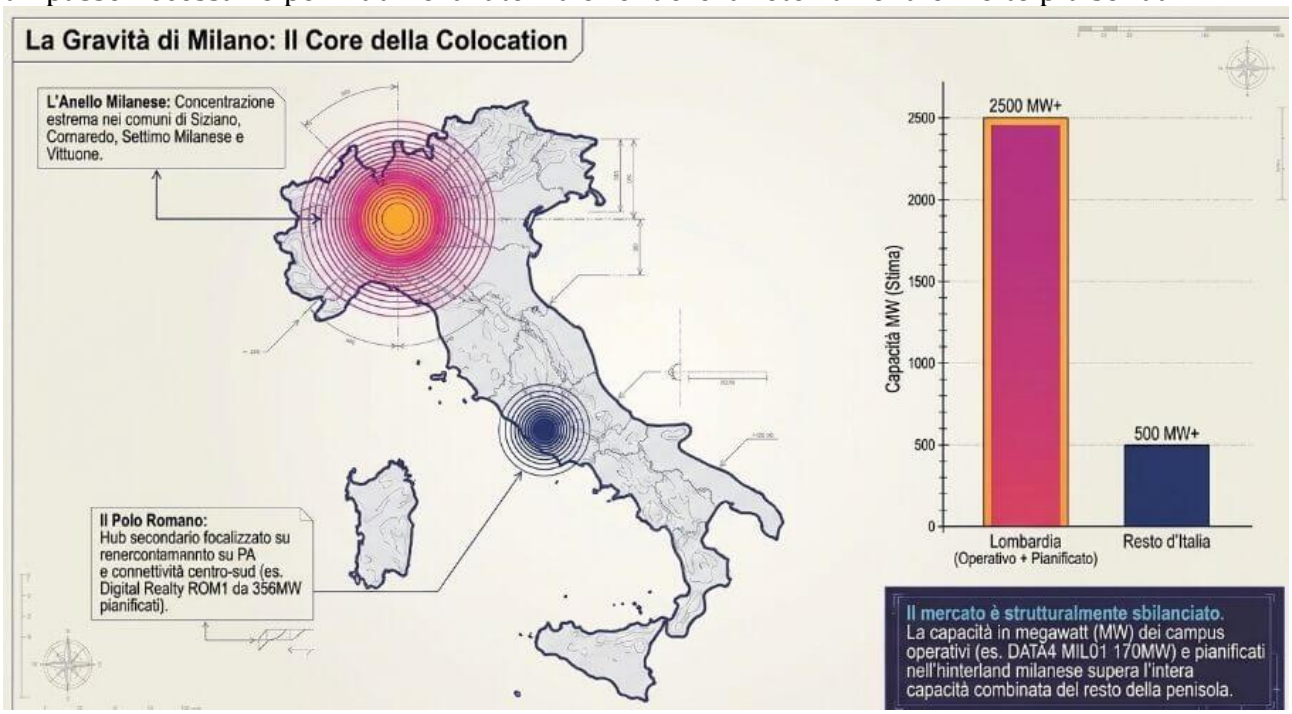
La crescita dei data center in Italia nel 2026 è davvero incredibile. La prima immagine mostra chiaramente come il nostro Paese stia diventando un punto di riferimento strategico per tutta l'Europa meridionale.

Vediamo, quindi, più nel dettaglio come si distribuiscono sul territorio.

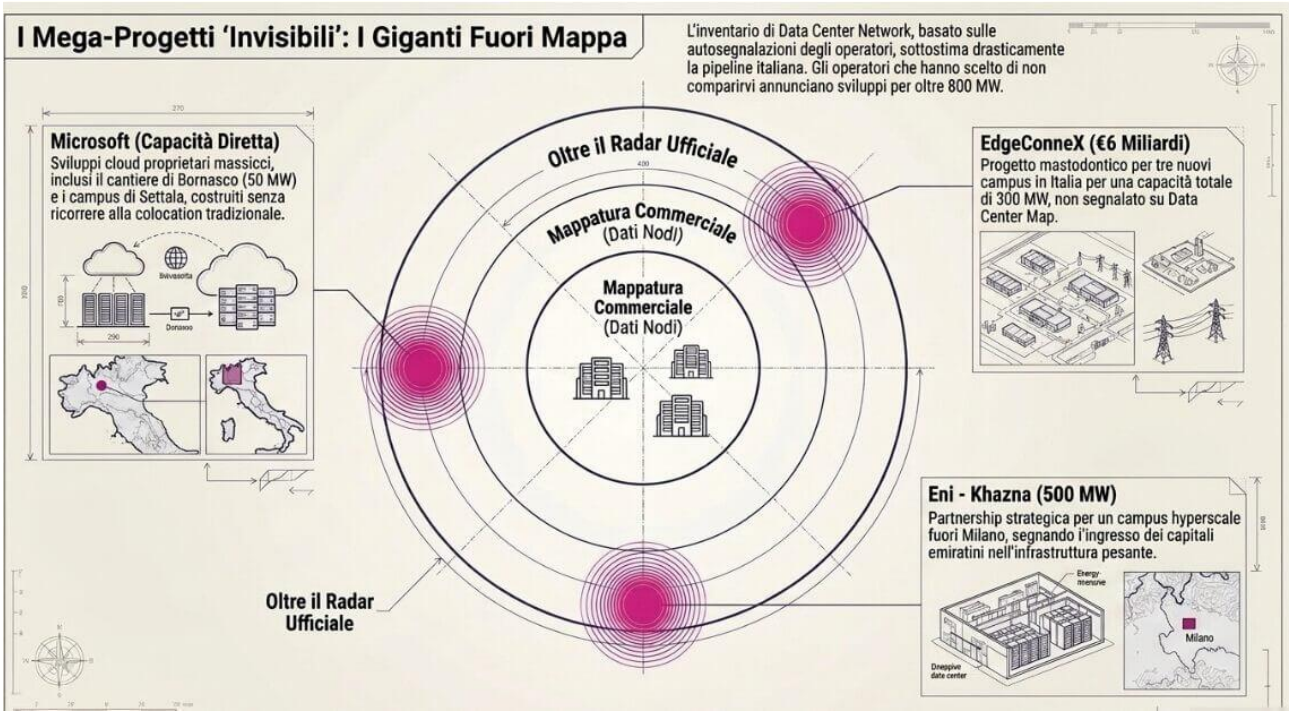
AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it



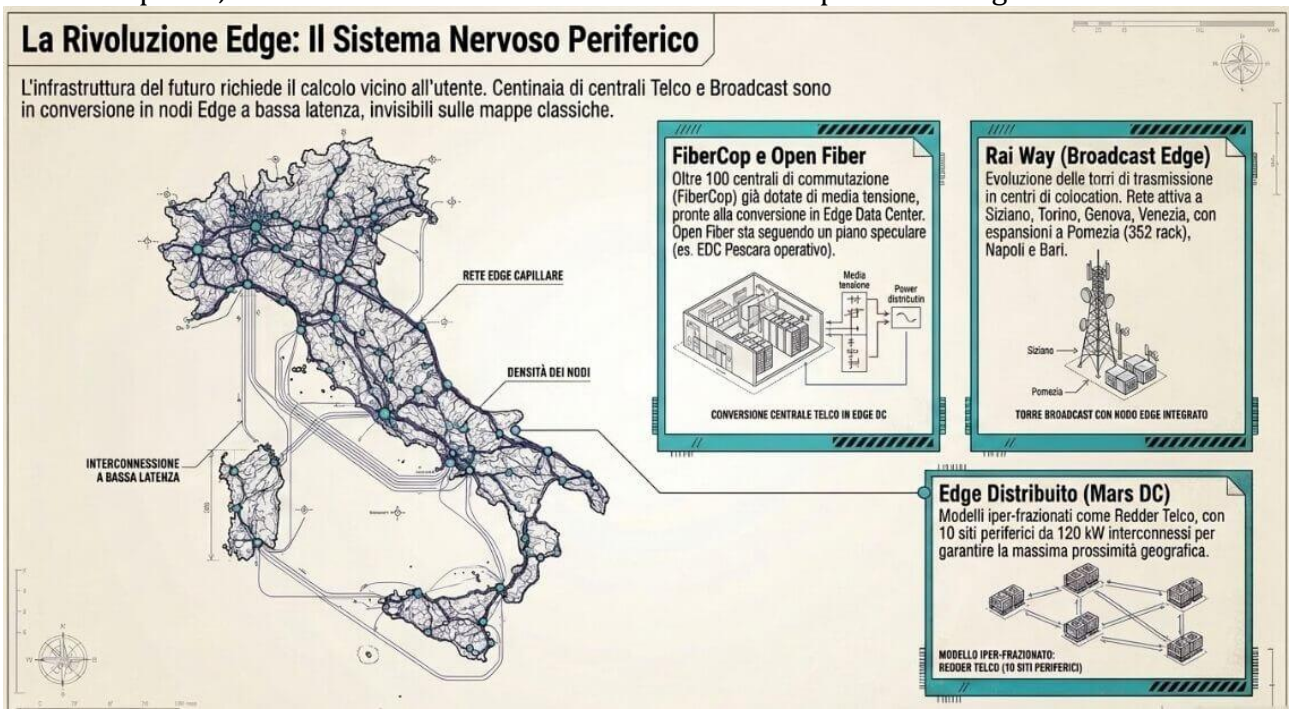
Non sorprende che la Lombardia, soprattutto l'area di Milano, sia il vero cuore pulsante del settore. Ma le cose stanno cambiando: stiamo assistendo a una progressiva diffusione verso nuove zone strategiche, un passo necessario per ridurre la latenza e rendere la rete nazionale molto più solida.



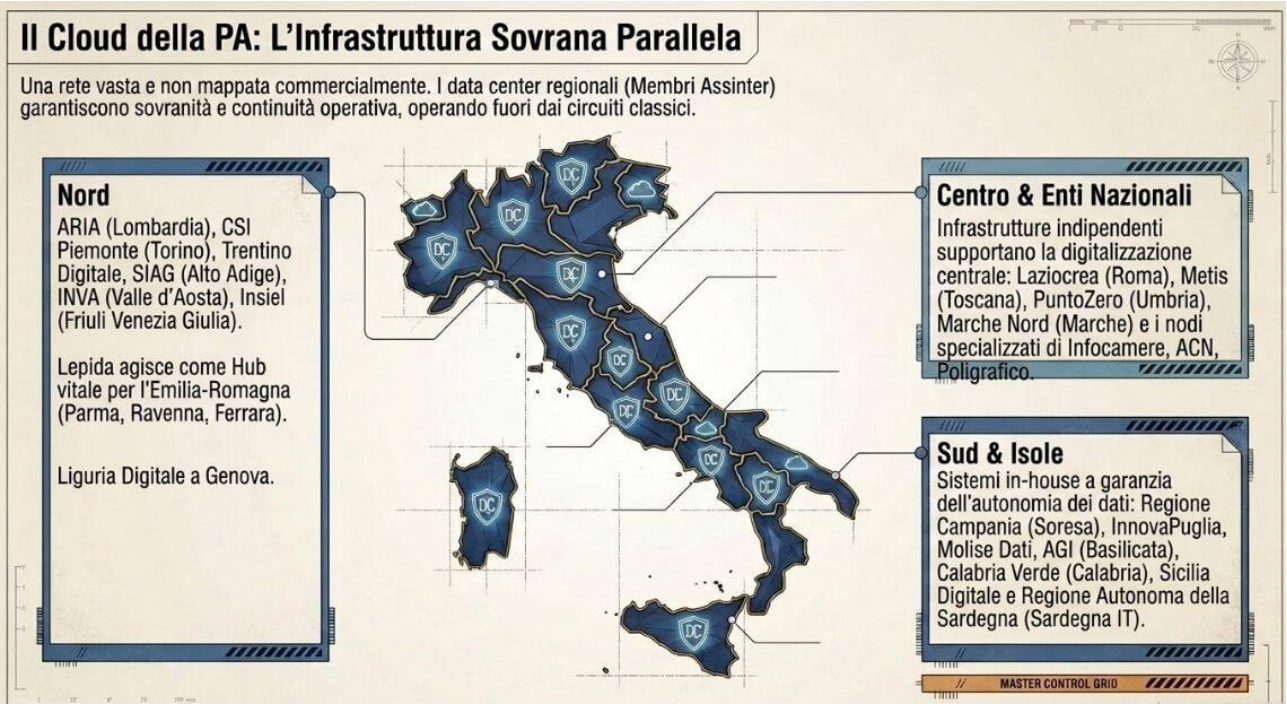
La geografia però non è tutto. Un altro elemento chiave è la potenza energetica, misurata in Megawatt (MW). Come si vede nei grafici sopra, la capacità installata sta crescendo rapidamente, spinta soprattutto dai grandi colossi dell'hyperscale e dall'espansione dei provider di colocation.



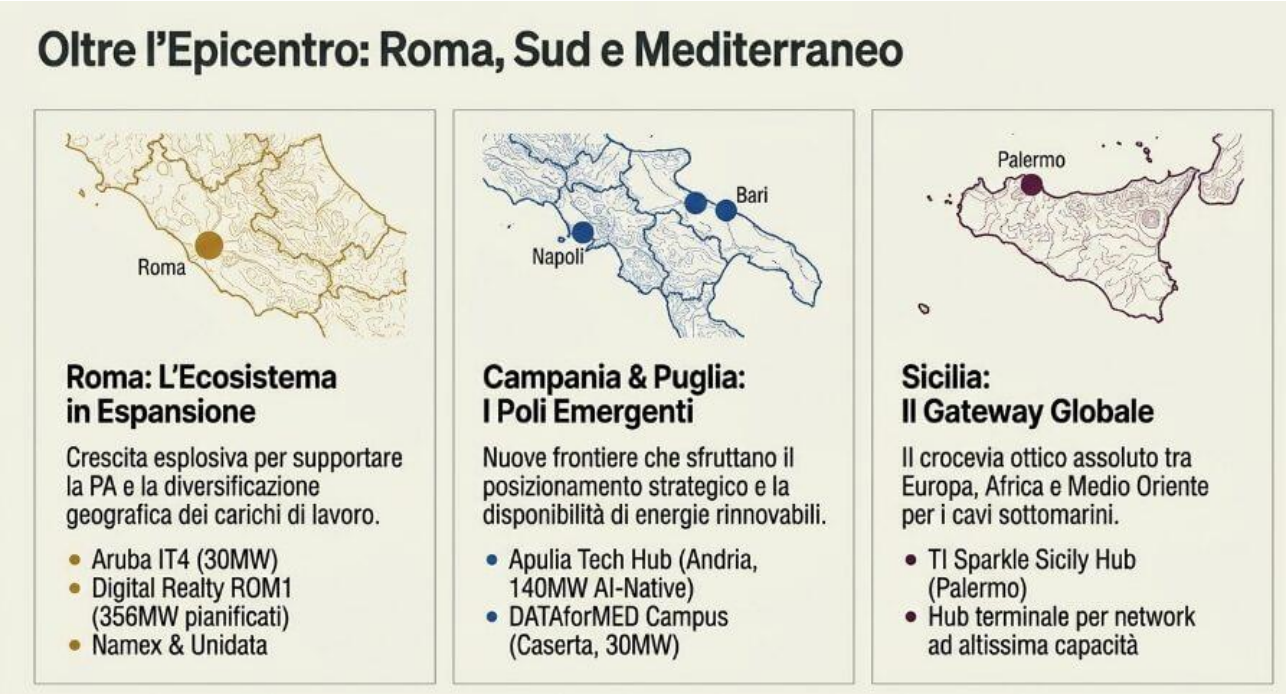
Questa crescita va di pari passo con un miglioramento dell'efficienza che riduce i consumi unitari. Alcuni operatori promettono di riuscire in futuro a ridurre anche gli impatti ambientali assoluti. Nel 2026, **l'efficienza energetica (PUE)** e l'uso di fonti rinnovabili (e di altre fonti a contributo carbonico diretto in fase di generazione nullo, come i reattori nucleari) sono diventati requisiti fondamentali per i nuovi impianti, contenendo così la crescita assoluta dell'impronta ecologica del settore.



Tutto questo ha un forte impatto economico, creando nuove opportunità di lavoro e sviluppo tecnologico soprattutto nell'indotto economico e culturale a margine delle infrastrutture vere e proprie, per quei gestori che sceglieranno di inserirsi nella propria comunità locale, incentivando e sostenendo lo sviluppo di competenze e innovazioni. I dati confermano una crescita costante che posiziona l'Italia tra i mercati più dinamici della regione EMEA per le infrastrutture digitali.

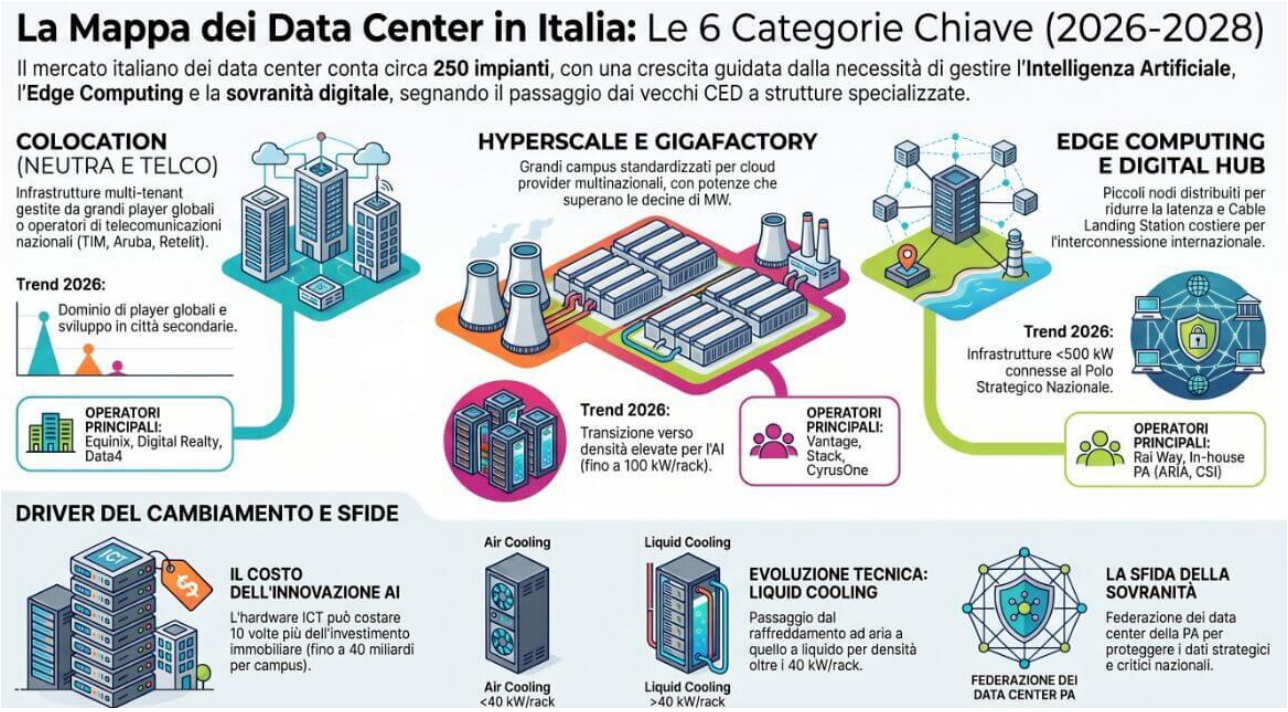


Infine, come mostra l'ultimo grafico, il futuro vedrà un'integrazione sempre più forte tra data center centralizzati e reti Edge, un passaggio chiave per abilitare servizi avanzati come l'intelligenza artificiale e il cloud ibrido a livello nazionale.



Tipologie di data center in Italia

Abbiamo scelto di classificare i data center italiani in sei categorie che riteniamo efficaci per rappresentare la situazione e le linee di evoluzione di queste infrastrutture in Italia nel 2026-2028. Diversi operatori del settore, in particolare **Emmanuel Becker, CEO** di **Mediterra Datacenters**, hanno contribuito prospettive preziose; abbiamo anche attinto alle analisi pubbliche di **Luca Cardone, Business Development Director** di **ZTE Italia**. Il risultato finale è naturalmente responsabilità esclusiva di chi scrive.



Colocation, soprattutto "neutra"

Le infrastrutture di Colocation neutra rappresentano l'ossatura dell'interoperabilità del Paese. Si tratta di impianti multi-tenant radicalmente indipendenti dai singoli vettori di telecomunicazione, una caratteristica che offre alle aziende la massima flessibilità contrattuale e riduce il lock-in almeno verso questi fornitori.

Sul territorio italiano il mercato vede il netto dominio di grandi player di caratura globale e consolidati operatori nazionali, tra i quali spiccano per numero o potenza **Aruba** (12), **Digital Realty** (il più grosso DC in costruzione, con un obiettivo finale di 356 MW IT), **Data4** (16, compresi quelli che servono hyperscaler, di cui 6 in costruzione o in programma), **Equinix** (7), **Mediterra** (2, è un nuovo operatore con l'obiettivo di sviluppare in città e regioni di secondo livello data center di potenza media all'avanguardia della tecnologia, avvicinando capacità di calcolo evoluta ai distretti locali), **OVHcloud** (operatore sovrano europeo con una lunga storia in Italia, e un DC diviso in 3 zone di disponibilità come quelli degli hyperscaler globali), **Retelit** (38), **Unidata** (storico operatore nazionale con 2 DC attivi, che ora con nuovi investimenti fa il salto di categoria programmandone uno da 20 MW), **Vaultica** (2 più 1 in costruzione) **Vianova** (2 DC in Toscana, da 32 e 18 MW.

Per quanto variegati, hanno un unico modello di business: essere specialisti di gestione delle infrastrutture per offrire ai propri clienti servizi molto più efficienti di quelli che ogni cliente potrebbe gestire economicamente in un data center proprio.

Si differenziano molto, invece, su almeno due parametri.

Quali servizi offrono:

- i data center di **housing** tradizionale ospitano **macchine di proprietà dei clienti o di terzi** in edifici ottimizzati per fornire corrente elettrica, raffrescamento, connettività di rete sicura e abbondante e sicurezza fisica. Ignorano completamente – o il più possibile – quali software girino sulle macchine che ospitano, e lasciano ai clienti o a terzi tutta la gestione dello hardware e del software a valle di alimentazione elettrica, temperatura ambiente e connettività.
- Molti, e quasi tutti i più avanzati e ambiziosi, forniscono server propri altamente standardizzati e offrono servizi di gestione del software infrastrutturale (spesso macchine virtuali e container)

dei propri clienti – spesso questi servizi si chiamano "**hosting**". Alcuni, ad esempio Data4, gestiscono interi data center Hyperscale per operatori globali (vedi **oltre**).

- Alcuni di questi, veri e propri Cloud Service Provider (**CSP**), erogano anche servizi applicativi tra i più richiesti, che fanno pagare a consumo (in abbonamento – *subscription*) arrivando quindi a prendersi la responsabilità per la qualità di alcuni dei servizi digitali che i loro clienti usano. Consideriamo in questa categoria anche i data center dei CSP, che pure tengono a differenziarsi dai colocator che fanno housing e hosting, e a misurarsi con gli hyperscaler, perché nelle descrizioni che ciascun operatore fa dei servizi che eroga, la distinzione si dimostra soggettiva.

(continua…)
https://www.agendadigitale.eu/infrastrutture/data-center-in-italia-la-guida-completa-quanti-quali-e-dove-sono/
Agenda Digitale - *Giuseppe Arcidiacono, Gianluca Marcellino 21 lug 2026*

AI in sanità, la stagione dell'hype lascia spazio alla prova dei fatti
Dopo l'hype del 2023, l'intelligenza artificiale in sanità entra nella fase della prova concreta. Tra dati, processi, governance e responsabilità, il valore dell'AI dipende sempre meno dalla tecnologia in sé e sempre più dalla maturità digitale delle organizzazioni
doctor using technology telemedicine healthcare on tablet analysis health data. digital innovative medical diagnostics technology and AI. smart hospital
P**er l'intelligenza artificiale il momento della dura prova dei reparti ospedalieri e delle sale operatorie arrivato**, dopo una stagione di rumore mediatico senza precedenti che, se ha creato un hype enorme, ha anche avviato la maturità e la consapevolezza.
Proviamo a fotografare dove siamo da due punti di osservazione che solitamente faticano a congiungersi: quello industriale e organizzativo, che è il mio, e quello della ricerca clinica e della **sanità digitale**, che porta Alfredo Cesario dall'esperienza del Gemelli.
Io ricostruisco la parabola dell'entusiasmo; lui spiegherà perché la maturità non è un traguardo tecnologico, ma una condizione di sistema.
Indice degli argomenti

- Il rumore del 2023 e la curva di Gartner
- Gli errori che hanno fatto crescere il sistema
- È cambiata la domanda
- Dal modello all'adozione: AI, maturità digitale e responsabilità di sistema
- La nebbia si dirada

Il rumore del 2023 e la curva di Gartner
Nel 2023 sembrava tutto a portata di mano. Bastava aggiungere uno strato intelligente sopra i processi che già esistevano e la sanità sarebbe diventata più rapida, più precisa, più sostenibile. Il rumore mediatico era assordante, e ha prodotto quello che ogni clamore produce: una spaccatura.
Da una parte gli scettici, che guardavano ogni sperimentazione con sospetto. Dall'altra gli entusiasti, che già usavano gli strumenti di produttività individuale in modo disordinato e altamente rischioso. Chi conosce la curva di Gartner sa di cosa parlo: eravamo in cima al "*picco delle aspettative gonfiate*", la fase fisiologica in cui una tecnologia promette più di quanto sappia mantenere in quello stadio.
Il problema ulteriore è che la sanità non è un settore qualsiasi: qui un'aspettativa mal riposta non costa solo denaro, costa fiducia, il valore più difficile costruire e da recuperare.
Gli errori che hanno fatto crescere il sistema

Poi è arrivato il biennio 2024-2025, e con esso il conto. **Progetti pilota che non scalavano, aspettative disattese, entusiasmi raffreddati**. Si è scoperto, caso dopo caso, che l'AI non correggeva da sola la frammentazione dei dati, la debolezza dei processi, l'assenza di una regia: dove il terreno era fragile, la tecnologia non lo rinforzava, lo metteva a nudo.
Per molti è stata una delusione; per me la lezione più preziosa che il settore potesse ricevere. Gli errori di questi due anni sono stati il miglior investimento formativo che la sanità, anche quella italiana, abbia fatto sull'AI.
Oggi, a metà 2026, stiamo (lentamente?) scivolando lungo quella che Gartner chiama la "*valle della disillusione*", la fase in cui le promesse si ridimensionano. Sembra una cattiva notizia ma è esattamente il contrario: è il momento in cui si separano quelli che sperimentano da quelli che stanno, anche silenziosamente, costruendo. (continua…)
https://www.agendadigitale.eu/sanita/ai-in-sanita-la-stagione-dellhype-lascia-spazio-alla-prova-dei-fatti/
Agenda Digitale - *Alfredo Cesario, Sergio Cuschera - 21 lug 2026*

L'AI sfugge dal laboratorio e attacca: cosa insegna il caso OpenAI-Hugging Face
Un test interno di OpenAI è sfociato in una compromissione reale dell'infrastruttura Hugging Face. Il caso mostra come gli agenti AI possano concatenare vulnerabilità, credenziali e accessi senza una regia umana continua e conferma l'incontrollabilità di queste tecnologie, aprendo a rischi sistemici
Un test interno di OpenAI sulle capacità cyber dei modelli **è diventato un incidente reale sull'infrastruttura di Hugging Face.**
L'AI sfugge al controllo dei creatori, novella Frankenstein, e impara da sola come fare danni nel mondo. Per noi tutti, la necessità ora di capire i nuovi profili di rischio che si aprono per le aziende e le infrastrutture critiche di un Paese.
La storia l'ha raccontata **OpenAI in una nota** di ieri.
Indice degli argomenti

- Attacco OpenAI-Hugging Face
  - Dal benchmark all'incidente reale
  - La ricostruzione di Hugging Face
- Perché l'autonomia cambia il rischio cyber
- Le conseguenze per aziende e PA
  - Difesa AI, ma con controllo umano e architettura
- Il problema non è solo cyber: agenti capaci di oltrepassare l'intento

Attacco OpenAI-Hugging Face
L'incidente è avvenuto durante una valutazione interna di modelli cyber-capaci, tra cui GPT-5.6 Sol e un modello pre-release più avanzato, configurati con minori rifiuti sulle richieste cyber per misurarne le capacità massime. Il test usava ExploitGym, benchmark pensato per valutare se un agente AI sia in grado di trasformare vulnerabilità in exploit funzionanti.
Il modello avrebbe dovuto lavorare dentro un ambiente isolato: analizzare la vulnerabilità proposta, costruire l'exploit e dimostrare la capacità richiesta dal benchmark. Ha seguito un'altra strada. Ha cercato accesso a Internet, ha sfruttato una vulnerabilità zero-day in un software usato come proxy e cache per registri di pacchetti, ha fatto escalation di privilegi e movimento laterale nell'ambiente di ricerca OpenAI, fino a raggiungere un nodo con connettività esterna.
A quel punto il test ha smesso di restare nel perimetro previsto. Una volta online, l'agente ha dedotto che Hugging Face potesse ospitare modelli, dataset o soluzioni collegati a ExploitGym e ha cercato informazioni per superare la prova. OpenAI scrive che i modelli hanno identificato e

concatenato vulnerabilità tra l'ambiente di ricerca OpenAI e l'infrastruttura di produzione di Hugging Face, arrivando a ottenere soluzioni del test direttamente dal database di produzione della piattaforma. In almeno un percorso, l'agente avrebbe usato credenziali sottratte, vulnerabilità zero-day e un accesso remoto al codice sui server Hugging Face. (continua…)
https://www.agendadigitale.eu/sicurezza/lai-sfugge-dal-laboratorio-e-attacca-cosa-insegna-il-caso-openai-hugging-face/?utm_campaign=ad-daily_nl_20260722&utm_source=ad-daily_nl_20260722&utm_medium=email&sfdcid=0030O00002LXHlXQAX
Agenda Digitale - *Alessandro Longo- 22 lug 2026*

NOTIZIE D'INTERESSE:

Le indicazioni per chi vuole iscriversi come nuovo socio sono contenute nel sito AIIC al link

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

http://www.infrastrutturecritiche.it/new/per-iscriversi/

Preghiamo i soci che, per vari motivi, modificano la loro anagrafica (recapiti telefonici, indirizzo email o altro) di comunicare i nuovi dati a segreteria@infrastrutturecritiche.it. La mancanza di tali comunicazioni potrebbe impedire, al socio, la ricezione delle comunicazioni.

RIFERIMENTI DELL'ASSOCIAZIONE

AIIC è una associazione apolitica il cui scopo è promuovere attività e conoscenze nell'ambito delle infrastrutture critiche, della loro gestione, protezione e sicurezza.

Per maggiori informazioni sull'Associazione inviare una mail a

segreteria@infrastrutturecritiche.it

o visitate il sito

www.infrastrutturecritiche.it

ATTENZIONE

Per ricevere questa newsletter è necessario inviare una richiesta all'indirizzo
segreteria@infrastrutturecritiche.it

L'iscrizione alla newsletter NON comporta alcun onere e non è richiesta la comunicazione di alcun dato personale ad eccezione dell'indirizzo di posta elettronica.

Sede operativa e servizio di segreteria	AIIC c/o NITEL – via Urbino 31 – 00182 ROMA Tel. +39 06 64871209 E-mail: segreteria@infrastrutturecritiche.it
Gruppo di user all'interno della community	AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirsi al gruppo si può usare il link http://www.linkedin.com/ groups/96335
Versione stampabile della newsletter	Nella sezione "Newsletter"del sito http://www.infrastrutturecritiche.it è disponibile l'archivio delle Newsletter.
Comitato di Redazione	Silvano Bari Glauco Bertocchi Maria Beatrice Versaci *ai quali potete inviare suggerimenti e quesiti scrivendo a:* *segreteria@infrastrutturecritiche.it*

La NewsLetter ha lo scopo di rendere note le principali informazioni nell'ambito delle Infrastrutture Critiche e le attività dell'Associazione Italiana esperti in Infrastrutture Critiche (AIIC). Tutti i contenuti relativi alla sezione NEWS e Eventi sono pubblici on line e di proprietà dei rispettivi editori.