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. 6/ 2026** **giugno 2026**

L'11 giugno scorso la Presidenza del Consiglio ha pubblicato la Strategia Nazionale per la Resilienza dei Soggetti Critici, dando corpo operativo al decreto legislativo 134/2024 che recepisce la Direttiva CER. È un passaggio atteso, da accogliere con soddisfazione. Ma sarebbe un errore leggerlo come un punto di arrivo. Il documento infatti apre più che chiudere la questione più urgente del momento: come si governa la sovrapposizione tra CER e NIS2, due regimi normativi che insistono sugli stessi operatori con logiche distinte?

La domanda non è retorica. Gestori di reti energetiche, infrastrutture idriche, nodi di trasporto, operatori sanitari: un numero rilevante di soggetti CER è contestualmente destinatario degli obblighi NIS2. La CER guarda alla resilienza fisica, NIS2 alla sicurezza informatica. Il problema è che nella realtà operativa la distinzione è ormai artificiale: un attacco a un sistema SCADA è anche un evento fisico, un'interruzione fisica ha conseguenze immediate sui sistemi digitali interdipendenti. Le due dimensioni non si sommano, si moltiplicano. La Strategia riconosce il nodo e istituisce un tavolo di raccordo permanente tra il Punto di Contatto Unico (PCU) e l'ACN, con l'obiettivo di garantire scambio informativo coerente e un'interpretazione armonizzata degli obblighi. L'ambizione è evitare che lo stesso operatore risponda due volte alla stessa esigenza con regole diverse.

In questo quadro, la scadenza del 17 luglio per il DPCM che individuerà i soggetti critici italiani acquista un peso particolare. Sapere se si è un "soggetto critico" non è un dettaglio burocratico: è la condizione necessaria per pianificare investimenti, attivare risk assessment, strutturare la governance interna.

La vera sfida, tuttavia, è operativa. Qualunque coordinamento PCU-ACN si riuscirà a costruire, il peso dell'integrazione CER-NIS2 ricade sulle strutture interne degli operatori: sui security manager, sui risk officer, sui responsabili della continuità. Sono loro che devono tradurre due linguaggi normativi in procedure coerenti e convincere i vertici aziendali che un piano di resilienza fisica e un piano di sicurezza informatica, da soli, non bastano. Ed è per questo che il coordinamento CER-NIS2 non è un tema istituzionale da monitorare a distanza: è un cantiere aperto che chiama direttamente in causa la nostra comunità professionale.

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).

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

ATTIVITA' DELL'ASSOCIAZIONE

RINNOVO ASSOCIATIVO ANNO 2026

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

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

PUBBLICAZIONE DI ARTICOLI DA PARTE DI SOCI E PARTECIPAZIONE AD EVENTI

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

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

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

SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

Vi ricordiamo che il sito web www.infrastrutturecritiche.it rappresenta la **fonte ufficiale dell'Associazione Italiana esperti in Infrastrutture Critiche**: è accessibile a tutti, e contiene tutte le

informazioni necessarie per un corretto svolgimento della vita associativa. Vi invitiamo a consultarlo e anche a farci pervenire le vostre osservazioni: i vostri suggerimenti sono sempre preziosi e ci aiutano a migliorare il prodotto.

COLLABORAZIONE ALLE ATTIVITA' AIIC

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

NEWS E AVVENIMENTI

La sfida della tutela strutturale dei beni storici nell'era dell'intelligenza artificiale - La conservazione strutturale dei beni storici richiede oggi strumenti avanzati capaci di interpretare fenomeni complessi e dinamici. L'integrazione tra intelligenza artificiale e modellazione predittiva consente di anticipare criticità e scenari di rischio, come mostrato dal caso studio della Torre Garisenda. L'articolo analizza l'applicazione dell'intelligenza artificiale alla tutela strutturale dei beni storici, con un focus sulla Torre Garisenda di Bologna. Il tema centrale è il passaggio da controlli periodici e interventi correttivi a modelli predittivi basati su serie temporali, dati climatici, geotecnici e deformativi. L'approccio permette di riconoscere pattern, anomalie e trend evolutivi, supportando manutenzione preventiva, gestione del rischio e programmazione degli interventi.
Tutela dei beni storici nell'era dell'AI: come passare dalla manutenzione reattiva a quella predittiva
La conservazione del patrimonio storico è oggi una delle sfide più complesse dell'ingegneria civile.
Le strutture monumentali, spesso realizzate con materiali non omogenei, tecniche costruttive arcaiche e soggette a continue interazioni con l'ambiente, richiedono approcci che vadano oltre la semplice manutenzione reattiva.
Per decenni la gestione del rischio si è basata su monitoraggi periodici, analisi visive e interventi correttivi successivi al manifestarsi delle criticità.
Oggi, tuttavia, l'integrazione fra intelligenza artificiale e modellazione predittiva consente di passare da una logica reattiva ad una proattiva. Le strutture non vengono più "osservate" ma vengono ascoltate, interpretate, contestualizzate e simulate, con l'obiettivo di prevederne l'evoluzione nel tempo.
(continua…)
https://www.ingenio-web.it/articoli/la-sfida-della-tutela-strutturale-dei-beni-storici-nell-era-dell-intelligenza-artificiale/
Ingenio - *Sarah Olimpia Sardone – 08/01/2026*

Droni e Security: come le nuove tecnologie costruiscono perimetri di sicurezza dinamici anche in tempo di pace - L'impiego dei droni nel campo della security rappresenta oggi una delle evoluzioni più rilevanti nei sistemi di protezione di infrastrutture, cantieri, siti industriali e territori estesi. Se per lungo tempo il drone è stato percepito soprattutto come uno strumento legato a contesti militari o emergenziali, la sua applicazione in tempo di pace dimostra invece come questa tecnologia possa diventare parte integrante di un modello di sicurezza preventiva, intelligente e multilivello. In questa prospettiva, il drone non sostituisce l'uomo, ma ne estende capacità di osservazione, rapidità di reazione e consapevolezza situazionale.

Cambia il concetto di perimetro

La security contemporanea non può più essere interpretata come una mera barriera fisica. Recinzioni, cancelli, pattugliamenti e telecamere restano fondamentali, ma non sono più sufficienti quando si tratta di proteggere opere lineari, aree remote, siti temporanei o contesti caratterizzati da elevata estensione territoriale e difficoltà logistiche. In questi scenari il concetto di perimetro cambia natura: non è più soltanto una linea materiale da presidiare, ma diventa un sistema informativo e operativo capace di rilevare, analizzare e reagire in tempo reale.

È proprio qui che si colloca il contributo dei droni. Grazie alla possibilità di effettuare ronde programmate, missioni su allarme, sorveglianza diurna e notturna, riprese ottiche e termiche, essi consentono di trasformare il perimetro da elemento statico a dispositivo dinamico. Il perimetro non è più soltanto ciò che delimita uno spazio, ma ciò che permette di avere "occhi" mobili e intelligenti sul territorio, in grado di anticipare eventi avversi, individuare accessi non autorizzati, seguire movimenti sospetti e supportare gli operatori a terra con informazioni immediate e georeferenziate.

(continua…)

https://www.snewsonline.com/droni-security-come-nuove-tecnologie-costruiscono-perimetri-sicurezza-dinamici-anche-tempo-pace/

SNews - Umberto *Saccone - 10 Aprile 2026*

La guerra in Iran e il nuovo ordine mondiale del petrolio - D'ora in poi il prezzo del petrolio continuerà a risentire dell'instabilità geopolitica perché l'Iran ha dimostrato di poter decidere in qualsiasi momento di interrompere le forniture.

Indice dei contenuti

L'effetto della guerra USA all'Iran: il prezzo del petrolio continuerà a risentire dell'instabilità geopolitica
Premio permanente sui prezzi legato a un ambiente operativo permanentemente più rischioso
La questione del pedaggio
Guerra USA all'Iran, Golfo permanentemente più pericoloso

L'effetto della guerra USA all'Iran: il prezzo del petrolio continuerà a risentire dell'instabilità geopolitica

La guerra USA all'Iran potrebbe aver modificato per sempre il mercato petrolifero perché quello che emergerà da un eventuale accordo tra Washington e Teheran potrebbe apparire molto diverso rispetto a prima.

Il possibile accordo tra Stati Uniti e Iran riaprirebbe lo Stretto di Hormuz, lasciando in sospeso la questione del nucleare ma riportano sul mercato grandi quantità di petrolio. Intanto, le scorte petrolifere globali, che hanno in parte permesso di attenuare gli effetti della crisi energetica, si stanno riducendo a un ritmo record.

Tuttavia, anche dopo un accordo (ammesso che arrivi) con l'Iran, ci vorrà del tempo per ripristinare le condizioni precedenti alla guerra. E d'ora in poi, prima di tutto, il prezzo del petrolio potrebbe continuare a risentire dell'instabilità geopolitica perché l'Iran ha dimostrato di poter decidere in qualsiasi momento di interrompere le forniture.

Fino a pochi mesi fa la chiusura di Hormuz era solo una possibilità teorica presa in considerazione dagli analisti e nessun Presidente statunitense si era mai avventurato in una guerra contro l'Iran per non incorrere in questa possibilità. Trump, invece, l'ha resa realistica. E anche dopo un accordo, niente assicura che Teheran possa decidere di richiudere nuovamente il canale.
(continua)
https://www.rinnovabili.it/mercato/guerra-usa-iran-prezzo-petrolio/
Rinnovabili - *Erminia Voccia - 28 Maggio 2026*

Dutch govt disrupts malware botnet with 17 million infected devices
Dutch authorities have taken offline a massive botnet of 17 million devices and seized more than 200 servers at a local provider that supported the operation.
The action was carried out following an investigation from the Police in collaboration with the country's cybersecurity agency, the National Cyber Security Centre (NCSC).
According to the authorities, the seized servers controlled "computers, tablets, and smartphones to carry out cyberattacks."
Botnets are networks of compromised devices used for illegal activities such as distributed denial-of-service (DDoS) attacks, malicious traffic proxying, or cryptocurrency mining.
"The investigation revealed that the botnet consisted of at least 17 million infected devices and that the 200 servers used to host the infrastructure were located in the Netherlands," the NCSC said.
" The police subsequently seized several botnet servers from a hosting provider for investigation purposes. The hosting provider took the botnet offline because it was being used for criminal activities."
Although the authorities did not name the botnet, local media reported that it was linked to a service called Asocks, which advertises itself as a "universal proxy service" with 7 million IP addresses, 150 locations, and 100,000 clients. (continua…)
https://www.bleepingcomputer.com/news/security/dutch-govt-disrupts-malware-botnet-with-17-million-infected-devices/
Bleepingcomputer *Bill Toulas May 29, 2026*

Cosa rischia il sistema elettrico italiano questa estate? - Durante l'estate 2026 l'Italia dovrebbe trovarsi in una situazione di adeguatezza complessivamente favorevole nonostante risultino irrisolte alcune vulnerabilità legate alle ondate di calore e la gestione della rete.
Indice dei contenuti
Il Summer Outlook 2026 di ENTSO-E
L'adeguatezza del sistema elettrico europeo
Quale Paese è più a rischio nell'estate 2026?
Il sistema elettrico italiano e i rischi estivi
Vulnerabilità specifiche
Il Summer Outlook 2026 di ENTSO-E
Come sarà l'estate 2026 per il sistema elettrico italiano? Con un Maggio decisamente sopra la media sul fronte delle temperature, la domanda sorge spontanea. E mentre crescono le preoccupazioni sull'approvvigionamento dei carburanti, appare opportuno capire quanto il sistema sia pronto alle incertezze della prossima stagione. Ondate di calore in primis.
La risposta arriva dal nuovo Summer Outlook 2026 di ENTSO-E, la rete dei 40 gestori europei della trasmissione elettrica. Il rapporto fornisce un chiaro quadro dell'adeguatezza europea, entrando nel dettaglio di ogni paese e provando a mettere a fuoco i punti sensibili da attenzionare.

L'adeguatezza del sistema elettrico europeo

Nel complesso il documento restituisce uno scenario positivo: il sistema elettrico europeo risulta resiliente e adeguato, ossia capace di garantire costantemente la fornitura energetica necessaria a coprire la domanda dei consumatori, mantenendo margini di sicurezza anche in condizioni critiche. Non solo. I potenziali problemi individuati fanno riferimento ad un numero limitato di mercati.

Il documento sottolinea anche come da un anno all'altro il mix elettrico abbia cambiato proporzioni. Rispetto all'estate 2025, la capacità rinnovabile è aumentata di oltre 90 GW, per lo più grazie agli impianti fotovoltaici (77 GW). Di pari passo quella dei sistemi di accumulo a batteria è quasi raddoppiata sebbene si muova ancora su una scala ridotta. La capacità legata ai combustibili fossili ha, invece, mostrato una leggera flessione (meno 12 GW).

Il rapporto conferma inoltre lo schema di manutenzioni delle centrali termoelettriche secondo il modello della "U" rovesciata: le attività di manutenzione programmata vengono concentrate a giugno e settembre/ottobre, riducendole ai minimi a luglio e agosto per evitare carenze durante le possibili ondate di calore.

(continua)

https://www.rinnovabili.it/energia/infrastrutture/sistema-elettrico-italiano-estate/

Rinnovabili *- Stefania Del Bianco, 1° giugno 2026*

Exposed Fuel Tank Gauges Under Attack in the US

Threat actors are taking advantage of Internet-exposed tank gauges by breaching gas stations, opening the door to disruption.

Cyberattackers are targeting Internet-exposed automatic tank gauge (ATG) systems in the United States, and the feds are urging site owners to take swift action.

ATGs are the electronic gauges that industrial sites use to monitor liquid storage tanks, whether they contain dangerous chemicals, fuel, or whatever else. Compared to some more elaborate machinery, they're rather straightforward things: probes that feed displays, which feed data to broader supervisory control and data acquisition (SCADA) systems so that plant operators can monitor their readings at a distance. Perhaps most folks give them little thought, especially in a cybersecurity context, but they're arguably as grave of a potential risk as any other equipment at any industrial facility anywhere.

This week, the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), Department of Energy (DoE), Environmental Protection Agency (EPA), Transportation Security Administration (TSA), Department of Transportation (DOT), and US Department of Agriculture (USDA) published a joint notice urging industrial organizations to harden their ATGs from cyberattack.

The agencies said they're "aware of malicious cyber activity" targeting these systems in the US, but didn't attribute it to any one particular threat group; the statement might be in reference to reports last month that threat actors loosely linked to Iran have been attacking ATGs at gas stations around the country. (continua…)

https://www.darkreading.com/cyberattacks-data-breaches/exposed-fuel-tank-gauges-attack-us

Darkreading *- Nate Nelson - June 5, 2026*

Data centers aerospaziali: è una proposta tecnologicamente sostenibile? - I Data Center nello spazio potrebbero ridurre il consumo di risorse terrestri. Un'analisi del GAO esamina opportunità, vantaggi e rischi di questa innovativa soluzione tecnologica.

È noto che oggi gli applicativi di intelligenza artificiale, ed altri applicativi similari, richiedono enormi risorse di calcolo e capacità di memorizzazione dei dati. Ad esempio, un grande centro di calcolo terrestre ha bisogno di essere alimentato con 100 MW di energia elettrica e utilizza oltre 200.000 galloni di acqua al giorno per il raffreddamento dei circuiti elettronici.
Ecco il motivo per cui numerosi ricercatori hanno cominciato ad esaminare la possibilità che questi centri di elaborazione vengano installati su satelliti.
La maggior parte delle proposte prevede che questi satelliti si trovino ad orbitare in orbite terrestri basse, soprattutto per garantire un'elevata rapidità di comunicazione con le stazioni terrestri. Inoltre, queste orbite possono garantire un elevato livello di radiazione solare e quindi la possibilità di alimentare i centri stessi con pannelli fotovoltaici.
Alcuni problemi da superare, già individuati, riguardano la capacità di raffreddare gli elementi di calcolo. Ad oggi, le soluzioni di raffreddamento idonee per grandi centri di calcolo, in ambito spaziale, non sono state ancora sperimentate e si prevedono difficoltà, perché il calore non è facilmente dissipabile nel vuoto dello spazio. (continua…).
https://www.puntosicuro.it/sicurezza-informatica-C-90/data-centers-aerospaziali-una-proposta-tecnologicamente-sostenibile-AR-26476/
Punto Sicuro *- Adalberto Biasiotti - 08/06/2026*

AI in sanità, perché non basta più scegliere il modello migliore
L'evoluzione dell'intelligenza artificiale in sanità, dai Large Language Model ai sistemi Agentic AI, impone nuovi criteri di valutazione, governance e procurement. Le Direzioni ICT dovranno misurare affidabilità, sicurezza, trasparenza e capacità operative lungo l'intero ciclo di vita delle soluzioni
L'**intelligenza artificiale** rappresenta oggi uno dei principali fattori di trasformazione dei **sistemi sanitari**. Se fino a pochi anni fa **le applicazioni di AI erano prevalentemente limitate all'analisi predittiva**, al supporto diagnostico o all'elaborazione di immagini cliniche, l'avvento dell'AI generativa ha modificato radicalmente il panorama tecnologico e organizzativo.
Per comprendere questa evoluzione è utile distinguere quattro livelli progressivi di maturità: **Large Language Model (LLM)**, **Retrieval Augmented Generation (RAG)**, **AI Agent** e **Agentic AI**.
Indice degli argomenti

- Dai Large Language Model all'Agentic AI
  - Cosa cambia con gli agenti AI
- La crisi dei benchmark tradizionali
- Valutare l'AI in sanità oltre la semplice accuratezza
- Dall'AI Testing all'AI Assurance
- Il procurement dell'AI in Sanità
  - I cambiamenti necessari
- Cosa dice il Codice dei Contratti Pubblici
- Lo scenario

Dai Large Language Model all'Agentic AI
Gli **LLM** costituiscono il primo livello. Si tratta di modelli linguistici in grado di comprendere e generare testo, sintetizzare documenti, supportare attività redazionali e interagire in linguaggio naturale. In sanità possono assistere il personale nella consultazione di linee guida, nella redazione di documentazione clinica e nella produzione di contenuti informativi.
Il paradigma **RAG** introduce un secondo livello di evoluzione. Integrando il modello linguistico con basi documentali e sistemi di ricerca semantica, l'intelligenza artificiale può accedere a contenuti aggiornati

e contestualizzati. In ambito sanitario ciò significa poter interrogare procedure aziendali, regolamenti, protocolli clinici, documentazione tecnica e basi di conoscenza specialistiche, migliorando accuratezza e affidabilità delle risposte.

Cosa cambia con gli agenti AI

Con gli **AI Agent** si compie un ulteriore salto di qualità. L'intelligenza artificiale non si limita più a fornire informazioni, ma acquisisce la capacità di pianificare attività, utilizzare strumenti software, accedere a sistemi informativi, interrogare basi dati ed eseguire operazioni all'interno di processi organizzativi.

L'ultima fase di questa evoluzione è rappresentata dall'**Agentic AI**, nella quale più agenti collaborano tra loro per perseguire obiettivi complessi. Questi sistemi possono coordinare attività articolate, mantenere memoria persistente, adattare il proprio comportamento ai risultati ottenuti e interagire con molteplici applicazioni aziendali.

La progressione da **LLM ad Agentic AI** rappresenta un cambiamento sostanziale anche per le **Direzioni ICT**. Non si tratta più di acquistare semplici applicazioni software, ma sistemi dotati di capacità cognitive crescenti, in grado di influenzare processi clinici, amministrativi e decisionali. Di conseguenza, anche i criteri di valutazione e **procurement** devono evolvere. (continua…)

https://www.agendadigitale.eu/sanita/ai-in-sanita-perche-non-basta-piu-scegliere-il-modello-migliore/

Agendadigitale *-Claudio Caccia - 23 giu 2026*

EUROPOL DISRUPTS STEALC AND AMADEY MALWARE INFRASTRUCTURE IN OPERATION ENDGAME

Operation Endgame disrupted malware services like StealC and Amadey that enable ransomware, fraud, and attacks on critical infrastructure.

Between June 15 and 19, 2026, Europol coordinated a two-week law enforcement operation involving agencies from Canada, Denmark, Germany, the Netherlands, the UK, and the US, alongside private firms like Microsoft, Bitdefender, IBM X-Force, Proofpoint, Infoblox, Shadowserver, Orange Cyberdefense, and a dozen other private partners.

The operation targeted the infrastructure behind three malware families, SocGholish, Amadey, and StealC, that together form the opening stages of the cybercrime attack chain.

"The main common goal was to disrupt the "assembly lines" cybercriminals use to launch ransomware, financial fraud, and attacks on critical infrastructure." reads the report published by EUROPOL. "Crypto assets of criminal origin currently valued at over EUR 41 million (USD 47 million) were identified, flagged, and thereby restricted from use. "

The numbers from the action are substantial. Law enforcement and private partners actioned 326 servers and 142 domains, recovered 27 million stolen login credentials, and identified, flagged, and restricted over €41 million in criminal cryptocurrency assets.

During the SocGholish portion of the operation, 14,971 infected websites were remediated, including restaurants, auto repair shops, and other everyday businesses whose WordPress installations had been quietly compromised and turned into malware distribution points. The Dutch Police removed vulnerabilities from infected sites and notified owners directly.

SocGholish works by injecting fake browser update prompts into legitimate websites. A visitor clicks what looks like a routine update, and the malware installs.

"This approach, which has caused countless victims, is primarily done by hacking websites built with WordPress and infecting them with malware." continues the report." The unauthorised access was then exploited for further crimes, such as installing ransomware for the purpose of digital extortion."

SocGholish is linked to Evil Corp, the Russian cybercriminal group previously responsible for Zeus and Dridex, and associated with multiple large-scale ransomware and money-laundering operations. (continua…)
https://securityaffairs.com/194173/cyber-crime/europol-disrupts-stealc-and-amadey-malware-infrastructure-in-operation-endgame.html
Securityaffairs - *Pierluigi Paganini - June 24, 2026*

Oltre i benchmark: la gara che non vediamo
Il report JPMorgan sulla competizione USA–Cina rivela una sfida che i grafici non catturano
C'è una figura retorica che domina il discorso pubblico sull'intelligenza artificiale: il benchmark. Un numero, una classifica, un grafico a dispersione che mostra dove si colloca questo modello rispetto a quello, su questa capacità rispetto all'altra. La figura è rassicurante perché è traducibile, comparabile, comunicabile in un tweet. Ma come ogni misura, un benchmark dice molto su ciò che sceglie di misurare e quasi nulla su ciò che decide di non misurare.
Il Centro per la Geopolitica di JPMorgan Chase ha pubblicato a maggio 2026 un documento che si propone esattamente questo obiettivo: andare "oltre i benchmark". Il titolo è già una presa di posizione epistemica. Beyond the Benchmarks: A Systemic View of U.S.–China AI Competition non è il consueto esercizio di intelligence competitiva che traccia curve di performance e proietta chi arriverà per primo a qualche soglia prestabilita. È un tentativo di costruire una grammatica diversa per leggere una competizione che è, nelle parole stesse del documento, "una delle dinamiche geopolitiche definitive del XXI secolo".
Quello che colpisce di questo testo non è la quantità di dati che mobilita, pur considerevole, ma il gesto intellettuale che lo sottende: la decisa affermazione che le variabili che fanno titolo, quelle che generano le regular headlines, non sono le più importanti. L'infrastruttura energetica, l'accesso ai mercati dei capitali, le tendenze di produttività nei dati delle contabilità nazionali: questi indicatori si muovono silenziosamente e possono rivelarsi più decisivi dei benchmark nel determinare dove andrà la competizione, prima che quella traiettoria diventi visibile nelle capacità stesse. È una lezione di epistemologia geopolitica: ciò che non fa rumore può cambiare tutto. (continua…)
https://www.linkedin.com/posts/paolo-benanti-94aa1915_oltre-i-benchmark-la-gara-che-non-vediamo-share-7475806420072972288-sfvB/?utm_source=share&utm_medium=member_ios&rcm=ACoAAAcNCUkB3Si-cw_LFtTzVfmL-JzyKYrPPFA
LINKEDIN - *Paolo Benanti - giugno 25, 2026*

Pax Silica: perché l'Europa entra nell'alleanza USA sui chip
L'Unione Europea aderisce a Pax Silica, l'iniziativa americana per la sicurezza delle filiere di chip e AI. Una scelta dettata dalle esigenze industriali ma accompagnata da un rafforzamento della strategia europea sulla sovranità tecnologica
Il 23 giugno 2026, **l'Unione Europea ha aderito formalmente a Pax Silica** attraverso la Commissione. Alcuni stati membri, Grecia, Finlandia, Svezia, avevano già aderito individualmente nelle settimane precedenti; Germania e Paesi Bassi hanno firmato a titolo nazionale lo stesso giorno. L'iniziativa era stata lanciata dal Dipartimento di Stato americano nel dicembre 2025 per mettere in sicurezza le catene di fornitura dell'intelligenza artificiale: semiconduttori, minerali critici, energia, manifattura avanzata, logistica.

Al summit di Washington, Jacob Helberg, Under Secretary for Economic Affairs e architetto dell'iniziativa, ha annunciato l'ingresso anche di Argentina, Cile, Costa Rica, Kazakistan e Panama, portando la coalizione a 24 paesi.
Il nome non è casuale. **Pax Silica evoca la Pax Romana e la Pax Americana**, un ordine garantito dalla supremazia di chi controlla la risorsa strategica fondamentale. Nel ventunesimo secolo, quella risorsa è il silicio, e tutto ciò che serve a trasformarlo in capacità di calcolo.
Indice degli argomenti

- Pax Silica e Unione Europea: che cosa cambia nell'alleanza dei chip
  - Una coalizione di capabilities, non un trattato
- La frattura europea su Pax Silica e il compromesso francese
- Pax Silica e sovranità tecnologica UE: la doppia polizza
- Dai chip ai modelli AI: i due perimetri di Pax Silica
- Il terreno regolatorio della sovranità europea

Pax Silica e Unione Europea: che cosa cambia nell'alleanza dei chip
La prima cosa da capire è cosa **Pax Silica non è**. Non è un trattato vincolante, la Dichiarazione è un atto politico, senza finanziamento congiunto dedicato e senza mandati operativi per i firmatari. La Commissione ha ottenuto garanzie esplicite su questo punto, proprio per superare le resistenze interne.
Una coalizione di capabilities, non un trattato
Ma non è neppure una semplice dichiarazione d'intenti. Il modello è quello che l'American Enterprise Institute ha definito **coalition of capabilities**: ogni paese porta un asset specifico, capitale qatariota, ingegneria israeliana, assemblaggio filippino, capacità di raffinazione latino-americana, ricchezza sovrana norvegese, e riceve in cambio accesso allo stack tecnologico. Il progetto bandiera, **Fort Foundry One**, è un impianto di semiconduttori previsto in Israele con un contratto di locazione a 99 anni, finanziato da una dozzina di paesi.
Un modello transazionale, non di vassallaggio, questo cambia la natura della partita per l'Europa, che al tavolo porta carte tutt'altro che marginali: ASML e la litografia EUV olandese, la chimica di specialità tedesca, l'ecosistema di ricerca sui **materiali avanzati**. La domanda è se quelle carte vengono giocate come **leverage negoziale** o come semplice biglietto d'ingresso.
La frattura europea su Pax Silica e il compromesso francese
L'adesione non è stata indolore. La spaccatura tra gli stati membri ha seguito linee prevedibili. Germania, Italia e Paesi Bassi hanno spinto per l'adesione, insistendo sulla necessità di un fronte unito verso Washington. La Francia si è opposta con un linguaggio insolitamente duro, parlando di tentativo di colonizzare l'Europa e sabotare la sovranità tecnologica del continente. Parigi ha chiesto chiarimenti su tre punti: la governance dell'iniziativa, il rapporto con il G7 e il rischio che Pax Silica compromettesse l'autonomia dell'UE sui controlli alle esportazioni e sullo screening degli investimenti esteri. L'Italia, che pure era nel blocco favorevole all'adesione, ha scelto di entrare solo attraverso la cornice comunitaria, senza una firma individuale.
Il compromesso si regge su un punto, **la Dichiarazione non è vincolante**. La Commissione ha confermato che nulla nell'iniziativa pregiudica i processi decisionali interni dell'Unione né la sua autonomia regolamentare. (continua…)
https://www.agendadigitale.eu/cultura-digitale/pax-silica-perche-leuropa-entra-nellalleanza-usa-sui-chip/
Agendadigitale - *Maurizio Carmignani - 26 giu 2026*

Meeting Trump's 2030 Quantum Deadline Will be Expensive, Complex

Getting accurate visibility into IT and OT systems will be compounded by multivendor environments, misaligned update life cycles, and interoperability gaps.

Organizations will face major challenges — and even greater costs — on the road to becoming quantum-ready over the next five years.

US President Donald Trump signed two executive orders related to quantum technology on June 22.

One, "Ushering in the Next Frontier of Quantum Innovation," aims to bolster US leadership in quantum information science and technology through updating the national quantum strategy and building out a domestic ecosystem that will lead to the development of a quantum computer beyond current capabilities. It also includes workforce investment and partnering with various stakeholders, such as international allies, manufacturers, and private sector investors.

The second, "Securing the Nation Against Advanced Cryptographic Attacks," aims to prepare US infrastructure for the attackers that would use quantum technology to target organizations. The aim here is to accelerate the government's transition to post-quantum cryptography (PQC) and fortify sensitive government data.

The executive order requires federal agencies to appoint PQC migration leads within 30 days, establish PQC for key establishment and encryption by the end of 2030, and establish PQC for digital signatures by the end 2031 for high-value assets and high-impact systems.

The order also directs the National Institute of Standards and Technology (NIST) to begin a PQC pilot program to create standards for the transition and directs relevant agencies to create guidance for a cryptographic bill of materials. Relevant agencies must also assist critical infrastructure in becoming quantum ready.

While many of these requirements primarily exist for the federal government, federal contractors will also be required to adhere to NIST's PQC standards by Dec. 31, 2030.

These orders dramatically accelerate the timeline many organizations had in mind for quantum readiness. Much of the security industry's previous framing was that cryptographically relevant quantum computers were unlikely before 2035, so PQC migration was treated as something to prepare for rather than a compliance exercise.

How government and industry think about quantum computing has changed in recent years. Security experts say threat actors are stealing credentials they can't decrypt today to prepare themselves for a world where quantum computers can (harvest now, decrypt later). Google in March set a deadline of 2029 to integrate PQC cryptography into its systems, products, and services, and Apple has been ringing the quantum bell for years now.

Going Quantum: Big Challenges, Bigger Costs (continua…)

https://www.darkreading.com/cybersecurity-operations/meeting-2030-quantum-deadline-expensive-complex

Darkreading *- Alexander Culafi - June 26, 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/

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

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

RIFERIMENTI DELL'ASSOCIAZIONE

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

Per maggiori informazioni sull'Associazione inviare una mail a

segreteria@infrastrutturecritiche.it

o visitate il sito

www.infrastrutturecritiche.it

ATTENZIONE

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

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

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

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