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 2025 **n. 11/ 2025** **dicembre 2025**

Editoriale

Cari Soci,

con questo numero di fine anno vogliamo fermarci un momento a riflettere su quanto accaduto negli ultimi dodici mesi per mettere a fuoco ciò che il 2025 ci ha mostrato. Il 2025 è stato un anno che ha messo l'Europa – potremmo dire il mondo – di fronte a prove concrete. Eventi diversi per natura e contesto hanno avuto un denominatore comune: la difficoltà di garantire continuità operativa in sistemi sempre più interconnessi e sotto pressione.

In primavera, il blackout che ha interessato Spagna e Portogallo – con effetti anche in alcune aree della Francia meridionale – ha coinvolto decine di milioni di utenti, paralizzando trasporti, comunicazioni e servizi essenziali, mostrando come un guasto nella rete di trasmissione possa propagarsi rapidamente oltre i confini nazionali. Pochi mesi prima, in Cile, un malfunzionamento dei sistemi di protezione di una linea ad alta tensione aveva lasciato senza energia elettrica la quasi totalità del Paese, costringendo le autorità ad attivare misure di emergenza. In Brasile, a ottobre, l'incendio di una sottostazione ha causato un blackout esteso a tutti gli stati federali: in questo caso, la risposta operativa ha contenuto la durata dell'interruzione, ma non ha evitato interrogativi sulla gestione di eventi su scala nazionale.

Sul fronte digitale, il 2025 ha confermato una tendenza già evidente negli anni precedenti. I dati diffusi da centri di analisi e osservatori indipendenti indicano un aumento significativo degli attacchi ai sistemi IT e OT delle infrastrutture critiche, in particolare nel settore energetico.
Anche l'Italia è stata coinvolta in modo rilevante, con una crescita degli incidenti che hanno interessato trasporti, logistica e servizi essenziali, spesso in forme ibride tra hacktivismo, criminalità e pressione geopolitica.

Infine, il protrarsi degli attacchi alle infrastrutture energetiche ucraine ha continuato a ricordarci che, nei contesti di conflitto, le reti elettriche e i sistemi di distribuzione non sono solo asset tecnici, ma obiettivi strategici, con effetti diretti sulla popolazione civile e sulla stabilità dei servizi.

Da questi eventi emergono alcune lezioni operative difficili da ignorare.

La prima riguarda le interdipendenze: energia, telecomunicazioni, trasporti e servizi digitali non possono più essere analizzati separatamente. Un singolo punto di vulnerabilità è sufficiente a generare effetti a cascata.

La seconda è la definitiva convergenza tra sicurezza fisica e sicurezza cyber. Gli incidenti del 2025 mostrano che le due dimensioni si alimentano a vicenda e richiedono modelli di gestione integrati, non paralleli.

La terza lezione è legata alla preparazione operativa. Dove esistevano procedure aggiornate, ruoli chiari e capacità di decisione rapida, l'impatto degli eventi è stato contenuto. Dove questi elementi mancavano, anche guasti tecnicamente gestibili hanno prodotto conseguenze rilevanti.

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

Infine, il 2025 ha ribadito il valore della condivisione delle competenze. Nessun operatore, pubblico o privato, può affrontare da solo scenari complessi e dinamici come quelli che abbiamo osservato.
Con questo spirito guardiamo al 2026, consapevoli che la resilienza non si costruisce con dichiarazioni di principio, ma con analisi, metodo e lavoro continuo.

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.

ATTIVITA' DELL'ASSOCIAZIONE

RINNOVO ASSOCIATIVO ANNO 2026

Il 31 dicembre 2025 scadrà 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.

Il Consiglio Direttivo di AIIC ha deciso una facilitazione per chi si iscriverà come nuovo socio: a partire dal mese di ottobre 2025, pagando la relativa quota sociale, il nuovo socio avrà diritto a vedere la propria iscrizione valida fino a tutto l'anno 2026.

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

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.

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

NEWS E AVVENIMENTI

Come la Geomatica supporta la comprensione e la previsione degli impatti del cambiamento climatico - La prof.ssa Eufemia Tarantino (Politecnico di Bari) illustra le tecnologie geomatiche più efficaci per documentare, analizzare, e prevedere l'evoluzione del clima e dei suoi impatti sull'ambiente su scala locale e globale: dai satelliti ai droni, dall'IA ai Digital Twin ambientali.
Dall'osservazione satellitare ai rilievi UAV, dai modelli predittivi all'IA, la Geomatica offre oggi strumenti fondamentali per analizzare e prevedere gli effetti del cambiamento climatico su scala locale e globale. Ne abbiamo parlato con la prof.ssa Eufemia Tarantino, Ordinaria di Geomatica al Politecnico di Bari.

Tecnologie geomatiche integrate per l'analisi multiscala degli effetti del clima sull'ambiente

Prof.ssa Tarantino, quali tecnologie geomatiche sono oggi più efficaci per documentare e analizzare il cambiamento climatico su scala locale e globale?

Le tecnologie geomatiche attualmente utilizzate per le analisi sui cambiamenti climatici a scala locale e globale si distinguono per la complementarità tra osservazione da satellite, rilievo locale (UAV, GNSS), sistemi GIS e modelli predittivi. La loro sinergia consente il monitoraggio continuo e multiscala, l'analisi predittiva dei rischi e il supporto alle decisioni per la mitigazione e l'adattamento.

L'ausilio fornito dalle tecniche del telerilevamento sta cambiando il modo in cui comprendiamo gli effetti dei cambiamenti climatici e addirittura riusciamo a prevederli sulla base di osservazioni tempestive e complete dell'atmosfera, dei mari e della superficie terrestre.

La capacità dei modelli climatici di esaminare grandi moli di dati, per cogliere tendenze, irregolarità o stabilità nelle analisi a lungo termine, è infatti irrobustita dall'uso dei dati geospaziali satellitari, poiché essi conducono al perfezionamento dell'interpretazione e della validazione dei risultati. Questa capacità è particolarmente cruciale nel quadro degli studi globali sugli accordi sul clima, in cui i dati devono essere accurati e trasparenti per poter monitorare il rispetto degli impegni e i progressi conseguiti nel raggiungimento degli obiettivi degli accordi sul clima e, di conseguenza, per validare il successo e l'efficacia delle misure adottate.

La complementarità di tutte le tecnologie geomatiche è resa fattibile all'interno dei Sistemi Informativi Geografici (GIS), concepiti come piattaforme fondamentali per l'integrazione, l'analisi geospaziale e la modellazione dei dati ambientali. I sistemi WebGIS e le piattaforme cloud (es. Google Earth Engine, ArcGIS Online) attualmente disponibili in Internet permettono ulteriori elaborazioni geospaziali, mediante modelli collaborativi e accesso gratuito ai dataset globali.

(continua…)

https://www.ingenio-web.it/articoli/come-la-geomatica-supporta-la-comprensione-e-la-previsione-degli-impatti-del-cambiamento-climatico/

IngenioWeb – *Dalila Cuoghi | Eufemia Tarantino 18-giugno 2025*

Riconosceremo l'intelligenza artificiale generale quando la vedremo? - L'arrivo dell'intelligenza artificiale generale segna un nuovo paradigma nella gestione della sicurezza: sarà un alleato indispensabile nella gestione dei rischi più complessi. A cura del Dott. Mario Ferraioli.

Negli ultimi anni, il dibattito sull'intelligenza artificiale generale (AGI) — ovvero la capacità di un sistema di eguagliare l'intelligenza umana nella maggior parte dei compiti — si è intensificato. Esperti dei principali laboratori, tra cui OpenAI, Google DeepMind e Anthropic, stimano che il traguardo possa essere raggiunto entro pochi anni. La questione centrale non è più soltanto quando, ma come misurare e impiegare queste capacità, in particolare in settori critici come la sicurezza sul lavoro.

L'AGI, se realizzata, promette di trasformare profondamente l'organizzazione dei cantieri, degli impianti industriali e dei trasporti. Sistemi dotati di intelligenza fluida, capacità di adattamento e comprensione causale potrebbero monitorare ambienti complessi, prevenire incidenti e supportare decisioni operative in tempo reale. Ad esempio, un cantiere edile ad alto rischio potrebbe beneficiare di un AGI in grado di rilevare comportamenti non sicuri, verificare la corretta applicazione delle procedure di sicurezza e segnalare immediatamente situazioni di pericolo, come cadute potenziali, sovraccarichi o errori nella movimentazione di macchinari.

Definire e misurare l'intelligenza artificiale resta però complesso. I test tradizionali di QI valutano memoria, ragionamento logico e competenze linguistiche, ma non catturano le capacità necessarie per operare in contesti dinamici e pericolosi. Come osserva Geoffrey Hinton, premio Nobel per l' intelligenza artificiale, "stiamo costruendo esseri alieni": le macchine ragionano secondo logiche che non

corrispondono agli schemi cognitivi umani, e questo vale anche per la gestione della sicurezza sul lavoro.
Nel corso degli anni, sono stati sviluppati diversi benchmark per valutare l'AGI. Il test di Turing, ideato nel 1950, non basta più. François Chollet, fondatore della ARC Prize Foundation, ha creato l'Abstraction and Reasoning Corpus (ARC) e le sue evoluzioni ARC-AGI-2 e ARC-AGI-3. Questi test richiedono di dedurre regole da pochi esempi e applicarle in nuovi contesti, simulando in parte la capacità di adattamento richiesta anche nei contesti lavorativi complessi. Sebbene le macchine mostrino ancora limiti evidenti, il progresso è tangibile, e le applicazioni pratiche cominciano a delinearsi.
(continua…)
https://www.puntosicuro.it/robotica-intelligenza-artificiale-C-137/riconosceremo-l-intelligenza-artificiale-generale-quando-la-vedremo-AR-25872/
***Punto Sicuro** – Mario Ferraioli, 1 dicembre 2025*

Quel cloud indispensabile che non sappiamo difendere al meglio - Le aziende investono nella sicurezza cloud più che mai, eppure faticano a proteggerla efficacemente. Ce lo rivela l'ultimo Thales Cloud Security Study, mentre l'AI generativa introduce nuove pressioni sui sistemi di protezione dati
Il **cloud** è ormai fondamentale per le aziende moderne, ma molte organizzazioni faticano ancora a sviluppare le competenze necessarie per proteggerlo efficacemente.
Inoltre, la diversità dei controlli tra i vari provider e l'approccio specifico richiesto dalla sicurezza cloud continua a mettere alla prova i team di sicurezza.
Il recente **Thales Cloud Security Study** conferma una verità scomoda: mentre le organizzazioni danno priorità agli investimenti nella sicurezza del cloud, la crescente complessità, l'aumento della pressione legata all'intelligenza artificiale e l'ampliamento delle lacune nella protezione dei dati le stanno mettendo a rischio.
E, con un aumento dei dati, delle applicazioni e dei carichi di lavoro che si spostano sul cloud, la posta in gioco non è mai stata così alta. Pertanto, la maggior parte delle organizzazioni necessita di progressi significativi nella protezione dei dati cloud, **una sfida amplificata dall'avvento dell'intelligenza artificiale**.
Indice degli argomenti

2025 Thales Cloud Security Study: a che punto siamo
Thales Cloud Security Study è scaturito dalle interviste di circa 3.200 professionisti in 20 paesi e fornisce una visione completa delle sfide, delle priorità e dei progressi delle organizzazioni che gestiscono la sicurezza del cloud.
Lo studio conferma che, mentre le organizzazioni danno priorità agli investimenti nella **sicurezza del cloud**, la crescente complessità, le sfide nella protezione delle proprie risorse cloud, un problema ulteriormente amplificato dalle esigenze dei progetti di intelligenza artificiale che spesso operano nel cloud e richiedono l'accesso a grandi volumi di dati sensibili.

Ad aggravare questo problema, **quattro delle prime cinque risorse prese di mira negli attacchi segnalati sono basate sul cloud**. Ne consegue che il rafforzamento della sicurezza del cloud e la semplificazione delle operazioni sono passaggi essenziali per migliorare l'efficacia e la resilienza complessive della sicurezza. (continua…)
https://www.cybersecurity360.it/outlook/quel-cloud-indispensabile-che-non-sappiamo-difendere-al-meglio/
Cybersecurity360 - *Federica Maria Rita Livelli - 3 dic 2025*

CISA Publishes Security Guidance for Using AI in OT - Global cybersecurity agencies published guidance regarding AI deployments in operational technology, a backbone of critical infrastructure.
A collection of agencies have published guidance on the best way to defend AI deployments in operational technology (OT).
Such guidance seems necessary, given that on their own, AI and OT environments are two of the most sensitive, high-profile attack surfaces. AI is a prime target, due to the wide range of attack techniques emerging constantly, and OT because of its use in critical and industrial settings.
The guidance was authored by the US's CISA, FBI, and NSA Artificial Intelligence Security Center; the Australian Signals Directorate's Australian Cyber Security Centre; the Canadian Centre for Cyber Security; the German Federal Office for Information Security; the Netherlands National Cyber Security Centre; the New Zealand National Cyber Security Centre; and the UK's National Cyber Security Centre.
As the 25-page document explained, large language model (LLM) deployments potentially can be used to increase efficiency and enhance decision making, but integrating AI into critical OT environments "also introduces significant risks — such as OT process models drifting over time or safety-process bypasses — that owners and operators must carefully manage to ensure the availability and reliability of critical infrastructure."
The guidance aims to help operators understand AI and how it might be best used in OT environments; establish AI governance and assurance frameworks; and embed safety and security practices into OT-AI integrations. In OT settings, AI is used to analyze critical data, identify signs of anomalies in things like SCADA systems, provide system recommendations for operator decision making, optimize workflows, and more.
Elements of the guidance, particularly those that involve understanding how to best deploy AI technology, are reminiscent of previous recommendations from public sector agencies. For example, the UK government recently published guidelines on how to best utilize AI-powered coding tools in His Majesty's Government.
Richard Springer, senior director of OT solutions at Fortinet (a vendor that contributed to the guidance), says widespread AI deployment in OT environments is limited. Most, he says, are still focused on foundational cybersecurity such as segmentation, asset visibility, patching, and basic detection and response. But because the stakes are so high, generative AI (GenAI) is less of a "not yet" and more a "never" for many operators, he adds.
"That said," Springer continues, "there's broad agreement that GenAI will eventually play a meaningful role: accelerating playbooks, assisting with diagnostics, supporting predictive maintenance, and helping operators manage increasingly complex environments. But any automation in OT must be bounded by a clear understanding of cause-and-effect, risk tolerances, and the absolute priority of safety and uptime, especially when people and critical infrastructure are on the line."(continua…)
https://www.darkreading.com/cybersecurity-operations/cisa-publishes-security-guidance-ai-ot
Dark Reading - *Alexander Culafi - December 4, 2025*

Cavi sottomarini e Spazio, Butti alza l'allerta: "Serve protezione europea immediata" - Il Sottosegretario alla Presidenza del Consiglio con delega all'Innovazione e alla Transizione digitale, richiama l'urgenza di agire su cavi sottomarini e infrastrutture spaziali: "Sono frontiere strategiche per sicurezza e competitività. L'Europa deve accelerare su regole, cooperazione e investimenti per non restare indietro rispetto a Stati Uniti e Asia"

"Le infrastrutture spaziali e sottomarine sono nuovi territori sovrani e dobbiamo difenderli con la stessa determinazione con cui difendiamo gli spazi terrestri". Con questa frase, pronunciata a Roma alla conferenza Space&Underwater – Space Economy, Submarine Cables & Cybersecurity, Alessio Butti, sottosegretario alla Presidenza del Consiglio con delega all'Innovazione e alla Transizione digitale, ha messo il tema cavi sottomarini e spazio al centro dell'agenda europea. E ha avvertito: "Non è più tempo di ritardi rispetto a Stati Uniti e altre aree del mondo".

Indice degli argomenti

Cavi sottomarini: la spina dorsale dell'Internet e le vulnerabilità del sistema

I cavi sottomarini trasportano la quasi totalità del traffico dati internazionale. Un milione e trecentomila chilometri di dorsali attraversano oceani e mari, con punti di approdo che diventano obiettivi delicati. Butti ha elencato rischi concreti: fondali saturi di dorsali, danni da pesca a strascico e un numero ridotto di navi in grado di eseguire riparazioni tempestive. In un contesto di tensione geopolitica, ogni interruzione può generare impatti economici e instabilità nei flussi digitali.

Il sottosegretario chiede una risposta europea coordinata. Propone di "costituire una flotta di pronto intervento", capace di intervenire rapidamente sulle dorsali, e invita a costruire un patto nel Mediterraneo con Paesi "like-minded" per condividere sorveglianza, manutenzione e standard tecnici. Per Butti, la resilienza delle infrastrutture sottomarine è un tassello della sovranità digitale. (continua)

https://www.corrierecomunicazioni.it/cyber-security/cavi-sottomarini-e-spazio-butti-alza-lallerta-serve-protezione-europea-immediata/

Corcom - *Veronica Balocco, 4 dic 2025*

Autostrade dell'energia: 8 corridoi critici e infrastrutture UE da accelerare - La nuova iniziativa UE intende rafforzare reti, interconnessioni e idrogeno accelerando i progetti più urgenti per completare l'Unione dell'energia.

La Commissione UE lancia le Autostrade dell'energie: 8 corridoi critici e infrastrutture da accelerare

Indice dei contenuti

Autostrade dell'energia, la nuova rotta UE per collegare elettricità e idrogeno

La Commissione Europea ha presentato una proposta di intervento operativo denominato “Autostrade dell’energia” che, insieme al “Pacchetto reti europee“, individua e accelera otto corridoi infrastrutturali strategici necessari per evitare ritardi nella transizione energetica e completare la rete europea.
Secondo la Commissione, molte infrastrutture energetiche europee non avanzano abbastanza rapidamente rispetto alla crescita delle rinnovabili, mentre diversi Stati membri sono lontani dall’obiettivo di interconnessione del 15% entro il 2030.
Le strozzature comportano rischi economici significativi, con costi di congestione che hanno raggiunto 5,2 miliardi di euro nel 2022 e che potrebbero arrivare a 26 miliardi entro il 2030. Le autostrade dell’energia operano quindi come una corsia preferenziale dell’Unione per accelerare i progetti energetici transfrontalieri più urgenti attraverso governance dedicata, strumenti finanziari e procedure autorizzative più rapide.
(continua)
https://www.rinnovabili.it/energia/infrastrutture/autostrade-dell-energia-ue/
Rinnovabili *– Alessandro Petrone, 11 Dicembre 2025*

Why a 17-Year-Old Built an AI Model to Expose Deepfake Maps
A high-school student is tackling the overlooked risk of AI-generated satellite imagery that could mislead governments and emergency responders.
When a deepfake targeted him personally, Vaishnav Anand panicked. But when everything settled down, he turned that panic into purpose.
The California high-school junior was inspired by the incident to ask a different question than most: If people already doubt celebrity videos and viral images, what about the satellite maps that governments and corporations quietly trust every day? If these could be altered to create distortions, such as faking natural disasters or hiding weak infrastructure, that could have serious effects, he pondered.
"I began because I was a victim of a deepfake, and it kind of made me realize how easily something true can be absolutely manipulated with AI and look so realistic," he says.
In the months that followed, Anand turned that shock into a research project he recently presented at the IEEE Undergraduate Research Technology Conference at the Massachusetts Institute of Technology. The project focuses on how to detect altered satellite imagery before it can distort public decisions.
His work fills a gap in a field with surprisingly little research. Only a handful of studies have explored what some scientists now call "deepfake geography." One 2021 paper showed how artificial intelligence can blend features from one city into the satellite imagery of another to create convincing but false landscapes.
Why Geospatial Deepfakes Matter
Anand first explored voice and face forensics before widening his focus to geospatial data, recognizing how it underpins everything from disaster response to national security planning. Through his work on the National 4-H Geospatial Team, he learned to "take every point as data" and to interpret maps and satellite imagery with precision.
Anand says he was surprised by how little research exists on detecting manipulated satellite imagery — despite the fact that the potential consequences could be "catastrophic," he says.
"Satellite imagery is really a national security issue," he says, adding that if adversaries can alter even a "little bit of that data," the downstream impact on infrastructure and government decisions could be severe. (continua…)
https://www.darkreading.com/threat-intelligence/why-17-year-old-built-ai-expose-deepfake-maps
Dark Reading - *Joan Goodchild, - December 16, 2025*

Bolla AI, grande opportunità per l'Europa: ecco come sfruttarla - Il dibattito sulla bolla AI nasconde una questione strategica: chi sarà pronto dopo la correzione? L'Europa può trasformare il rallentamento del mercato in vantaggio competitivo puntando su qualità, auditabilità e AI settoriali. Marietje Schaake analizza rischi e opportunità di una transizione che richiede coordinamento istituzionale rapido

La discussione **sul possibile scoppio della bolla AI** è diventata onnipresente, ma raramente va oltre la speculazione su tempistiche e conseguenze. Marietje Schaake, ex europarlamentare e studiosa di tecnologia e democrazia a Stanford, propone una lettura diversa: **il punto non è prevedere lo scoppio, ma capire chi sarà attrezzato per trasformare la correzione in opportunità strategica.**

Indice degli argomenti

La scorciatoia narrativa della "bolla dell'AI"

La Schaake sostiene che una correzione dell'"AI trade" – la "scommessa di Borsa" sull'AI: l'allocazione di capitale basata sull'idea che l'intelligenza artificiale sarà il grande motore di crescita dei prossimi anni – aprirà uno spazio per un modello europeo fondato su fiducia, sicurezza e applicazioni settoriali. Un argomento potente perché sposta la discussione dalla finanza alla governance: il vero rischio per l'UE non è lo scoppio della bolla, ma arrivare anche questa volta senza una linea univoca e senza strumenti operativi all'altezza.

L'idea di **"bolla dell'AI"** è infatti diventata una scorciatoia narrativa, un'etichetta che serve per spiegare l'euforia dei mercati, criticare le Big Tech o anticipare un imminente bagno di sangue. Marietje Schaake prova a sottrarre il tema a questa semplificazione e a ricondurlo alla sua dimensione più interessante: non tanto la domanda "scoppierà o no?", quanto la domanda "chi sarà pronto quando accadrà?".(continua…)

https://www.agendadigitale.eu/mercati-digitali/oltre-il-panico-da-bolla-ai-perche-leuropa-puo-guadagnarci-e-come/

Agenda Digitale -*Maurizio Carmignani - 16 dic 2025*

Intelligenza artificiale per fare le leggi, il caso del Senato italiano - Un documento del Senato racconta come l'IA generativa stia entrando, per sperimentazioni progressive, nelle diverse fasi del processo legislativo. Dalla classificazione degli atti alla gestione degli emendamenti, fino a trascrizioni e ricerca sul sito, resta fermo un principio: decisione e responsabilità sono sempre umane

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

La settimana scorsa è stato pubblicato sul sito del Senato un PDF scaricabile, titolato **"L'intelligenza artificiale in Senato. Sperimentazioni, opportunità e risultati nelle diverse fasi del processo legislativo – documento di analisi 34"**. Un titolo **intrigante**, che incuriosisce subito e invita ad andare oltre gli slogan.
Il documento spiega che sin dagli anni '70 il Senato della Repubblica ha affrontato la necessità di **gestire, classificare e pubblicare** un'enorme quantità di documenti attraverso tecnologie informatiche. Dal 2023, però, è stata avviata un'**analisi strutturata** per integrare tecnologie di **IA generativa**, basate **su Large Language Model (LLM),** con le funzioni del Senato stesso.

Indice degli argomenti

Intelligenza artificiale in Senato: dati, trasparenza e LLM "nazionali"

Dato atto dei problemi legati alla **qualità** e alla **trasparenza** dei dati di addestramento dei modelli commerciali (prevalentemente statunitensi), il Senato ha assunto un ruolo **strategico** nel promuovere lo sviluppo di "intelligenze artificiali generative" nazionali.
In questa prospettiva, mette a disposizione **resoconti, dossier e pubblicazioni ufficiali** (attraverso il portale open data **dati.senato.it**) e lavora allo sviluppo di LLM tramite **accordi con università e centri di ricerca**, con l'obiettivo di rafforzare affidabilità e controllo sul patrimonio informativo pubblico.

Usare l'AI per scrivere le leggi: supporto, non sostituzione

L'AI viene oggi utilizzata anche nel processo legislativo come **strumento di proposta**, lasciando però la decisione finale e la **responsabilità** agli utenti umani. È un punto essenziale: l'IA supporta, suggerisce e accelera, ma non "firma" né sostituisce le scelte che restano in capo agli organi competenti.
Vediamo allora, in sintesi, l'**iter legislativo** e il supporto dell'AI lungo le diverse fasi operative, come ricostruito nel documento richiamato. (continua…)
https://www.agendadigitale.eu/documenti/intelligenza-artificiale-per-fare-le-leggi-il-caso-del-senato-italiano/
Agenda Digitale *- Silvia Stefanelli - 17 dic 2025*

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

Quando i sistemi di intelligenza artificiale possono collassare - La possibilità di degradazione esiste e le conseguenze potrebbero impattare su più fronti: affidabilità dei dati, sicurezza e modelli economici. Gli esperti: attenti, in alcuni casi si rischia di non poter più tornare indietro

L'onda di entusiasmo per i **sistemi di intelligenza artificiale generativa** (i cosiddetti **Large Language Model,LLM**) è ancora nel pieno della sua fase crescente, tanto che le aziende potrebbero ricorrervi a piene mani spinte da messaggi di marketing e da report che ne evidenziano caratteristiche e peculiarità, con costi che sembrano suggerire maggior convenienza rispetto alla forza lavoro umana.

Premesso che, come sempre, non è tutto oro quello che luccica, le AI hanno delle **significative limitazioni rispetto alle prerogative umane**. Quest'ultime, infatti, non sono immediatamente sostituibili se non in pochi casi ristretti, ma sembra esserci di più: si chiama "collasso dei sistemi di AI" ed è un significativo e progressivo problema segnalato fin dal 2023 da diversi gruppi di ricercatori e rivalutato e misurato dai ricercatori Apple qualche mese fa (fonte: *The Register*).

Le conseguenze di **sistemi digitali di AI soggetti a collasso** potrebbero avere impatti critici in ambito sicurezza e privacy.

Indice degli argomenti

I rischi di degradazione e di competizione sul mercato

Con la definizione **"Collasso dei sistemi di AI" si indica il fenomeno in cui i modelli di apprendimento automatico (machine learning) si degradano gradualmente a causa di errori derivanti da un addestramento non accurato dei sistemi di AI**, che appaiono quindi, contaminati.

I dati puliti creati da esseri umani, che fino a qualche tempo fa hanno costituito la fonte preferenziale dell'apprendimento, sono stati sostituiti o aggiunti da tanti, anche troppi strati di contenuti sintetici.

Questo ha reso progressivamente complesso l'addestramento di nuovi modelli e ha causato la comparsa di errori ricorsivi.

Il problema non è solo relativo alla qualità del dato per l'apprendimento: dato che dovrebbe essere pulito, anonimizzato perché sia fruibile per l'apprendimento la prima volta.

Il problema descritto in vari paper di ricerca (**sofferenza degli LLM su loop di autoaddestramento**, **declino della diversità linguistica**, **maledizione della ricorsione**) è anche relativo al riuso continuo di dati sporchi: insiemi di dati (chiamato corpus) usati per l'addestramento di sistemi di AI che sono contaminati da dati sintetici prodotti da altre AI.

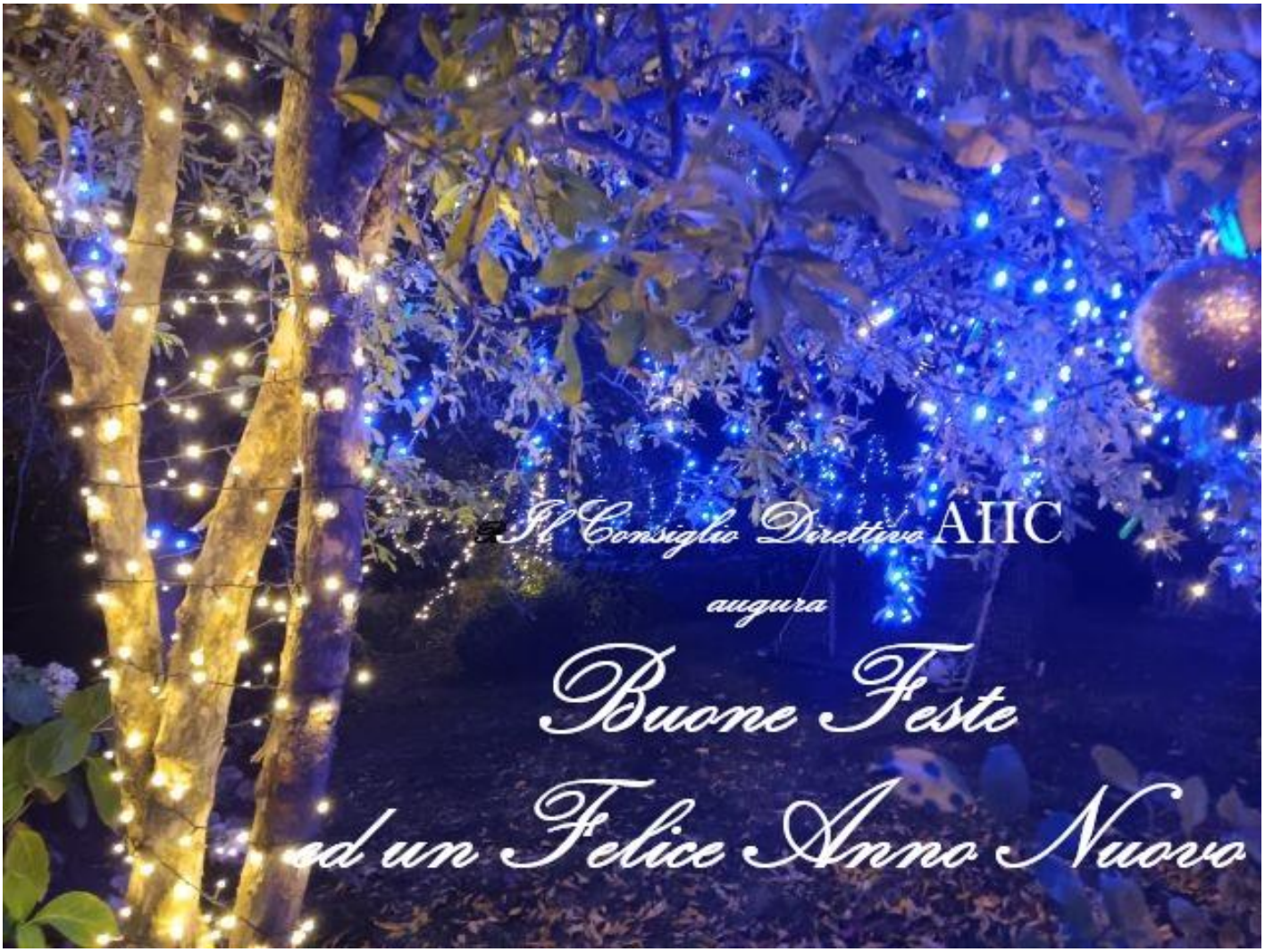
Oppure corpus che si auto-alimentano di dati auto-prodotti. E così via ciclicamente. Il tutto ha delle conseguenze catastrofiche e descritte come "Disturbo dell'Autofagia dei Modelli" (**Model Autophagy Disorder – MAD**).

Nello studio che tratta del MAD si evidenzia come "in tutti gli scenari esaminati, senza un numero sufficiente di dati reali aggiornati ad ogni generazione di ciclo, che riprende in ingresso i propri dati (autofago *n.d.r.*), i futuri modelli generativi sono destinati a vedere la loro qualità (precisione) o diversità (richiamo/varianza) diminuire progressivamente". Questa condizione è stata chiamata "Modello generativo autoconsumante impazzito", facendo un'analogia con la malattia della mucca pazza. (continua…)

https://www.cybersecurity360.it/outlook/quando-i-sistemi-di-intelligenza-artificiale-possono-collassare/

AGENDA DIGITALE - *Alessia Valentini - 17 dic 2025*

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



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.

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.

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

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.