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. 3/ 2026** **marzo 2026**

Il caso dello Stretto di Hormuz

In un'ipotetica classifica degli argomenti più discussi del mese, lo Stretto di Hormuz si collocherebbe certamente ai primi posti. L'area è tornata infatti al centro della scena internazionale in quanto nodo critico del sistema energetico globale: parliamo di un choke point attraverso cui transita stabilmente una quota compresa tra il 20% e il 25% del petrolio mondiale via mare, oltre a una parte significativa del GNL diretto verso Europa e Asia. E, soprattutto, non esistono rotte alternative in grado di assorbirne rapidamente i volumi. Quando la capacità di transito dello stretto viene compromessa, si attivano immediatamente effetti a catena: incremento dei premi assicurativi marittimi (war risk), riallocazione delle flotte, congestione nei porti alternativi, volatilità dei prezzi spot e pressione sulle riserve strategiche.

Negli ultimi anni, la letteratura sulle infrastrutture critiche ha insistito correttamente su concetti come resilienza, robustezza e capacità di recovery. Tuttavia, il caso dello Stretto di Hormuz evidenzia un limite di questo approccio quando viene applicato in modo isolato: la minaccia non è da intendersi soltanto disruption-driven (guasti, attacchi cyber, eventi naturali), ma sempre più spesso intention-driven, cioè legata a strategie di attori statuali o para-statuali.

Se traduciamo questo concetto nel linguaggio delle infrastrutture critiche europee, il parallelismo è immediato. Reti elettriche interconnesse, dorsali del gas, backbone digitali e cavi sottomarini, nodi logistici multimodali: tutti questi sistemi presentano caratteristiche analoghe ai choke points globali, ovvero alta centralità topologica, bassa sostituibilità e forte effetto di propagazione del rischio.

Dal punto di vista tecnico, si tratta di asset con: elevato grado di interdipendenza intersettoriale, bassa elasticità operativa nel breve termine, forte esposizione a effetti di cascading failure, asimmetria tra costo dell'attacco e impatto sistemico.

In questo contesto, la distinzione tradizionale tra sicurezza fisica, sicurezza informatica e sicurezza operativa diventa sempre meno significativa. Le minacce contemporanee operano simultaneamente su più livelli: interferenze nei sistemi di navigazione, attacchi a supply chain digitali, sabotaggi fisici mirati, pressione normativa o economica.

Lo Stretto di Hormuz rappresenta quindi un modello di riferimento per comprendere come infrastrutture apparentemente "esterne" al perimetro nazionale possano avere un impatto diretto sulla sicurezza energetica e sulla continuità dei servizi essenziali.

Per l'Italia, fortemente dipendente da importazioni energetiche e inserita in reti infrastrutturali europee complesse, questo scenario impone alcune riflessioni operative.

La prima riguarda la valutazione del rischio: i modelli tradizionali, spesso basati su probabilità storiche e scenari lineari, faticano a incorporare variabili geopolitiche dinamiche. È necessario integrare strumenti di scenario analysis e stress testing che considerino esplicitamente l'indisponibilità di tali choke points globali.

La seconda riguarda la ridondanza e diversificazione: non solo in termini di fonti energetiche, ma anche di rotte, fornitori e modalità di trasporto. In questo caso, tuttavia, è fondamentale riconoscere che la ridondanza completa, in sistemi globalizzati, è economicamente e tecnicamente irrealistica.

La terza – forse la più critica – riguarda la governance. La gestione del rischio sistemico richiede coordinamento tra operatori di infrastrutture critiche (OES), autorità nazionali competenti e organismi sovranazionali. In ambito europeo, questo si traduce anche nell'attuazione concreta della Direttiva NIS2 e nel rafforzamento delle capacità di risposta congiunta.
Infine, emerge con forza il tema della consapevolezza strategica. Gli operatori infrastrutturali non possono più considerarsi soggetti puramente tecnici: gestiscono nodi che, in determinate condizioni, assumono rilevanza geopolitica. Questo implica l'integrazione di competenze di intelligence, analisi geopolitica e risk anticipation nei processi decisionali.
Per chi opera in questo settore, la sfida non è soltanto garantire la continuità operativa, ma comprendere e gestire il ruolo strategico delle infrastrutture all'interno di un contesto globale sempre più instabile e interdipendente.

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.

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.

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

WEBINAR

Artificial Intelligence and Climate Change

14 aprile 2026 alle ore 15.00.

AIIC, in collaborazione con Isaca Roma, organizza un nuovo webinar il giorno 14 aprile 2026 alle ore 15.00.
Oggetto del webinar è l'illustrazione del report "**Artificial Intelligence and Climate Change**" recentemente prodotto da un Gruppo di Lavoro AIIC coordinato da Sandro Bologna.
Riportiamo qui di seguito la locandina dell'evento.

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

Il webinar è aperto a tutti gli interessati, previa prenotazione all'indirizzo e-mail segreteria@infrastrutturecritiche.it entro e non oltre la data del 9 aprile 2026. A tutti coloro che si prenoteranno entro tale data verrà fornito il link per la partecipazione all'evento.

WEBINAR

Artificial Intelligence and Climate Change

Webinar a cura AIIC & ISACA Rome Chapter

14 Aprile 2026, ore 15:00

c/o Piattaforma GOTOMeeting

Il Rapporto esplora modi innovativi in cui l'IA può migliorare e accelerare l'azione per il clima, con particolare attenzione al processo decisionale e alle misure di adattamento per promuovere la resilienza contro gli impatti dei cambiamenti climatici. Esso offre uno spunto per il dialogo interdisciplinare, al fine di facilitare il coinvolgimento intersettoriale, identificare applicazioni in cui l'IA può orientare l'azione per prevenire e combattere i cambiamenti climatici. Per favorirne la diffusione il rapporto è redatto in lingua inglese

Obiettivo del Webinar è l'illustrazione del Rapporto e dei diversi aspetti che caratterizzano l'impatto derivante dall'utilizzo della Intelligenza Artificiale nel trattare il soggetto "Climate Change".

PROGRAMMA

15:00 - I GdL nella storia di AIIC *Silvano Bari*

15:10 – Applicazioni della Intelligenza Artificiale nel campo del Cambiamento Climatico: stato dell'arte *Sandro Bologna*

15:30 – Intelligenza Artificiale e Cambiamento Climatico tra passato, presente e futuro: cosa ci aspettiamo? *Alberto Stefanini*

15:50 – Come affrontare il tema dei consumi di acqua – energia nel campo della Intelligenza Artificiale, impatto della evoluzione tecnologica *Glauco Bertocchi*

16:10 – Intelligenza Artificiale: vincoli Normativi ed Etici *Adriana Peduto*

16:30 – Intelligenza Artificiale: la visione industriale *Lorenzo Vandoni*

16:50 – Conclusioni e chiusura del Webinar

Ricordiamo che il Report dedicato ai rapporti tra Intelligenza Artificiale e Cambiamenti Climatici è pubblicato sul sito dell'Associazione al seguente link:

AIIC-Artificial-Intelligence-and-Climate-Change-versione-finale-1.1-30gen2026.pdf

Questo Rapporto è il risultato di un progetto congiunto coordinato da Sandro Bologna e realizzato con il contributo di Silvano Bari, Glauco Bertocchi, Sandro Bologna, Gabriele Balzano, Luigi Carrozzi, Raffaella D'Alessandro, Tommaso Diddi, Elenio Dursi, Adriana Peduto, Beatrice Rosa, Alberto Stefanini, Cristina Turconi, Lorenzo Vandoni, Maria Beatrice Versaci.
L'intelligenza artificiale (IA) sta rapidamente ampliando le frontiere della climatologia, fornendo nuove informazioni sulla nostra comprensione del sistema climatico e contribuendo a trasformare la climatologia in un insieme di informazioni fruibili.
Il Rapporto esplora modi innovativi in cui l'IA può migliorare e accelerare l'azione per il clima, con particolare attenzione al processo decisionale e alle misure di adattamento per promuovere la resilienza contro gli impatti dei cambiamenti climatici.
Il Rapporto offre uno spunto per il dialogo interdisciplinare, al fine di facilitare il coinvolgimento intersettoriale, identificare applicazioni in cui l'IA può orientare l'azione per prevenire e combattere i cambiamenti climatici, e considerare come il più ampio impatto sociale dell'IA influenzi gli approcci per affrontare i cambiamenti climatici. In conclusione, l'IA rappresenta sia un'opportunità che una responsabilità. Se adeguatamente compresa, gestita e integrata, l'IA può contribuire a rendere le infrastrutture più resilienti, a una gestione più efficiente delle risorse e a strategie climatiche più consapevoli.
Il Gruppo di Lavoro auspica che questo Rapporto possa fungere da riferimento costruttivo per iniziative future e da punto di partenza per una più profonda cooperazione tra ricercatori, professionisti e istituzioni, tutti impegnati ad affrontare una delle sfide globali più significative del nostro tempo.

NEWS E AVVENIMENTI

"L'Europa si prepari a un riscaldamento di 3°C entro il 2100", avverte l'ESABCC - L'aggravarsi del cambiamento climatico in Europa impone di rafforzare la resilienza: l'appello del Comitato scientifico consultivo dell'UE.

Indice dei contenuti

Rafforzare la resilienza climatica: l'appello del Comitato scientifico consultivo dell'UE
Gli sforzi attuali sono insufficienti
L'Europa si scalda al doppio della velocità
Prepararsi a un riscaldamento di 3°C
Le 5 raccomandazioni per affrontare il cambiamento climatico in Europa
L'adattamento non può sostituire la mitigazione

L'Unione Europea non è preparata all'aggravarsi del cambiamento climatico e dovrebbe incrementare con urgenza gli investimenti necessari a proteggere i cittadini e le infrastrutture dagli eventi estremi, come inondazioni, incendi boschivi e ondate di calore. A causa del cambiamento climatico l'Europa è diventata il continente che si sta riscaldando più velocemente rispetto ad altre aree del mondo. Gli europei stanno già sperimentando quali sono gli effetti di tale mancanza di preparazione. Adattarsi a un futuro più caldo, però, è una sfida del tutto gestibile, anche se molto ardua da vincere.

Il nuovo rapporto, Rafforzare la resilienza al cambiamento climatico, suggerisce come l'Unione possa potenziare il proprio approccio di fronte a rischi climatici crescenti e sistemici. Il rapporto, cura del Comitato scientifico consultivo europeo sul cambiamento climatico (ESABCC), organo indipendente chiamato a fornire consulenza scientifica alle istituzioni UE, individua delle raccomandazioni per un quadro d'azione efficace in materia di adattamento. (continua…)
https://www.rinnovabili.it/clima-e-ambiente/cambiamenti-climatici/cambiamento-climatico-europa-riscaldamento-3c-adattamento/
Rinnovabili - *Erminia Voccia - 17 Febbraio 2026*

Enigma Cipher Device Still Holds Secrets for Cyber Pros
The Nazi relic's history is riddled with resilience errors, and those lessons still apply to
Enigma cipher machines have endured in the minds of history buffs and cryptography hobbyists for more than a century, still discovered at dusty French flea markets and dredged up from under beach sludge by treasure hunters. And a dive at this year's upcoming RSAC Conference into lessons the Enigma can teach today's defenders suggests cybersecurity professionals should keep the history of the Nazis' hubris and failure of imagination in mind.
The Enigma machine was created by German Arthur Scherbius in 1918 as a way to protect sensitive information coming across telegraph lines for banks and business. A quirky-looking typewriter, it could be used to code and decode messages easily. Scherbius's device was subsequently nationalized and modified by the Nazis to add even more complexity to the cryptography, and was used with wild success in the German war effort — until 1932, when Polish cryptographers secretly broke the code. The Polish team didn't share their findings until 1939, when it was given to British Intelligence and sent to The Government Code and Cipher School at Bletchley Park, where it was put to work against the Nazi army and is credited as a huge contributor to the Allied Forces victory.
Marc Sachs, who is senior vice president and chief engineer of the Center for Internet Security and a collector of Enigma machines, estimates that anywhere between 35,000 and 40,000 Enigma machines were produced. But fleetingly few remain: maybe 350 to 360, according to Sachs. Many of the devices were obliterated along the way by German army rifle butts, then burned and buried in a hole, preferably a latrine, to keep them out of Allied hands, he explained. (continua…)
https://www.darkreading.com/threat-intelligence/enigma-cipher-device-secrets-cyber-pros
Dark Reading - *Becky Bracken February 23, 2026*

Bug in Google's Gemini AI Panel Opens Door to Hijacking
Attackers could have exploited the vulnerability to escalate privileges, violate user privacy while browsing, and access sensitive resources.
Google has fixed a high-severity flaw in its implementation of Gemini AI in the Chrome browser that could have allowed attackers to escalate privileges, violate user privacy while browsing, and access sensitive system resources. Researchers said the vulnerability demonstrates new security hazards that come with the deployment and use of agentic browsers that have AI built in.
Specifically, the flaw tracked as CVE-2026-0628 could have allowed malicious browser extensions with only basic permissions to escalate privileges to access the victim's camera and microphone without consent; take screenshots of any website; and access local files and directories, according to a report published today by researchers from Palo Alto Networks' Unit 42, who discovered the flaw.
"The vulnerability put any user of the new Gemini feature in Chrome at risk of system compromise if they had installed a malicious extension," Gal Weizman, senior principal researcher, Palo Alto Networks,

tells Dark Reading. "Beyond individual users, the risk profile was significantly amplified within business and organizational environments."
In Chrome, the Gemini Live feature operates within a privileged browser side panel, granting it elevated capabilities to perform actions such as accessing on-screen content and interacting with local system resources to complete complex tasks. Indeed, many browsers now have agentic AI capabilities integrated into the browsing experience, allowing for quick dissemination of data, and executing complex, multistep operations that were previously impossible or required extensions and manual steps by the operator.
However, with this expanded capability and privileged access comes "a new and widened attack surface" that introduces new risks to both home and corporate users, Weizman wrote in the report. "This creates security implications that are not present in traditional browsers." (continua…)
https://www.darkreading.com/endpoint-security/bug-google-gemini-ai-panel-hijacking
Dark Reading **-** *Elizabeth Montalbano - March 2, 2026*

Iran, attacchi cyber e minacce sull'Italia: il fronte invisibile della crisi
Nella notte tra 28 febbraio e 1° marzo 2026, insieme alle operazioni militari, emergono attacchi cyber: crollo della connettività iraniana, defacement e manomissioni di app, attivazione di gruppi APT e rivendicazioni su ICS. Il rischio è una ritorsione asimmetrica verso target anche occidentali
La dimensione **cibernetica del conflitto** tra Israele, Stati Uniti e Iran rappresenta uno degli aspetti più **complessi** e strategicamente **rilevanti** della crisi in atto nel Medio Oriente. Nella notte tra il **28 febbraio** e il **1° marzo 2026**, in concomitanza con l'avvio delle operazioni militari convenzionali – denominate **"Operation Roaring Lion"** da parte israeliana e **"Operation Epic Fury"** da parte statunitense – si è registrata una serie di operazioni **cyber** di notevole portata.
Tra le prime evidenze documentate vi è il **crollo quasi totale** della connettività internet in Iran. Secondo **Doug Madory**, direttore dell'analisi internet presso la società **Kentik**, la connettività è precipitata in due distinte finestre temporali: la prima alle **07:06 GMT** e la seconda alle **11:47 GMT** del 1° marzo. **NetBlocks** ha a sua volta osservato un forte calo della connettività in coincidenza con l'inizio degli attacchi cinetici.
Il **Jerusalem Post**, citando fonti dell'intelligence occidentale, ha riferito di attacchi all'infrastruttura di comunicazione iraniana finalizzati a limitare la capacità delle forze armate di Teheran di **coordinarsi** e rispondere agli attacchi cinetici. Resta tuttavia da chiarire se l'interruzione sia stata causata da un'azione **cyber esterna** o da una misura difensiva adottata autonomamente dalle autorità iraniane, che in passato hanno già fatto ricorso al **"kill switch"** internet in situazioni di crisi interna.
Indice degli argomenti

- Attacchi cyber e operazioni offensive: defacement e app nel mirino
- Attribuzione e incertezza operativa nel dominio digitale
  - Segnali di pre-posizionamento e assenze "anomale"
- Attacchi cyber e rischio ICS: rivendicazioni e raccomandazioni
- Proxy, coalizioni e campagne di disturbo ad alto impatto
- Attori, settori esposti e continuità della minaccia
- Attacchi cyber e capacità residua: la logica dell'asimmetria
- Impatti e postura: implicazioni per aziende europee e italiane

Attacchi cyber e operazioni offensive: defacement e app nel mirino

Sul fronte delle operazioni offensive rivolte verso l'Iran, si segnala la manomissione (**defacement**) dell'applicazione religiosa **BadeSaba**, con oltre **cinque milioni di download** — sebbene non sia stata ottenuta una conferma ufficiale da parte della società sviluppatrice.
L'app ha iniziato a visualizzare messaggi del tipo **"È tempo di fare i conti"** e inviti rivolti alle forze armate a deporre le armi e unirsi alla popolazione civile. Secondo **Hamid Kashfi**, ricercatore di sicurezza e fondatore della società **DarkCell**, la scelta di colpire questa applicazione non è casuale: la sua base utenti è prevalentemente composta da sostenitori del governo, spesso di orientamento religioso osservante, rendendola un vettore di comunicazione strategicamente efficace. Contestualmente, diverse testate giornalistiche iraniane sono state **hackerate** per la diffusione di messaggi alternativi, in quello che appare come un tentativo strutturato di **operazioni di influenza** parallele all'azione militare (continua…).
https://www.agendadigitale.eu/sicurezza/iran-attacchi-cyber-e-minacce-sullitalia-il-fronte-invisibile-della-crisi/?utm_campaign=ad-sicurezza_nl_20260306&utm_source=ad-sicurezza_nl_20260306&utm_medium=email&sfdcid=0030O00002LXHlXQAX
Agenda Digitale *- Tommaso Diddi, Luisa Franchina - 2 mar 2026*

Gestione incidenti cyber nel settore aeroportuale: la strategia di SEA Milano - Tre sono le direttrici fondamentali: condivisione delle informazioni, ruolo del SOC, cultura dell'esercitazione costante. L'analisi di Thomas Piret, Head of ICT Security & Compliance della società.
Il panorama della sicurezza informatica per le infrastrutture critiche ha assunto una dimensione di urgenza che va ben oltre la semplice manutenzione tecnica.
Durante il convegno "Cybersecurity: immaginare l'imprevedibile", organizzato dall'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano, Thomas Piret, Head of ICT Security & Compliance di SEA Milano, ha offerto una panoramica dettagliata sulle dinamiche che regolano la gestione incidenti cyber in un ambiente ad altissima pressione come quello aeroportuale.
La discussione, che ha evidenziato la complessità del difendere realtà nevralgiche — specialmente dopo eventi di portata internazionale come le recenti Olimpiadi — ha messo in luce una realtà dove l'incidente non è più un'eventualità remota, ma un elemento da integrare nei processi operativi.
Piret ha esordito accogliendo con favore una definizione forte per descrivere il lavoro quotidiano del responsabile della sicurezza: «La parola 'combattere' è spesso associata al ruolo del CISO in varie aziende. Sovente è così». Questa dimensione di conflitto costante nasce da un dato numerico preciso: la crescita degli attacchi nel settore del trasporto aereo, che nel biennio 2024-2025 ha registrato un incremento significativo sia in Italia che nel resto del mondo. La gestione incidenti cyber diventa quindi la priorità assoluta per garantire la continuità di servizio in scali di importanza strategica.
Indice degli argomenti
Le minacce dominanti: l'impatto dei DDoS e dei Ransomware
La complessità dell'ecosistema e le interdipendenze tecnologiche
Tre pilastri per una gestione incidenti cyber efficace
Collaborazione e condivisione delle informazioni
Il ruolo centrale del Security Operations Center (SOC)
La cultura dell'esercitazione costante
La gestione della reputazione e il fattore esterno (continua)
https://www.zerounoweb.it/cyber-security/gestione-incidenti-cyber-nel-settore-aeroportuale-la-strategia-di-sea-milano/
SearchSecurity Zero *- Mattia Lanzarone, 6 mar 2026*

Polo Strategico Nazionale: perché è il cuore della sovranità cloud italiana

Il Polo Strategico Nazionale consolida le infrastrutture IT della PA in un'unica architettura cloud, con forte presidio di sicurezza e governance. In tre anni ha superato le attese di adesione, raggiunto milestone PNRR e strutturato un'offerta multicloud. Il focus resta la sovranità digitale, anche nel contesto europeo

L'iniziativa del **Polo Strategico Nazionale (Psn)** è stata avviata in via preliminare nel corso del **2020**, anche grazie agli esiti di un censimento condotto da parte dell'**AgID** relativamente allo stato dei **Data Center** che ospitano i dati delle **Pubbliche Amministrazioni** (ca. **1000 PA coinvolte**).

Da qui emerse una generale **inadeguatezza dell'infrastruttura**, venne promossa dal Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri (**"DTD"**) e dall'Agenzia per la Cybersicurezza Nazionale (**"ACN"**), come pilastro della **Strategia Cloud Italia**, nel più ampio piano di trasformazione digitale della PA.

Strategia Cloud Italia: le nuove opportunità del PNRR per migrare a Polo Strategico Nazionale

La società Polo Strategico Nazionale venne così costituita il **4 agosto 2022**, dopo poco più di due anni dalle prime ipotesi di lavoro, anche per accelerare la realizzazione della **infrastruttura** dove avviare le migrazioni principalmente delle PA Centrali (**"PAC"**), **ASL** e Aziende Ospedaliere (**"AO"**) italiane – che peraltro furono identificate dal **PNRR** come beneficiarie di finanziamenti europei (per circa **un miliardo di euro**, cfr. **PNRR M1C1 1.1**).

Indice degli argomenti

- Il cloud sovrano italiano e la nascita del Polo Strategico Nazionale
- Il modello di business del cloud sovrano italiano, Polo Strategico Nazionale
- Sovranità digitale nel Psn
  - Vincoli contrattuali nel contesto europeo
- Il cloud sovrano italiano PSN nel contesto europeo
  - Francia
  - Germania
- Polo Strategico Nazionale: i principali risultati raggiunti a fine 2025
- I benefici per le PA aderenti al cloud sovrano italiano
- Prospettive del Polo Strategico Nazionale e sfide future

Il cloud sovrano italiano e la nascita del Polo Strategico Nazionale

La Società, istituita mediante un **partenariato pubblico-privato** promosso da **CDP Equity, TIM, Leonardo e Sogei** (quindi a controllo indirettamente pubblico) e grazie ad una **Concessione** stipulata in data **24 agosto 2022** per il tramite di una **Convenzione** con il DTD, nasce con l'obiettivo di **consolidare le infrastrutture IT** della Pubblica Amministrazione (prevalentemente **PAC e ASL/AO**) in un'unica infrastruttura, mediante l'adozione del **paradigma cloud**. (continua…)

https://www.agendadigitale.eu/industry-4-0/polo-strategico-nazionale-perche-e-il-cuore-della-sovranita-cloud-italiana/?utm_campaign=agenda_nl_20260314&utm_source=agenda_nl_20260314&utm_medium=email&sfdcid=0030O00002LXHlXQAX

Agenda Digitale - *Lucia Fioravanti - Mar 9, 2026*

Italia sotto attacco cyber: più incidenti e difese ancora in ritardo

Nel 2025 la sicurezza informatica in Italia peggiora per intensità e qualità delle minacce, mentre crescono anche i dati compromessi e il peso dell'AI nelle frodi. Le imprese migliorano la governance,

ma la risposta operativa resta sotto pressione. Ecco il punto con i dati Clusit, Crif e Confindustria-Generali

Nel 2025 il panorama della sicurezza informatica in Italia ha registrato una trasformazione profonda e multidimensionale, che non riguarda soltanto la crescita in frequenza degli attacchi, ma anche la loro qualità, la sofisticazione degli strumenti impiegati e la varietà dei soggetti presi di mira. A fotografare questo scenario convergono tre fonti di rilievo: **il Rapporto Clusit 2026, l'Osservatorio Cyber di CRIF 2026 e il terzo Rapporto Cyber Index PMI promosso da Confindustria e Generali.**

Letti insieme, i tre studi restituiscono un quadro coerente: **gli incidenti crescono, i dati rubati migliorano qualitativamente oltre che quantitativamente, e la capacità difensiva del sistema Paese**, pur migliorando, fatica a tenere il passo.

A livello globale, il **Rapporto Clusit 2026** registra tra il 2024 e il 2025 un incremento del 48,7% nella frequenza degli incidenti, il più elevato mai rilevato dall'associazione. La **gravità media degli eventi** è a sua volta cresciuta, con un aumento dei danni inflitti alle singole vittime stimato intorno al 9% rispetto all'anno precedente. In questo scenario globale in forte accelerazione, **l'Italia presenta dinamiche proprie**, per certi versi più articolate e non riconducibili a una semplice lettura quantitativa.

Indice degli argomenti

- Cybersecurity in Italia: attaccanti e bersagli
  - Comparti pubblici, industria e logistica sotto pressione
- Il balzo dell'hacktivism e i settori più esposti
  - Credenziali compromesse e identità digitali complete
- Cybersecurity in Italia tra dati esposti e dark web
- L'AI come moltiplicatore delle frodi
- Sicurezza informatica in Italia e maturità delle PMI
  - Governance in crescita, attuazione ancora debole

Cybersecurity in Italia: attaccanti e bersagli

Sul fronte degli attaccanti attivi nel Paese, secondo Clusit il cybercrime rappresenta il 60,9% degli incidenti registrati nel 2025, in calo rispetto al 78% del 2024, sebbene in valore assoluto gli eventi siano aumentati: si passa da 277 a 309 incidenti. Il dato più significativo riguarda però **l'hacktivism**, che in Italia registra una crescita del 145% rispetto all'anno precedente, passando da 80 a 196 incidenti. (continua…)

https://www.agendadigitale.eu/sicurezza/italia-sotto-attacco-cyber-piu-incidenti-e-difese-ancora-in-ritardo/?utm_campaign=ad-daily_nl_20260317&utm_source=ad-daily_nl_20260317&utm_medium=email&sfdcid=0030O00002LXHlXQAX

***Agenda Digitale** - Tommaso Diddi, Luisa Franchina - 17 mar 2026*

New font-rendering trick hides malicious commands from AI tools

A new font-rendering attack causes AI assistants to miss malicious commands shown on webpages by hiding them in seemingly harmless HTML.

The technique relies on social engineering to persuade users to run a malicious command displayed on a webpage, while keeping it encoded in the underlying HTML so AI assistants cannot analyze it.

Researchers at browser-based security company LayerX devised a proof-of-concept (PoC) that uses custom fonts that remap characters via glyph substitution, and CSS that conceals the benign text via small font size or specific color selection, while displaying the payload clearly on the webpage.

During tests, the AI tools analyzed the page's HTML, seeing only the harmless text from the attacker, but failed to check the malicious instruction rendered to the user in the browser.

To hide the dangerous command, the researchers encoded it to appear as meaningless, unreadable content to an AI assistant. However, the browser decodes the blob and shows it on the page.
LayerX researchers say that as of December 2025, the technique was successful against multiple popular AI assistants, including ChatGPT, Claude, Copilot, Gemini, Leo, Grok, Perplexity, Sigma, Dia, Fellou, and Genspark.
"An AI assistant analyzes a webpage as structured text, while a browser renders that webpage into a visual representation for the user," the researchers explain.
"Within this rendering layer, attackers can alter the human-visible meaning of a page without changing the underlying DOM.
"This disconnect between what the assistant sees and what the user sees results in inaccurate responses, dangerous recommendations, and eroded trust," LayerX says in a report today.
The attack begins with the user visiting a page that appears safe and promises a reward of some kind that could be obtained by executing a command for a reverse shell on the machine. If the victim asks the AI assistant to determine if the instructions are safe, they will receive a reassuring response. (continua…)
https://www.bleepingcomputer.com/news/security/new-font-rendering-trick-hides-malicious-commands-from-ai-tools/
Bleeping Computer - *Bill Toulas - March 17, 2026*

Boom dei data center in Italia: Milano punta a diventare il nuovo hub europeo - *Il mercato dei data center in Italia sta vivendo una fase di espansione senza precedenti. Secondo i dati dell'Osservatorio Data Center del Politecnico di Milano, tra infrastrutture operative e nuovi progetti in pipeline il settore è destinato a crescere rapidamente nei prossimi anni, con Milano candidata a diventare uno dei principali hub europei dell'economia digitale.*
Il mercato dei data center in Italia sta vivendo una fase di forte espansione, trainata dalla crescita dei servizi cloud, dell'intelligenza artificiale e della domanda di capacità computazionale. Secondo i dati dell'Osservatorio Data Center del Politecnico di Milano, nel 2025 il Paese conta 26 infrastrutture attive e una potenza IT installata di 609 MW, con decine di nuovi progetti previsti nei prossimi anni. Milano e la sua area metropolitana stanno emergendo come principale hub nazionale ed europeo per nuovi investimenti, grazie alla presenza di reti di connettività, domanda digitale e infrastrutture energetiche. La crescita del settore pone però anche interrogativi su energia, pianificazione territoriale e sostenibilità degli investimenti.
Sommario tematico

- crescita dei data center in Italia
- evoluzione della potenza IT installata
- sviluppo dei campus data center
- ruolo di Milano nel mercato europeo
- investimenti previsti nel triennio 2026-2028

(continua)
https://www.ingenio-web.it/articoli/boom-dei-data-center-in-italia-milano-punta-a-diventare-il-nuovo-hub-europeo/
Ingenio *- Pietro Mezzi* - 18.03.2026

Gli enti normativi che si occupano di intelligenza artificiale - Alcuni lettori ci hanno chiesto di offrire una panoramica sulle norme afferenti all'intelligenza artificiale. Il quadro che è scaturito è ben più complesso di quello che inizialmente i lettori probabilmente si aspettavano.
Il tema della intelligenza artificiale è talmente importante, che numerosi enti normativi italiani, europei ed internazionali hanno dedicato la loro attenzione all'elaborazione di norme afferenti a questo tema. Ecco una panoramica degli enti coinvolti e dei comitati tecnici che hanno elaborato o stanno elaborando norme specifiche. Invitiamo i lettori a consultare in proprio il significato di ogni acronimo, che ora non offriamo per non appesantire troppo l'esposizione. Cogliamo l'occasione per ringraziare un relatore ad un recente convegno di ETSI, che ci ha aiutato a dipanare la matassa, per la verità assai aggrovigliata.
Cominciamo con una panoramica degli enti normativi coinvolti:
enti normativi di dimensione internazionale, come ISO, IEC ed ITU
enti normativi di dimensione europea, come CEN, CENELEC, ETSI
agenzie europee, come ENISA, JRC, CNCT, GROW
enti normativi di dimensione nazionale, come NIST, UNI, CEI, DIN, AFNOR, ecc.
associazioni normative aziendali, come OASIS, Open Forum, OACI, W3C, IEEE, e via dicendo.
L'ente normativo internazionale ISO, in particolare, ha allestito una sottocommissione specifica, che sviluppa normative afferenti alla sicurezza informatica, alla protezione dei dati ed alle nuove tecnologie, tra i quali indubbiamente rientra l'intelligenza artificiale. (continua…)
https://www.puntosicuro.it/nuove-tecnologie-ia-C-148/gli-enti-normativi-che-si-occupano-di-intelligenza-artificiale-AR-26242/
Punto Sicuro - *Adalberto Biasiotti - 18/03/2026*

FDA Issues Recall Notice for GE HealthCare Centricity Universal Viewer
A class 2 recall has been issued by the U.S. Food and Drug Administration (FDA) for certain GE HealthCare Centricity medical imaging products due to a vulnerability that could potentially be exploited by an unauthorized individual to manipulate data or impact system availability. Centricity Universal Viewer is a device that displays medical images such as mammograms and data from various imaging sources. The vulnerability affects the following Centricity Universal Viewer software versions:

- Versions 5.0 SP6 through UV 5.0 SP7.1
- Versions 6.0 through 6.0 Sp10.4.1
- Versions 7.0 through 7.0 Sp2.0.1

The recall was issued as the vulnerability may cause temporary or medically reversible adverse health consequences, but where the probability of serious adverse health consequences is remote. The vulnerability is due to user login credentials being exposed on the local client workstation. As such, an unauthorized individual could obtain the credentials and potentially impact system availability and/or manipulate data; however, the potential for exploitation is limited, as direct physical access to the local workstation is required.
"Patient safety is our top priority. There have been no reports of unauthorized access to patient data as a result of this potential issue. Direct physical access to the workstation is necessary to exploit this potential vulnerability," a GE HealthCare spokesperson told *The HIPAA Journal.* The vulnerability was discovered by GE Healthcare during routine testing, and the company is working on a permanent fix. GE HealthCare has issued instructions for customers to follow to allow them to continue using their devices until the fix is issued. (continua..)
https://www.hipaajournal.com/fda-recall-ge-healthcare-centricity-medical-imaging-products/?is=0b8f2776946dfb918b4bb1b43d6713cbf6a927ebd5e2184a38ea2f92df6f9da9
HipaaJournal - *Steve Alder - Mar 20, 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

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.

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*

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 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.