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. 1/ 2026** **gennaio 2026**

Cari soci,
Abbiamo concluso il 2025 parlando di resilienza, nel contesto di un breve riepilogo degli eventi di sicurezza più rilevanti che hanno interessato i servizi essenziali globali nell'anno appena trascorso. Per questo inizio 2026, vogliamo invece proporre una riflessione su una nuova parola chiave, presa in prestito dal matematico e filosofo Nassim Nicholas Taleb: antifragilità.
Il termine, protagonista di una pubblicazione il cui ambito esula in realtà dai temi della nostra Associazione, si riferisce alla qualità di un sistema che trae vantaggio dal disordine e dall'incertezza, un sistema capace di imparare, adattarsi e perfino prosperare in condizioni di perturbazione. Taleb sostiene che "alcune cose beneficiano dagli shock; prosperano e crescono quando sono esposte alla volatilità, al caso, al disordine e allo stress". In questa visione, ciò che è resiliente resta – o per meglio dire: torna – sostanzialmente invariato di fronte agli shock, mentre ciò che è antifragile si rafforza grazie a essi.
Ma possibile considerare la possibilità che le infrastrutture critiche non solo sopravvivano alle perturbazioni, ma che imparino da esse in modo da adattare la propria architettura logica, operativa e gestionale? E soprattutto: Ha concretamente senso applicare questo concetto ai servizi fondamentali per il funzionamento del Paese? Come fanno ad esempio i trasporti o il sistema elettrico a beneficiare dall'essere messi sotto stress?
In merito a quest'ultimo quesito, ha senz'altro senso parlarne solo se si chiarisce a quale livello si colloca il concetto di antifragilità. Se la intendiamo come "il sistema che migliora automaticamente mentre è sotto attacco", allora no: per infrastrutture come elettricità o trasporti, per non parlare della sanità, sarebbe una formula retorica pericolosa. Se invece la intendiamo come capacità strutturale di trasformare lo stress in informazione utile, in questo caso non solo ha senso, ma descrive qualcosa che già accade.
In altre parole, le infrastrutture critiche non possono essere antifragili a livello di servizio, ma possono esserlo a livello di sistema decisionale e progettuale.
Se pensiamo ai sistemi critici solo come ad asset da proteggere, rischiamo di perdere di vista che essi sono ecosistemi dinamici immersi in un contesto geopolitico, climatico e tecnologico in continuo mutamento. Nel portare avanti questa riflessione, non si tratta di abbandonare la resilienza (che rimane fondamentale), ma di ampliare il nostro orizzonte concettuale: ragionare non solo in termini di sopravvivenza, ma per l'evoluzione continua attraverso l'esperienza delle crisi stesse.

Maria Beatrice Versaci
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). Attualmente analista presso Hermes Bay srl.

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

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.

NUOVO SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

Ricordiamo che è attivo il nuovo sito dell'Associazione Italiana Esperti in Infrastrutture Critiche.
L'indirizzo è sempre **www.infrastrutturecritiche.it** ma il sito è stato completamente rinnovato, sia nelle veste grafica che nei contenuti e nelle funzioni a disposizione.
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.

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

Vi ricordiamo inoltre che il sito web www.infrastrutturecritiche.it rappresenta la **fonte ufficiale dell'associazione**, accessibile a tutti, e contiene tutte le informazioni necessarie per un corretto svolgimento della vita associativa.

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

AIIC – GRUPPO DI LAVORO

Artificial Intelligence and Climate Change

È in dirittura di arrivo il report su **"Artificial Intelligence and Climate Change"** predisposto dall'apposito Gruppo di Lavoro costituito dai seguenti soci:

Sandro Bologna (Coordinatore)
Silvano Bari, Glauco Bertocchi Luigi Carrozzi, Raffaella D'Alessandro, Tommaso Diddi, Elenio Dursi, Alberto Stefanini, Maria Beatrice Versaci, Cristina Turconi, Adriana Peduto, Beatrice Rosa, Lorenzo Vandoni, Gabriele Balzano

La chiusura dei lavori e l'emissione del report è prevista entro la fine del prossimo mese di febbraio.

NEWS E AVVENIMENTI

Come cambia il mondo dei sottomarini? - Le nuove tecnologie applicate all'ambiente subacqueo rendono sempre più identificabili e localizzabili i sottomarini e aumentano il ruolo dei droni marittimi underwater. Quale futuro per i guardiani degli oceani?
1. SULL'ONDA DELLA RICERCA
I sottomarini rivestono un ruolo cruciale nella protezione delle linee di comunicazione e delle infrastrutture civili e militari installate in profondità, quali cavi e gasdotti sottomarini, oltre a un ruolo di deterrenza nucleare. Il loro successo si basa su caratteristiche fondamentali come la furtività, intesa come difficoltà di essere rilevati dall'avversario. Tuttavia, l'accelerazione tecnologica dei sistemi di rilevamento integrati con l'intelligenza artificiale renderà l'ambiente marino sempre più "trasparente e affollato". Tale previsione è supportata dal rapporto scientifico Transparent Oceans pubblicato dalla National Security College dell'Australian National University, il quale evidenzia come entro il 2050 i progressi scientifici e tecnologici applicati all'ambiente subacqueo possano compromettere la sicurezza della maggior parte dei sistemi meccanici ed elettronici impiegati per le tecniche stealth. Di particolare rilievo è anche lo studio condotto da un gruppo di ricercatori italiani per la Texas National Security, che analizza gli effetti del cambiamento climatico sulle proprietà fisico-chimiche dell'acqua marina (come salinità e temperatura) e le conseguenze sulla propagazione delle onde sonore. Esiste pertanto un

dibattito anche sul futuro di questa piattaforma: almeno in alcuni casi i grandi sottomarini potrebbero evolversi in piattaforme di lancio, simili alle portaerei, per veicoli subacquei senza equipaggio (UUV) come l'Echo Voyager, drone subacqueo autonomo lungo circa 15 metri sviluppato da Boeing. (continua…)
https://ilcaffegeopolitico.net/1000124/come-cambia-il-mondo-dei-sottomarini
IlCaffèGeopolitico – *Sante Grande - 12 Settembre 2025*

Intelligenza artificiale in azienda, subire un attacco è quasi una certezza - Solo l'1% delle applicazioni e dei servizi aziendali di AI non ha registrato tentativi di attacco in 12 mesi: un report di Palo Alto.
Per le aziende che utilizzano applicazioni e servizi di intelligenza artificiale, subìre un attacco informatico di un qualche tipo, o anche più di uno, è quasi una certezza. A dirlo è un nuovo studio di Palo Alto Networks (State of Cloud Security Report 2025"), che evidenzia l'ulteriore espansione della cosiddetta "superficie di attacco", e nella fattispecie la sua componente cloud. Tra gli intervistati, cioè 2.800 dirigenti e professionisti della sicurezza di aziende di 10 Paesi (Australia, Brasile, Francia, Germania, Giappone, India, Messico, Regno Unito, Singapore e Stati Uniti), uno schiacciante 99% ha detto di aver osservato nell'anno precedente uno o più tentativi di attacco verso i propri sistemi o applicazioni di AI.
Non si parla, quindi, genericamente di minacce rivolte ai servizi di intelligenza artificiale accessibili via Web o tramite app, anche gratuiti, come ChatGpt o Gemini. Il problema riguarda nello specifico le applicazioni e i sistemi di AI sviluppati o acquistati dalle aziende per utilizzi interni. All'AI generativa si legano anche altri rischi: il vibe coding, per esempio. Grazie alla scrittura di codice assistita, gli sviluppatori sfornano applicazioni o parti di applicazioni sempre più rapidamente, anche troppo, senza che i team di sicurezza abbiano il tempo per svolgere i loro controlli. Sul totale del campione d'indagine, nel 52% delle aziende la distribuzione di nuovo codice avviene su base settimanale, ma solo il 18% è in grado di correggere le vulnerabilità altrettanto velocemente.
(continua)
https://www.ictbusiness.it/news/intelligenza-artificiale-in-azienda-subire-un-attacco-e-quasi-una-certezza.aspx
ICTBusiness *– 17/12/2025 di redazione*

Graph Neural Networks: la nuova difesa europea contro i droni - Il drone wall europeo, previsto per il 2027, integrerà tecnologie avanzate di intelligenza artificiale. Le reti neurali a grafo consentono di modellare interazioni complesse tra sensori, radar e unità autonome, catturando relazioni non locali e dinamiche temporali degli attacchi coordinati
Le Graph Neural Networks stanno ridisegnando gli scenari della difesa anti-drone in Europa.
Entro il 2027, il continente dovrà proteggere i propri confini orientali con tecnologie capaci di prevedere e neutralizzare sciami coordinati in movimento.
La sfida è complessa: sistemi distribuiti, sensori mobili, interazioni che cambiano in tempo reale.
Indice degli argomenti

Prestazioni comparative: accuratezza, scalabilità e gestione temporale
Relazioni dinamiche: il vantaggio competitivo delle GNN
Caso d'uso: difesa contro sciami coordinati di droni
Edge AI e sicurezza: resilienza e riservatezza dei dati
Leadership europea: opportunità strategiche e tecnologie chiave
Iniziative europee: sovranità tecnologica e interoperabilità
Conclusioni: il vantaggio competitivo europeo nelle GNN
Bibliografia
(continua…)
https://www.agendadigitale.eu/sicurezza/graph-neural-networks-la-nuova-difesa-europea-contro-i-droni/
Agenda Digitale - *Ernesto Damiani - 18 dic 2025*

E-fuel marittimi: tanti progetti in Ue, ma non sostenuti da apparato normativo - La Norvegia è il principale potenziale fornitore europeo di carburanti sintetici per il settore navale, seguita da Spagna, Finlandia e Danimarca
L'Europa potrebbe diventare leader mondiale negli e-fuel marittimi, i carburanti sintetici prodotti per decarbonizzare uno dei settori più difficili da elettrificare: il trasporto navale. I progetti non mancano. Nel suo aggiornamento 2025 dell'Osservatorio sugli e-fuel per il trasporto marittimo, Transport & Environment (T&E) ha analizzato 80 progetti europei di idrogeno verde ed e-fuel potenzialmente destinabili al settore navale.
Indice dei contenuti
Situazione in stallo
Norvegia e Spagna guidano la corsa agli e-fuel marittimi
E-metanolo ed e-ammoniaca: il mare è il mercato chiave
E-fuel marittimi: una scelta climatica, industriale e geopolitica
Situazione in stallo
Sebbene i progetti censiti potrebbero arrivare a produrre 3,6 milioni di tonnellate equivalenti di petrolio (Mtep) entro il 2032, meno del 5% dei volumi è destinato in via prioritaria al trasporto marittimo. Un segnale debole per il settore, soprattutto se confrontato con gli obiettivi di FuelEU Maritime, che prevedono una quota dell'1% di e-fuel entro il 2031 e del 2% entro il 2034. In assenza di politiche europee e nazionali più chiare e di incentivi finanziari dedicati, il rischio è che questi target vengano raggiunti ricorrendo a carburanti importati – o non vengano centrati affatto – con una occasione persa per la leadership climatica europea. A dirlo è una nuova analisi di T&E, che fotografa un continente in bilico tra ambizione climatica e immobilismo regolatorio. (continua…)
https://www.rinnovabili.it/mobilita/biocarburanti/e-fuel-marittimi-tanti-progetti-in-ue-ma-non-sostenuti-da-apparato-normativo/
Rinnovabili - *La Redazione, 18 Dicembre 2025*

As More Coders Adopt AI Agents, Security Pitfalls Lurk in 2026
Developers are leaning more heavily on AI for code generation, but in 2026 the development pipeline and security need to be prioritized.

The Code May Be Correct, But Is It Secure?

While Claude Opus 4.5 Thinking gets top marks for being correct, just slightly half of the code it generates is both correct and secure.

Source: BaxBench.com

Rank	Model	Correct & Secure	Correct	% Insecure of Correct
1	Claude Opus 4.5 Thinking	56.1%	86.2%	34.9%
2	GPT-5	54.3%	70.7%	23.1%
3	OpenAI o3	46.4%	67.6%	31.3%
4	Claude 4 Sonnet Thinking	45.7%	75.0%	39.1%
5	GPT-4.1	40.8%	56.4%	27.7%
6	Claude 3.7 Sonnet Thinking	37.0%	63.3%	41.5%
7	DeepSeek R1	34.4%	58.4%	41.0%
8	OpenAI oe-mini	34.4%	63.0%	45.3%
9	Grok 4	33.4%	57.7%	42.0%
10	Gemini 2.5 Pro	32.0%	49.8%	35.8%

DARKREADING

Claude Opus 4.5 Thinking gets top marks, but only slightly more than half of the code generated is correct and secure. Source: BaxBench.com

Software may be eating the world — to paraphrase one tech luminary — but in 2025, artificial intelligence (AI) ate software development. The vast majority of professional programmers now use large language models (LLMs) for code suggestions, debugging, and even vibe coding.

Yet challenges remain: Even as developers start to use AI agents to build applications and integrate AI services into the development and production pipeline, the quality of the code — especially the security of the code — varies significantly. Greenfield projects may see better productivity and security results than rewriting current code, especially if vulnerabilities in the older code are propagated. Some companies see few productivity gains, while others see significant benefits.

Software developers are moving faster, but depending on their knowledge and practices, they may not be producing secure code, says Chris Wysopal, chief security evangelist at application security firm Veracode.

AI-assisted coding, refactoring, and architectural generation will dramatically increase code volume and complexity, so organizations will ship more software faster but with less human visibility, he explains. (continua…)

https://www.darkreading.com/application-security/coders-adopt-ai-agents-security-pitfalls-lurk-2026

DARKREADING - *Robert Lemos - December 26, 2025*

Si combatte così come ci si è addestrati: le logiche militari sottese al DORA - Leggere il DORA con la lente militare dimostra come la resilienza operativa digitale sia un'estensione naturale dei principi che regolano la leadership: preparazione, addestramento, disciplina. Ecco perché il Regolamento europeo che definisce la resilienza operativa digitale non è un set di adempimenti tecnici, ma una dottrina del comando

Nel mondo digitale, la distanza tra il comando e la crisi si misura in pochi attimi nel corso dei quali non si può improvvisare.

Si reagisce nel modo in cui ci si è preparati, cioè come si è costruita la cultura interna e come si è organizzato il sistema.
Questo capitolo inaugura una tetralogia dedicata alla lettura con lente militare del DORA, il Regolamento europeo che definisce la resilienza operativa digitale come responsabilità essenziale del vertice.
L'obiettivo è quello di mostrare come il DORA non sia un set di adempimenti tecnici, ma una vera e propria dottrina del comando che comprende visione, strategia, disciplina e addestramento.
Inizia un viaggio che unisce diritto, organizzazione e leadership per restituire al lettore chiari indicatori utili a guidare il governo delle crisi informatiche, nelle entità finanziarie, come si guidano le operazioni militari complesse.

Indice degli argomenti

Leggere il DORA con lente militare
La prima legge dell'addestramento: il rischio non concede appelli
Disciplina e struttura: la resilienza come forma mentis
Cultura organizzativa: la vera differenza tra chi resiste e chi cede
Prepararsi prima dell'impatto è l'unico modo per governare la complessità
Il perimetro strategico

Leggere il DORA con lente militare

C'è una frase che porto con me dal 1980, quando varcai il portone della Scuola militare Nunziatella. La frase ha attraversato quattro decenni di servizio e oggi la considero uno dei principi più lucidi per comprendere il dominio digitale: "Si combatte per come ci si è addestrati".
Questa frase non appartiene al folclore militare, ma è una legge del comando.
Chi guida un reparto militare o un'azienda, sa bene che quando arriva l'impatto non c'è tempo per aprire manuali o cercare ispirazione. In quel momento comanda solo ciò che è stato interiorizzato e che è diventato una sorta di riflesso condizionato perché è stato provato decine di volte.
È qualcosa che fa parte del modo di pensare prima ancora del modo di operare.
Ecco, questa, secondo me, è esattamente la chiave con cui leggere il DORA.
(continua)
https://www.cybersecurity360.it/legal/si-combatte-cosi-come-ci-si-e-addestrati-le-logiche-militari-sottese-al-dora/
Cybersecurity360 - *Giuseppe Alverone, 2 gen 2026*

Cybersecurity Predictions for 2026: Navigating the Future of Digital Threats

Cybersecurity experts discuss 2026 predictions, highlighting the rise of AI-driven threats, the shift to resilience over prevention, and the urgent need for advanced security measures to combat evolving risks.
As the digital landscape continues to evolve, so too do the threats that organizations must contend with. In this year's final "Reporter's Notebook" conversation, cybersecurity experts Rob Wright from Dark Reading, David Jones from Cybersecurity Dive, and Alissa Irei from Tech Target Search Security share their insights on what the future holds for cybersecurity in 2026. Drawing from industry reports and expert opinions summarized by artificial intelligence (AI), the conversation highlights key trends, challenges, and opportunities that will shape the way businesses approach security in the coming years. From the rise of AI-driven threats to the growing importance of resilience, the panelists paint a vivid picture of the road ahead.
One of the most pressing concerns is the increasing sophistication of cyber threats, particularly those involving AI and autonomous systems. Threat actors are expected to target agentic AI, exploiting its

capabilities for malicious purposes. While AI offers tremendous potential for productivity gains, the lack of robust security measures and awareness could lead to devastating consequences, such as the rise of AI-driven social engineering and deepfakes, which are poised to erode trust and manipulate human vulnerabilities. As technology advances, organizations must strike a balance between innovation and protection.
Another major shift in cybersecurity priorities is the growing emphasis on resilience and recovery over prevention. The reporters note that businesses are moving away from the traditional focus on secure systems and instead prioritizing defensible, recoverable systems that can withstand catastrophic incidents. This shift reflects a broader understanding of cybersecurity as a form of risk management rather than an attempt to eliminate breaches entirely. With board-level awareness and executive accountability on the rise, organizations are recognizing the importance of preparing for the inevitable and ensuring they have the systems and processes in place to recover quickly.
In a world where cyber threats are becoming more sophisticated and pervasive, the discussion underscores the need for vigilance, innovation, and collaboration. As organizations brace for the challenges of 2026 and beyond, the focus must remain on building resilient systems, fostering awareness, and staying ahead of emerging risks. The future of cybersecurity is uncertain, but with proactive measures and a commitment to adaptation, businesses can navigate the complexities of the digital age. (continua…)
https://www.darkreading.com/threat-intelligence/cybersecurity-predictions-for-2026-navigating-the-future-of-digital-threats
DARKREADING - *Kristina Beek, Rob Wright - January 2, 2026*

Intelligenza artificiale e crisi climatica stanno riscrivendo le disuguaglianze globali - L'1% più abbiente detiene disponibilità economiche, potere e controllo delle tecnologie chiave. Diversi rapporti recenti descrivono la progressiva concentrazione della ricchezza e l'erosione della classe media.
La disuguaglianza nelle condizioni di vita delle persone è oggi estremamente ampia. Il divario tra ricchi e poveri nel mondo continua ad allargarsi. I miliardari, che secondo Oxfam sono meno di 2.800, sono più ricchi che mai. Insieme, ora possiedono una ricchezza netta complessiva di oltre 15mila miliardi di dollari. Se fossero un Paese, sarebbero il terzo più ricco del pianeta, subito dopo Stati Uniti e Cina. In fondo alla piramide, invece, i cittadini dei Paesi a basso e medio reddito faticano ad accedere a sanità, istruzione e altri servizi pubblici essenziali.
Il grafico qui sotto ci offre lo stato aggiornato dei Paesi con alta, media e bassa disuguaglianza nel mondo. È tratta dal recente G20 Global inequality report, commissionato dalla presidenza sudafricana del G20 e guidato dal premio Nobel Joseph Stiglitz. I numeri sono piuttosto impressionanti: circa l'83% dei Paesi ha un indice di Gini superiore a 0,4, che è la soglia identificata dalla Banca mondiale per un'elevata disuguaglianza di reddito. Il 10,5% ha una disuguaglianza media, mentre solo il 6% della popolazione mondiale vive in Paesi con bassa disuguaglianza di reddito. Negli Stati più diseguali, inoltre, la probabilità di un declino democratico è sette volte superiore rispetto alle società più eque. Nuovi dati mostrano anche mostrano anche che dal 2000 la quota di reddito dell'1% più ricco è aumentata nel 47% dei Paesi, quelli che ospitano il 68% della popolazione mondiale, mentre è inferiore o invariata nel 53% dei Paesi. (continua…)
https://www.puntosicuro.it/sostenibilita-C-149/intelligenza-artificiale-crisi-climatica-stanno-riscrivendo-le-disuguaglianze-globali-AR-26002/
Punto Sicuro – *Redazione, 08/01/2026*

Come spiegare le decisioni dell'AI: tecniche di attribuzione e casi reali

L'AI generativa ha reso i modelli più potenti ma anche più opachi: cresce l'esigenza di capire su quali segnali si basano le decisioni. Le tecniche di Explainable AI stimano il peso delle feature e lo rendono visibile con mappe e grafici, utili per validare risultati e individuare bias

Interpretare i modelli di AI significa capire quali segnali dell'input guidano una previsione e, sempre più spesso, come l'informazione viene trasformata dentro **reti profonde e LLM**.

Con **l'esplosione dell'AI generativa** e l'avanzare delle normative, la spiegabilità passa da "nice to have" a requisito: tecniche di attribuzione, strumenti di analisi e nuove linee di ricerca puntano a ridurre l'opacità delle black-box.

Indice degli argomenti

Le nuove frontiere dell'interpretabilità dei modelli di AI

Nel contesto del Deep Learning, soprattutto se guardiamo all'ampia diffusione recente dei modelli di AI Generativa, emerge un problema rilevante, riguardante la crescente complessità di questi modelli neurali. E' una complessità che si accompagna poi allo sviluppo di diverse normative internazionali **(AI Act**, **Executive Order 14179 in USA**, ecc.) e anche di linee guida specifiche, come i framework del **NIST**, che fissano dei principi fondamentali per lo sviluppo e l'utilizzo di questi sistemi.

Dobbiamo quindi affrontare una questione importante, su cui oggi si sta discutendo ampiamente: **come comprendere e spiegare il processo decisionale che è alla base delle previsioni di una rete neurale profonda**.

Nei modelli su scala molto ampia, come i *Large Language Models (LLM),* ma anche le moderne **Convolutional Neural Networks (CNN)**, possono esserci miliardi di parametri e varie decine, o anche centinaia, di "Hidden Layer", che elaborano i dati di input e li trasformano in rappresentazioni sempre più complesse, per giungere infine a delle predizioni finali. Questi modelli hanno ormai

raggiunto dei livelli di prestazione eccezionali nei compiti in cui sono impiegati, e in tutti i settori di attività.
Il problema che abbiamo di fronte è che a noi risultano molto spesso **opachi,** nel loro funzionamento interno e nella loro complessità, **come se fossero delle *black-box*,** che producono decisioni, o risultati in genere, di cui è difficile interpretare la logica interna, almeno dal punto di vista delle persone.
Da questa difficoltà di comprensione nasce, negli ultimi anni, la disciplina dell'**Explainable Artificial Intelligence (XAI)**, che mira a sviluppare metodi e strumenti per rendere più **interpretabili e verificabili** le decisioni dei sistemi di IA, pur con dei limiti e delle approssimazioni, dovute all'attuale livello della ricerca, tuttora in evoluzione.
Si tratta di capire **come e perché** un modello, ad esempio una rete neurale profonda convoluzionale (CNN) che elabora immagini, o anche un Large Language Model (LLM) come GPT, arrivino ad una certa decisione o ad una certa previsione, e di avere la possibilità di seguirne le logiche. In un'ottica di trasparenza, di analisi critica e di valutazione delle prestazioni. E questo in un periodo storico in cui, insieme all'evidenza delle grandi potenzialità di queste applicazioni di AI, si sta man mano diffondendo la consapevolezza dei loro limiti, in termini di affidabilità dei risultati (pensiamo ai ***bias*** e alle ***allucinazioni***) ma anche in termini di rischi sistemici.
Il grido d'allarme lanciato da molti esperti, e addirittura dai "padri" del Deep Learning, come Geoffrey Hinton (premio Nobel 2024 per la fisica) e Yoshua Bengio, hanno messo in guardia anche il grande pubblico, che usa questi strumenti ormai giornalmente, sui rischi e sulle necessità di controllo e di trasparenza.
Il tema della "***Trasparenza***" si è quindi posto all'attenzione generale, anche in seguito all'entrata in vigore progressiva delle recenti normative internazionali, come l'**AI Act** dell'Unione Europea. La necessità di rendere trasparenti e verificabili i processi interni di un sistema di AI, specie di quelli ad "**alto rischio**", ha portato al centro delle analisi e delle attenzioni le tecniche dell'Explainable AI e gli strumenti che questa disciplina ci fornisce, come le "***Tecniche di Attribuzione***".
Le tecniche di attribuzione rappresentano uno dei principali strumenti della **XAI,** per analizzare e quantificare il grado di importanza delle diverse variabili di input nelle **decisioni** di un modello. I ***grafici di attribuzione***, che ne costituiscono la rappresentazione visiva, consentono di visualizzare tali informazioni in delle mappe di intensità e colori diversi, che sono utili a rendere percepibile, anche se in modo approssimativo, il risultato dell'elaborazione, con il contributo dato da ciascun input al risultato finale.
E' una tecnica di rappresentazione facilmente interpretabile: ogni decisione della rete può essere suddivisa in **contributi locali** associati alle variabili di input. Visualizzare tali relazioni significa, in sostanza, cercare di **"aprire la black-box"** del modello, gettare lo sguardo sul suo meccanismo interno, rendendolo in parte comprensibile alle persone.
Adottando queste tecniche possiamo cercare di rendere più trasparenti questi modelli, aiutandoci ad interpretarne i risultati, e a trarre degli spunti per progressivi miglioramenti. In questo articolo verranno analizzate le principali metodologie di interpretabilità usate oggi, faremo degli esempi, dando uno sguardo ad alcune loro applicazioni.
L'esigenza di affrontare questa tematica deriva dall'insicurezza che spesso trapela tra gli analisti, e persino tra gli esperti, su **rischi** elevati, o addirittura incontrollabili, che potrebbero derivare da un difetto di controllo su questi nuovi strumenti della tecnologia. Avere dei metodi per renderli il più possibile trasparenti e controllabili è oggi una esigenza primaria, anche per favorirne l'utilizzo e la diffusione, superando alcuni timori ingiustificati.

Principi generali dell'attribuzione

L'attribuzione ha l'obiettivo di stimare il **contributo di ciascuna variabile** di input nel determinare l'output finale di un modello. In altre parole, serve a capire "quanto" ogni feature ha influenzato la

decisione della rete neurale, in modo da rendere evidenti quali siano le caratteristiche di input ad avere una maggiore **peso** nelle decisioni del modello.
Le principali famiglie di tecniche di attribuzione, utilizzate per l'analisi dei risultati, sono tre:

- **Gradient-based**, che analizzano come varia l'output del modello in risposta a piccole variazioni dell'input, come nelle ***Saliency Maps***, le ***Grad-CAM*** (tecnica ibrida) e le ***Integrated Gradients***.
- **Perturbation-based**, che valutano l'effetto sull'output rimuovendo o modificando dei singoli elementi dell'input, come nel metodo ***LIME***.
- **Additive game-theoretic**, che si basano sulla teoria dei giochi cooperativi per calcolare la "quota parte di responsabilità" di ciascuna feature di input, come nel caso di ***SHAP***.

Ogni approccio presenta sia vantaggi che limiti: i metodi basati su gradienti offrono una maggiore **precisione** locale, quelli di perturbazione una migliore **intuitività**, mentre gli approcci **additivi** garantiscono una maggiore coerenza e solidità nell'impianto teorico.
La scelta del metodo da utilizzare dipende quindi dal tipo di modello, dal dominio applicativo e dal livello di trasparenza richiesto. Un approccio integrato di metodi diversi può servire ad analizzare più a fondo i risultati di un modello, utilizzando diverse tecniche, specialmente nelle applicazioni più critiche, come in sanità, per avere la maggiore confidenza possibile.(continua…)
https://www.agendadigitale.eu/mercati-digitali/come-spiegare-le-decisioni-dellai-tecniche-di-attribuzione-e-casi-reali/
AGENDADIGITALE - *Giuseppe Ferrigno - 12 gen 2026*

Experian: AI Agents Could Overtake Human Error as Major Cause of Data Breaches
Artificial intelligence continues to be at the center of Experian's annual breach forecast for 2026, with the scope, frequency and cost of cyber incidents heavily influenced by the technology.
AI makes its way into many of the predictions in Experian's Data Breach Industry Forecast. Michael Bruemmer, vice president of global data breach resolution, and Jim Steven, head of crisis & data response services, UK, said agentic AI systems could be exploited by savvy hackers who might inject their AI agents "to disrupt the orchestration or governance of the victim's AI agents.
"At a minimum, this disruption could impact an organization's operations or siphon money, goods, or information," or perform ransomware-like operations, said Experian. "AI agents are the next frontier for fraud and cybercrime, and we predict this may overtake human error as the leading cause of data breaches."
With the use of AI, hackers might also be able to extract data at an unprecedented rate and "stitch together enriched identity profiles." Experian warns: "Get ready for a potentially massive spike in identity theft." Or, AI capabilities could bolster the spread of mutating malicious code—polymorphic or metamorphic malware. (continua…)
https://www.insurancejournal.com/news/national/2026/01/13/854019.htm
INSURANCE JOURNAL - *Chad Hemenway -. January 13, 2026*

Dati, AI e 5G: la corsa all'edge computing entra nella fase decisiva
Latenza, banda e sovranità dei dati spingono imprese e PA verso l'edge computing: calcolo vicino alla fonte, AI in tempo reale e 5G come piattaforma abilitante. Il cloud si frammenta in nodi distribuiti tra industria, sanità, smart city e infrastrutture critiche. La storia dell'informatica è scandita da un movimento pendolare costante tra centralizzazione e decentralizzazione, che è passato dai mainframe monolitici degli anni '60 ai personal computer distribuiti degli anni '80, per poi tornare alla centralizzazione massiccia con l'era del Cloud Computing iniziata a metà degli anni 2000.

Oggi, mentre ci avviciniamo alla metà del decennio 2020, il pendolo sta oscillando nuovamente, e con forza, verso la periferia, provocando una frammentazione ed estensione capillare del Cloud che, di fatto, apre l'era dell'Edge Computing.

Nel 2024 e 2025, l'Edge Computing ha smesso di essere una semplice un esperimento di laboratorio per diventare un imperativo architettonico fondamentale per la sopravvivenza digitale delle imprese, che devono affrontare una sfida semplice ma rivoluzionaria: spostare l'elaborazione dei dati il più vicino possibile alla fonte che li genera, sia essa un braccio robotico in una fabbrica tedesca, una telecamera semaforica a Barcellona, o un dispositivo a ultrasuoni in una clinica rurale dello Zambia.
Le ragioni di questo spostamento sono estremamente pragmatiche ed in qualche modo "brutali": la latenza della rete, i costi di banda esorbitanti e la sovranità dei dati non permettono più di inviare terabyte di informazioni grezze a data center distanti migliaia di chilometri per l'elaborazione.
Il mercato globale riflette questa urgenza con cifre che raccontano una storia di crescita esplosiva e diversificata.
Basti pensare che

- le previsioni di "MarketandMarket" indicano che l'edge computing raggiungerà i 168,4 miliardi di dollari nel 2025, con una crescita composta (CAGR) che potrebbe portare la cifra a quasi 250 miliardi entro il 2030, spinta dall'adozione dell'AI democratizzata e dell'analitica in tempo reale.
- secondo le stime più aggressive di "Grand View Research" si potrebbe arrivare addirittura a 327 miliardi di dollari

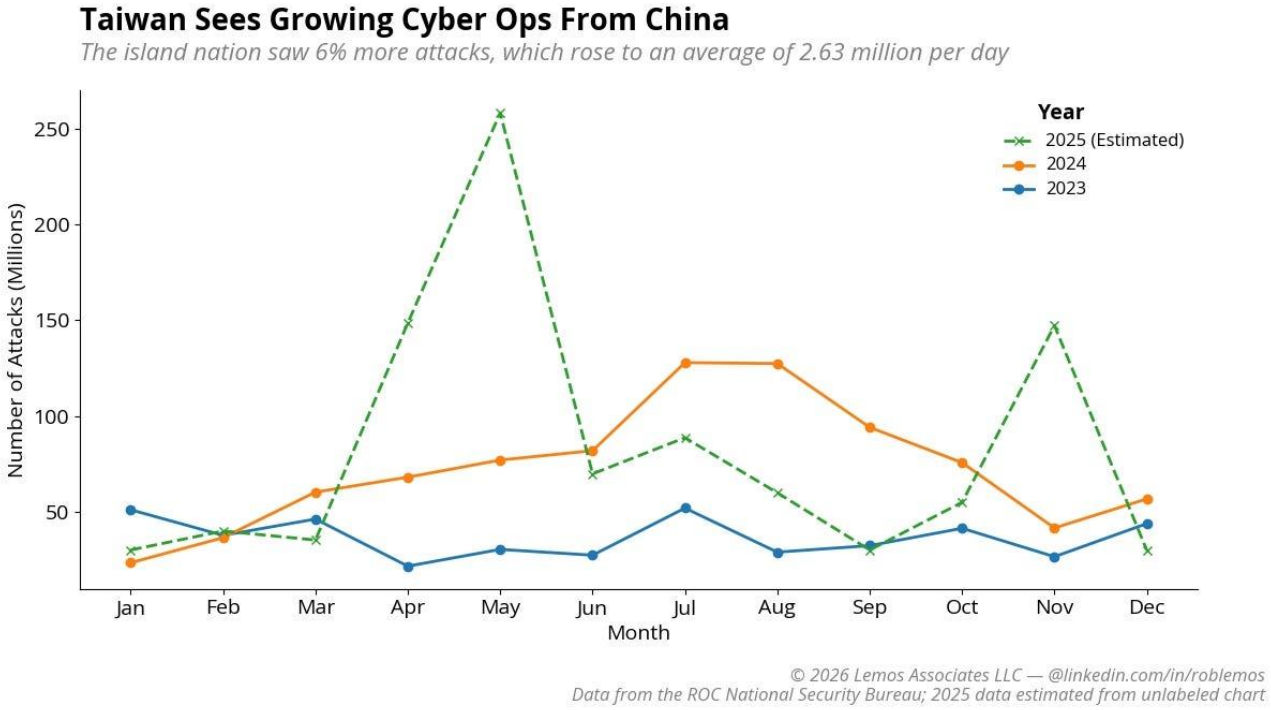
Come è di tutta evidenza, non si tratta semplicemente di installare server in periferia o di aggiungere qualche gateway IoT ma, al contrario, di ridisegnare la topologia stessa di Internet per supportare un mondo dove le macchine parlano con le macchine in millisecondi, prendendo decisioni autonome che impattano il mondo fisico.
L'adozione, allo stato attuale, non è uniforme, ma si muove a ondate settoriali: mentre il 40% delle grandi imprese prevede di adottare l'edge computing come parte integrante della propria infrastruttura IT entro il 2025, stiamo assistendo a una convergenza critica tra le tecnologie operative (OT) e quelle informatiche (IT).

Le aziende non possono più affidarsi esclusivamente alle regioni centralizzate degli hyperscaler in quanto necessitano di ambienti di colocation distribuiti e intelligenti che forniscano potenza, raffreddamento e connettività laddove serve davvero.
I provider che non abbracciano questo futuro rischiano l'obsolescenza, mentre quelli che si adattano diventeranno la spina dorsale delle città intelligenti, della sanità di nuova generazione e delle esperienze digitali immersive.
La spinta verso l'edge è ulteriormente accelerata dalla maturazione del 5G, che non funge solo da canale di trasmissione, ma svolge anche il ruolo fondamentale di piattaforma abilitante per servizi a bassissima latenza.
L'integrazione di AI e machine learning direttamente sui dispositivi periferici consente analisi più rapide e decisioni automatizzate senza la necessità di inviare dati sensibili al cloud, affrontando contemporaneamente problemi di privacy e costi di larghezza di banda.
Tuttavia, questa transizione non è priva di ostacoli: la sicurezza, l'interoperabilità tra dispositivi eterogenei e la gestione di flotte distribuite su scala globale rappresentano le sfide defining del prossimo quinquennio.
Indice degli argomenti

- Conclusioni e prospettive future (2026-2030)

Il Motore Tecnologico dell'Edge 2.0
Il 2025 ha rappresentato l'avvio della cosiddetta fase "Edge 2.0", caratterizzata dalla convergenza di tre vettori tecnologici che stanno ridefinendo le capacità computazionali alla periferia: l'Intelligenza Artificiale Generativa on-device (Edge AI), le reti 5G avanzate con capacità di slicing e le nuove architetture di processori neurali (NPU) e neuromorfici. (continua…)
https://www.agendadigitale.eu/infrastrutture/dati-ai-e-5g-la-corsa-alledge-computing-entra-nella-fase-decisiva/
AGENDADIGITALE - *Giuseppe Arcidiacono - 14 gen 2026*

Taiwan Endures Greater Cyber Pressure From China
Chinese cyberattacks on Taiwan's critical infrastructure — including energy utilities and hospitals — rose 6% in 2025, averaging 2.63 million attacks a day.
China's cyber-threat groups continue to ramp up their attacks on Taiwan, boosting cyber activity against the self-ruled island's critical infrastructure and seemingly conducting cyber operations during the majority of its joint military exercises targeting Taiwan.
As a result, Taiwan experienced an average of 2.63 million attacks every day in 2025, a 6% increase over the 2.46 million daily attack average targeting critical infrastructure the previous year, the National Security Bureau stated in a report published last week. Energy infrastructure suffered a 10-times increase in cyberattacks, while emergency rescue and hospital systems saw a 54% increase, the two largest increases in 2025.
The increasing attacks suggest "a deliberate attempt by China to compromise Taiwan's CI comprehensively and to disrupt or paralyze Taiwanese government and social functions," the NSB stated. "China's moves align with its strategic need to employ hybrid threats against Taiwan during both peacetime and wartime."
The report comes as the relationship between China and Taiwan suffered setbacks in the past year. China considers the island — a former Japanese colony that became independent when the Nationalist Party retreated to the island following its defeat in a civil war against the Chinese Communist Party in 1949 — as part of its territory. The island democracy, however, continues to resist political efforts to absorb it into the mainland. In December, the US committed to an $11 billion arms sale to Taiwan, and Japan's recently elected prime minister caused a kerfuffle by stating that if China attacked Taiwan, it would threaten Japan's survival and allow the country to exercise its right of self defense.



Attacks targeting Taiwan's critical infrastructure — and identified as coming from Chinese cyberthreat groups — peaked around two major political events. Source: ROC National Security Bureau

In the past year, cyberattacks have both coincided with political events — such as the one-year anniversary of the current president's inauguration — and correlated to some degree with the 40 joint combat readiness patrols (JCRP) conducted around Taiwan's territory by the People's Liberation Army. In nearly two dozen JCRPs, China's cyber operatives ramped up attacks against Taiwanese targets, the NSB stated in its report.

While the slight increase in daily attacks may not seem like an escalation, the fact that energy infrastructure and emergency services are increasingly targeted means that China is being more selective, says Collin Hogue-Spears, senior director of solution management at Black Duck, who has significant experience in both mainland China and Taiwan. (continua…)

https://www.darkreading.com/cyber-risk/taiwan-sees-greater-cyber-pressure-from-china

DARKREADING *- Robert Lemos - January 14, 2026*

NOTIZIE D'INTERESSE:

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

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

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	Glauco Bertocchi Silvano Bari 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.