



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. 8/ 2026

settembre 2026

PROTEZIONE DELLE INFRASTRUTTURE CRITICHE SUBACQUEE

Le infrastrutture subacquee sono sempre più strategiche per la connettività globale, la sicurezza delle comunicazioni e lo sviluppo dell'economia digitale. I cavi sottomarini trasportano oltre il 95% del traffico dati internazionale.

Le reti subacquee sono infrastrutture complesse, attraversano giurisdizioni diverse, coinvolgono operatori privati e istituzioni pubbliche, e possono avere impieghi civili e militari. La loro protezione richiede coordinamento tra attori civili e militari, tra istituzioni nazionali e alleanze internazionali.

Incidenti recenti, come il sabotaggio del gasdotto Nord Stream e i ripetuti danni ai cavi di comunicazione sottomarini in Europa, hanno evidenziato la vulnerabilità delle infrastrutture sottomarine a interruzioni sia accidentali che intenzionali.

Per far fronte a tali preoccupazioni, il 21 febbraio 2025 la Commissione europea e l'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno adottato il piano d'azione dell'UE sulla sicurezza dei cavi. Tale iniziativa delinea una serie di azioni coordinate volte ad affrontare le minacce e a rafforzare la resilienza delle infrastrutture sottomarine per le telecomunicazioni e l'energia, coprendo tutte le fasi del ciclo di resilienza: prevenzione, rilevamento, risposta e ripristino, nonché deterrenza. Al fine di sostenere l'attuazione del piano d'azione sui cavi e della precedente raccomandazione (UE) 2024/779 della Commissione relativa a infrastrutture di cavi sottomarini sicure e resilienti, la Commissione ha istituito il gruppo di esperti sulle infrastrutture di cavi sottomarini. Tale gruppo è presieduto dalla Commissione e composto da rappresentanti delle autorità degli Stati membri e dell'Agenzia dell'Unione europea per la cibersicurezza, con il compito di fornire orientamenti sul come muoversi.

A livello italiano, la Direttiva UE CER del 2022 è stata recepita con il D. Lgs 134 del settembre 2024, resa attuativa con la "**Strategia Nazionale per la Resilienza dei Soggetti Critici**":

https://www.governo.it/sites/governo.it/files/StrategiaNazionaleEesilienzaSoggettiCritici_EN.pdf

emanata dalla Presidenza del Consiglio dei Ministri in data **11 Giugno 2026**.

La **Strategia Nazionale per la Resilienza dei Soggetti Critici** tutela gli Enti pubblici e privati che erogano servizi essenziali. Essa mira a prevenire e mitigare gli impatti di eventi fisici e digitali attraverso la mappatura delle dipendenze, la gestione delle crisi e la protezione della *supply chain*.

Una delle attività previste dalla Strategia Nazionale è **Obiettivo 2.6.: Mappatura, classificazione e protezione delle infrastrutture critiche subacquee**, per garantire la sicurezza, l'integrità e la continuità operativa delle infrastrutture critiche subacquee contro possibili rischi. Come si legge dall'Obiettivo 2.6 della Strategia, il primo passo fondamentale consiste nella mappatura e classificazione delle infrastrutture esistenti, nonché sviluppare un **sistema di sorveglianza e monitoraggio continuo** che permetta di disporre di una *Situational Awareness* completa presso il Centro di Sorveglianza per le infrastrutture critiche sottomarine della Marina Militare, per una condivisione con gli omologhi centri della NATO e dell'UE; una correlata **procedura operativa nazionale per la gestione di incidenti** fisici che sia integrata e coordinata con la gestione degli incidenti cyber, anche in ambito NATO e UE.



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 la mappatura e classificazione delle infrastrutture esistenti il primo passo fondamentale consiste nella **mappatura e classificazione delle infrastrutture esistenti** anche attingendo a censimenti già esistenti, quali il **Sistema Informativo Nazionale Federato delle Infrastrutture (SINFI) del MIMIT**. Parallelamente, occorre sfruttare il **Polo Nazionale della Dimensione Subacquea**, quale incubatore delle conoscenze e delle tecnologie necessarie per esplorare la dimensione sottomarina e difendere le sue infrastrutture critiche; per promuovere, facilitare e coordinare la cooperazione delle diverse eccellenze nazionali del settore favorendo la sinergia del Sistema Paese, supportando tutti gli attori istituzionali nella implementazione di iniziative congiunte con la NATO, l'UE e altri Stati. Per il ruolo normativo è importante stabilire delle relazioni con l'**Agenzia per la sicurezza delle attività subacquee (ASAS)** è l'ente pubblico nazionale, istituito con la Legge 26 gennaio 2026, n.9, che opera alle dipendenze funzionali della Presidenza del Consiglio dei Ministri per coordinare e regolamentare l'intero settore.

A questo punto il lettore si chiederà: **perché applicare l'intelligenza artificiale?** La Direttiva UE sulla resilienza dei soggetti critici (CER), impone a tali soggetti di rafforzare la propria capacità di prevenire, assorbire e gestire incidenti dirompenti, nonché di riprendersi da essi e adattarvisi. L'intelligenza artificiale (IA) sta emergendo come un fattore chiave per la resilienza di tali infrastrutture, grazie a funzionalità quali manutenzione predittiva, rilevamento di anomalie, identificazione delle minacce, monitoraggio autonomo, supporto alle decisioni e sicurezza cyber-fisica.

In questo contesto, la **Physical AI** — ovvero l'integrazione dell'intelligenza artificiale con robotica, sistemi autonomi, sensori, gemelli digitali e sistemi di controllo cyber-fisici — offre capacità trasformative per potenziare la resilienza delle infrastrutture critiche sottomarine. A differenza dell'IA Generativa (GenAI), attualmente più utilizzata e diffusa, che fornisce principalmente analisi e approfondimenti basati su documenti (scritti, audio, video) e non su segnali provenienti da sensori nel mondo reale, la Physical AI consente ai gestori di infrastrutture di percepire, ragionare, decidere e agire all'interno dell'ambiente fisico, creando meccanismi di resilienza adattivi e semiautonomi.

In questo quadro di riferimento molto complesso sia a livello nazionale che internazionale, AIIC ha deciso di dare il proprio contributo con un Gruppo di Lavoro dedicato, con l'obiettivo di produrre un Rapporto entro il mese di Maggio 2027, dal titolo *"Artificial Intelligence for Critical Infrastructure Resilience in an Underwater Environment"*. Possono contribuire alla stesura del Rapporto tutti i Soci AIIC, semplicemente contattando il Coordinatore del GdL s.bologna@infrastrutturecritiche.it

Sandro Bologna



Graduated in Physics at the Sapienza University of Rome. At the present the main research activity concerns Critical Infrastructure Resilient to Disasters of different nature, with particular attention to the modeling, simulation and analysis of vulnerabilities and interdependencies, as well as the use of different technologies in order to increase their security. Recently he has started working on the topic of Sustainable Development Indices with reference to the Sustainable Development Goals of the 2030 Agenda.



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 2027

Il 31 dicembre 2026 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 2027".

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 2026, pagando la relativa quota sociale, il nuovo socio avrà diritto a vedere la propria iscrizione valida fino a tutto l'anno 2027.

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



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

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

AI Act, cosa entra in vigore dal 2 agosto 2026 e cosa slitta - Dal 2 agosto 2026 diventano efficaci gli obblighi di trasparenza dell'AI Act, mentre slittano molte regole sui sistemi ad alto rischio. Per le imprese italiane cambiano chatbot, contenuti sintetici, contratti, governance e controlli interni, con sanzioni già operative

Il 2 agosto 2026 acquista efficacia il nucleo generale dell'AI Act rimasto fuori dalle tappe anticipate del 2025 e dalle proroghe dell'AI Omnibus, con un perimetro diverso da quello raccontato negli ultimi mesi. Le regole sui sistemi ad alto rischio, tra cui valutazione di conformità, sistema di gestione della qualità, sorveglianza umana e gestione degli incidenti, sono state spostate al 2 dicembre 2027 per i casi dell'Allegato III e al 2 agosto 2028 per i prodotti dell'Allegato I. Quello che resta fermo al 2 agosto 2026 sono gli obblighi di trasparenza verso il pubblico.

Restano fermi anche il sistema sanzionatorio nazionale e i poteri pieni che la Commissione esercita sui fornitori di modelli per finalità generali. È un impatto più ristretto di quanto si temesse un anno fa, ma anche più immediato di quanto suggerisca la narrazione del rinvio. Tocca il modo in cui un'azienda parla con i propri clienti e il modo in cui un consiglio di amministrazione decide.

Indice degli argomenti

AI Act 2 agosto 2026, gli obblighi di trasparenza verso il pubblico

Contenuti generati dall'intelligenza artificiale e deepfake

Testi generati dall'IA e responsabilità editoriale

Riconoscimento delle emozioni e categorizzazione biometrica

Per le imprese italiane serve un censimento dei sistemi già in uso

Sanzioni AI Act e poteri della Commissione sui modelli GPAI

Sistemi ad alto rischio, cosa slitta al 2027 e al 2028

AI Act e diritto societario: il ruolo degli amministratori

Verbali, contratti e due diligence nell'adeguamento all'AI Act

Governance dell'intelligenza artificiale oltre l'adempimento

(continua)

<https://www.agendadigitale.eu/sicurezza/ai-act-cosa-entra-in-vigore-dal-2-agosto-2026-e-cosa-slitta/>

Agenda Digitale - Francesca Niola, 30 lug 2026

Con un anno di ritardo, il CDM ha completato l'esame del Piano Sociale per il Clima - Il 4 agosto il CDM ha approvato il Piano Sociale per il Clima, predisposto dal Ministero dell'Ambiente e della



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

Sicurezza Energetica. Lo strumento, dal valore complessivo di 9,3 miliardi di euro, è pensato per accompagnare la transizione energetica e mitigare gli effetti economici e sociali derivanti dall'ETS2, il nuovo sistema europeo di scambio delle quote di emissione per l'edilizia e il trasporto stradale, che sarà operativo dal 2028. Ora si può procedere alla trasmissione formale del Piano alla Commissione Europea. L'entrata in vigore dell'ETS2 è stata rimandata dal 2027 al 2028, ma la Commissione Europea ha previsto ugualmente la possibilità di avviare il Fondo Sociale per il Clima per finanziare la compensazione degli effetti sociali della transizione energetica. Il Fondo finanzia interventi di efficientamento energetico delle abitazioni, la diffusione delle energie rinnovabili e la promozione della mobilità sostenibile. Il Fondo Sociale per il Clima è strettamente legato all'ETS2. L'Italia, tuttavia, è molto in ritardo perché avrebbe dovuto trasmettere a Bruxelles la versione definitiva del Piano Sociale per il Clima già un anno fa per poter avviare un confronto con la Commissione UE.

Il Piano italiano avrebbe dovuto essere operativo già dall'inizio del 2026 ma per dodici mesi le organizzazioni della società civile coinvolte nella fase iniziale di consultazione non hanno ricevuto aggiornamenti sul contenuto del testo. (continua...)

<https://www.rinnovabili.it/mercato/politiche-e-normativa/cdm-piano-sociale-per-il-clima-case-elettrificazione-trasporti/>

Rinnovabili - Erminia Voccia, 6 agosto 2026

Il clima cambia più in fretta degli edifici: serve una progettazione adattiva - Le nostre case sono davvero pronte al clima del futuro? Tra ondate di calore, notti tropicali ed eventi meteorologici estremi, l'articolo propone una riflessione sul futuro della progettazione edilizia, mostrando come architettura, innovazione tecnologica e comportamento degli occupanti possano contribuire a realizzare edifici più adattivi, resilienti e capaci di garantire comfort e benessere anche nel clima di domani.

Il cambiamento climatico impone di volgere lo sguardo verso una nuova progettazione: dall'efficienza energetica all'edificio adattivo, capace di garantire comfort e resilienza anche con l'evoluzione climatica di domani.

L'edificio adattivo rappresenta l'evoluzione dell'edificio efficiente: non deve soltanto consumare meno, ma mantenere comfort e prestazioni anche in un clima che cambia. Ondate di calore, notti tropicali ed eventi estremi impongono di ripensare involucro, schermature, ventilazione e gestione degli impianti. Strategie bioclimatiche, BACS, SRI e comportamento degli occupanti diventano così parti di un unico sistema progettuale. L'articolo analizza questo cambio di paradigma e il ruolo del progettista nel costruire oggi edifici capaci di funzionare bene anche nel clima di domani.

Dall'efficienza energetica al comfort adattivo: perché il clima non stazionario cambia i criteri di progettazione

Le nostre case sono davvero pronte al clima del futuro?

Negli ultimi trent'anni il settore delle costruzioni ha mostrato il suo importante contributo nella mitigazione dei consumi energetici degli edifici. Si hanno isolamenti sempre più performanti e serramenti ad alta efficienza, la riduzione dei ponti termici è uno degli aspetti maggiormente presi in considerazione in fase progettuale e realizzativa, infine, il ricorso a sistemi impiantistici evoluti e a fonti rinnovabili hanno consentito di soddisfare il più possibile i fabbisogni energetici del patrimonio edilizio, contribuendo agli obiettivi di decarbonizzazione imposti a livello europeo.

(continua)

<https://www.ingenio-web.it/articoli/edificio-adattivo-comfort-estivo-cambiamento-climatico/>

Ingenio - Alessandra Gugliandolo, 18 agosto 2026

I modelli General Purpose Artificial Intelligence (GPAI): opportunità, compliance e rischi per le imprese - Oggigiorno l'intelligenza artificiale (IA) è sempre più evocata, in particolare, in ambienti



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

lavorativi aziendali, dove la stragrande maggioranza ascolta, riflette, cerca di capire frequentando corsi di formazione – per la maggior parte erogati in versione elearning – ma, nei dettagli, non ne riesce ad inquadrare gli ambiti di applicazione. In altri termini, mentre l'IA si appresta a modificare processi organizzativi, ad introdurre nuovi schemi decisionali e a gestire le informazioni, le Risorse Umane e le parti sociali nutrono un'apparente preoccupazione con riguardo all'impatto occupazionale che ne potrebbe derivare nel prossimo futuro.

A tal proposito, nel tentativo di sgombrare il campo da tali preoccupazioni – per lo più connesse alla rapida affermazione di una rivoluzionaria tecnologia e, nel contempo, alla mancata consapevolezza di come essa si declina nella vita lavorativa di tutti i giorni, con il presente lavoro inizio l'illustrazione tematica di alcune componenti dell'IA partendo dai cc.dd. General Purpose Artificial Intelligence Models (GPAI), vale a dire modelli funzionali progettati e sviluppati per svolgere molteplici compiti mediante l'integrazione nelle diverse applicazioni aziendali.

Nel colmare il vuoto normativo in tale ambito, il legislatore europeo ha dedicato una specifica disciplina ai citati modelli – già in essere in diverse realtà aziendali – con l'adozione del Regolamento (UE) 2024/1689 (AI Act), laddove ha tracciato il perimetro legale di possibili applicazioni tecnologiche e di impatto nella realtà digitale che ci circonda.

I modelli GPAI: di cosa parliamo?

Proprio l'AI Act viene in soccorso definendo il GPAI come un modello di intelligenza artificiale dotato di particolare capacità nell'eseguire molteplici attività costituendo un tutt'uno con i sistemi informatici operanti nelle diverse realtà aziendali o anche utilizzati a livello personale. Tra essi rientrano i modelli linguistici, conosciuti anche come LLM (Large Language Model)¹, nonché numerosi altri modelli multimodali in grado di elaborare testi, immagini, audio e altri contenuti digitali. (continua...)

<https://www.snewsonline.com/modelli-general-purpose-artificial-intelligence-gpai-opportunita-compliance-rischi-imprese/>

SNews - Domenico Voza - 25 Agosto 2026

Russian APT BlueDelta Uses HOOKEDGE to Target Defense and Diplomatic Organizations

BlueDelta (APT28) uses webhook.site and Microsoft Edge to hide HOOKEDGE espionage traffic targeting European governments.

Recorded Future's Insikt Group documented a campaign by BlueDelta, the Russian GRU-linked group that overlaps with the group APT28, running an entire espionage operation against European government targets using webhook.site, a service built for developers to test HTTP requests, as its command-and-control backbone.

The campaign ran from late September 2025 through early April 2026, targeting government and diplomatic organizations in Romania, Spain, and Türkiye.

"The campaigns delivered a lightweight Windows batch-script backdoor, dubbed "HOOKEDGE," via macro-enabled Microsoft Word documents using diplomatic-themed lures, including material impersonating Spain's Ministry of the Presidency, Justice and Relations with the Cortes, created shortly after a September 2025 meeting between Spanish and Moldovan officials." states the report by Insikt Group.

"Insikt Group assesses with moderate confidence that this activity was conducted by BlueDelta (which overlaps with APT28, Fancy Bear, and Forest Blizzard), a Russian state-sponsored threat group attributed to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU)."

The attackers used a fairly old-school trick: macro-enabled Word documents. One of them looked like a real meeting agenda from Spain's Ministry of the Presidency and appeared shortly after an actual meeting between Spanish and Moldovan officials. The timing was interesting because it came just



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

before Moldova's September 2025 parliamentary elections. The document looked credible enough to make the phishing attempt believable. (continua...)

<https://securityaffairs.com/197996/apt/russian-apt-bluedelta-uses-hookedge-to-target-defense-and-diplomatic-organizations.html>

SecurityAffairs -Pierluigi Paganini- 28 agosto 2026

You Need Cyber Deception for OT

The frustrating reality after an OT cyberattack: no data, no trail, and no history.

OPINION

There are three statements that sum up the frustrating reality for defenders responding to a cyberattack on operational technology (OT) systems: The attack data is not there. There is no trail to follow. There is no history to sort through.

While these dynamics will always be true for OT, defenders are getting help from cyber deception as it matures beyond honeypots to a more sophisticated, proactive cyber-defense tool.

To illustrate the problem, let's go back in time. Nearly 12 years ago, portions of Ukraine's electric grid went dark. It was an IT-to-OT attack, one that originates in the IT portion of the network and moves to the OT network. The adversary first established a position in enterprise systems, performed extensive reconnaissance, harvested credentials, found the paths toward operational systems, and then crossed into the technology that controlled the key components of the grid.

The pivot from IT into OT creates a debilitating problem: The OT half of the environment produces no useful security telemetry. It's also not so great at providing logs or forensics. The result is an uncomfortable reality: After an attacker reaches OT, the defender will be looking for evidence in an environment that was never designed to produce it.

Where Are the Attackers?

In a normal IT investigation, a security team will ask familiar questions: Which user authenticated to the system? Was the login interactive or remote? What process executed? Which parent process launched it? Was PowerShell used? Did the host make a connection to a known command-and-control (C2) address? Was a new service created? Was an endpoint detection agent disabled? Did a file hash match known malware? Did a security information and event management (SIEM) system correlate the activity with other suspicious events?

In OT environments, those questions are difficult or impossible to answer with confidence.

A programmable logic controller (PLC) will not tell you that an attacker queried it. A remote terminal unit (RTU) will not produce meaningful authentication logs. A camera system will not provide security event details. A printer VLAN will not be monitored at all. A building management controller will provide little visibility into reconnaissance, failed access, enumeration, or command attempts.

Even when logs exist, they may be retained locally, overwritten quickly, unavailable to the SIEM, or written in formats that do not map cleanly to normal security analytics. For defenders relying on signature or heuristics tools, the likelihood of detecting the attacker will be low. A signature-based tool cannot match a signature against telemetry it never receives. A SIEM cannot correlate events that were never collected. A log analytics tool cannot detect an attack path that passes through assets with no meaningful logs.

Cyber Deception Is a Tool for Both Sides of IT-to-OT Attacks

Cyber deception addresses these problems while providing insights across the entire attack path from IT to OT. In a well-designed deception defense, the attacker will be presented with the exact information and devices needed to continue the attack. There will be information about the network, and there will



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

be vulnerable assets to navigate. Each of these will capture forensics and alert defenders in real time.(continua...)

<https://www.darkreading.com/ics-ot-security/you-need-cyber-deception-ot>

DarkReading - Scott Hawk-August 28, 2026

Caldo estremo e allagamenti: come Houten, Parigi e Totnes stanno riprogettando la città - Dalla mostra Too Hot esposta al Deutsches Architekturmuseum di Francoforte, altri tre casi di centri urbani europei impegnati a contrastare gli effetti del climate change: Houten nei Paesi Bassi, Parigi e Totnes in Gran Bretagna.

Prosegue il viaggio di Ingenio tra le città europee che alle diverse latitudini sono impegnate a contrastare il cambiamento climatico, così come sono raccontate nella mostra Too Hot - Heiße Städte, neue Wege (Città calde, nuove strade) in calendario al Deutsches Architekturmuseum di Francoforte fino al 7 febbraio prossimo.

Nel primo dei cinque articoli in programma, abbiamo descritto le esperienze e i risultati di tre centri urbani collocati nella zona climatica Boreale: Lappeenranta, Liepaja, Stoccolma.

In questo secondo contributo si raccontano i casi di Houten nei Paesi Bassi, Parigi e Totnes in Gran Bretagna, città ricomprese nella zona climatica Atlantica.

Crisi climatica. L'esempio di tre città della zona Atlantica

Houten (Paesi Bassi)

Houten, centro urbano non lontano da Utrecht, è una città modello costruita negli Anni '60. Grazie a una pianificazione urbanistica improntata alla sostenibilità ambientale, dai suoi tremila abitanti originari oggi ospita oltre 50mila residenti.

La città è dotata di una rete stradale circolare, pensata e realizzata per tenere le auto fuori dal centro, mentre una rete di piste ciclabili e pedonali sicure modellano il tessuto urbano e una serie di spazi verdi collegano i quartieri.

Sebbene sia stata progettata come città per le due ruote, i cambiamenti climatici hanno portato nuove sfide: piogge torrenziali e inondazioni hanno reso necessarie politiche di adattamento. Allo stesso tempo, la città si è impegnata a ridurre la dipendenza dai combustibili fossili e a proteggere dal caldo intenso ciclisti e pedoni.

Ogni anno, con l'obiettivo di raggiungere la neutralità climatica, la municipalità del centro olandese investe risorse pubbliche nella piantumazione di alberi, nella de-pavimentazione, nell'ampliamento della circolazione ciclabile e pedonale e nel sostegno agli impianti eolici e solari locali.

(continua)

<https://www.ingenio-web.it/articoli/adattamento-climatico-citta-houten-parigi-totnes/>

Ingenio - Pietro Mezzi, 31 agosto 2026

L'intelligenza artificiale può rendere più letali gli attacchi terroristici - Uno studio mette in evidenza come il gruppo terroristico di Boko Haram in Nigeria utilizza l'intelligenza artificiale per mettere a punto nuove e più efficaci tecniche di attacco.

Uno studio recentemente pubblicato dall'Università di Cambridge mette in evidenza come il gruppo terroristico di Boko Haram, operativo in Nigeria, ha cominciato a utilizzare applicativi di intelligenza artificiale per mettere a punto nuove e più efficaci tecniche di attacco.

Un grande apprezzamento va indirizzato agli esperti dell'università, che sono riusciti a entrare in comunicazione con soggetti terroristici, per avere informazioni aggiornate su questo nuovo approccio alla pianificazione della loro attività.



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

Fino alla pubblicazione di questa ricerca, l'uso di intelligenza artificiale da parte di movimenti terroristici è stato individuato grazie ad alcune tracce lasciate su Internet, senza conferme esplicite.

La recente intervista invece ha messo in evidenza come i terroristi utilizzino questi applicativi in vari modi, appresso illustrati.

Un capo di questo gruppo ha recentemente dichiarato: "Dio ci ha aiutato e così ci aiuterà l'intelligenza artificiale!".

(continua...)

<https://www.puntosicuro.it/criminalita-C-105/l-intelligenza-artificiale-puo-rendere-piu-letali-gli-attacchi-terroristici-AR-26687/>

Punto Sicuro - Adalberto Biasiotti- 2 settembre 2026

What the AI Warning Letter Completely Missed

The recent open letter is right about the "window," but it omits naming who is coming through it or, critically, who will close it.

OPINION

Recently, more than 100 technology companies — OpenAI, Anthropic, Microsoft, and Google among them — published an open letter warning that AI is about to make sophisticated cyberattacks far cheaper and far more common, and that "we have a limited window to strengthen cyber defenses."

I read it twice. The first time as the head of a security organization, nodding along to very nearly every line. The second time hunting for the part about who actually does the work. I did not find it.

Before I get to the argument you can feel coming, I must acknowledge there is much this letter gets right. The threat is not hypothetical. On Aug. 19, five US federal agencies documented threat actors using AI-generated exploitation scripts, disguised as legitimate monitoring tools, against exposed Siemens S7 controllers, the sort that run water treatment plants, power stations, and chemical plants. Building such a tool once demanded specialist protocol knowledge. That knowledge was, in practice, the moat around a great many small utilities — that, and the hope of isolation from the Internet. But the moat has been drained, and the people wading across know that.

However, I confess to some skepticism about the premise, and I'm in good company. The same day the letter appeared, analysts at RUSI, Britain's oldest defense think tank, published an assessment of AI and cybercrime that's also worth reading. Their argument: "Criminal innovation is a response to a revenue stream closing, not to a new technology opening a window." Adversaries focus on what pays and not what impresses. Phishing, pilfered credentials, and machines left facing the Internet that never should have been still pay handsomely and at scale. Threat actors are not incurious. They are curious about money, a rather more disciplined curiosity than the one our industry tends to practice.

That is exactly what the recent water-sector campaign actually is: by the agencies' own assessment, it's reconnaissance and pre-positioning. Patient staging and not smash-and-grab. Tellingly, they decline to name who is behind it, even as a sister advisory this summer pinned a parallel wave of programmable logic controller (PLC) attacks squarely on Iran. Whoever it is, they needed no frontier model to stroll through a door that's been left open. Siemens itself conceded the point in its response: no new flaw in the controllers, merely new techniques aimed at old misconfiguration. AI has changed who can write the exploit. It has not changed what stops them.

The evidence points both ways; others report criminal adoption speeding up as open-weight models improve. Which way the next 12 months break, I can't tell you. Nor, and this is the point, do I need to. However it breaks, the assignment does not.

Read the plan closely. Fix your highest-risk weaknesses. Raise the bar on what you buy, build, and deploy. Scrutinize AI-generated code. Deploy AI-powered defense. Share intelligence.



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

Every recommendation is a verb, and every verb in security is performed by a person. It is a plan written entirely in verbs, with no subject. Should the adversary come through the window, the plan wants for trained operators. Should they never come, defending against the attacks already upon us wants the same operators performing the same verbs. The plan is identical in either future. Only the people are missing from it.

The AI Defense Gulf Is Measured in People

Consider the defenders the letter itself names as most exposed: hospitals, water utilities, the small operators of critical infrastructure. Its single most effective mitigation is thoroughly unglamorous and has nothing to do with frontier AI: Take the Internet-facing controllers off the Internet. For a well-staffed security team, that is a Tuesday afternoon. For a rural water utility whose entire IT function is one exhausted engineer wearing five hats, it may as well be written in Aramaic. The gulf between those two is measured in people, not products, and no model subscription closes it. The adversary keeps what is profitable and discards the elegant; we do the precise reverse and call it progress.

There is also a deeper incoherence. We are told in one breath that these models are so uncontrollable that no one can be held accountable when they get out and break the law, and in the next that it should be trusted to defend our critical infrastructure. Both can't be true. Judicious use, by the right skilled people, is the only sane way to hold those two thoughts together.

This points to three things I should dearly have liked to see in the letter and should still like to see from its signatories. /(continua....)

<https://www.darkreading.com/cyberattacks-data-breaches/ai-warning-letter-missed-people>.

DarkReading James Lyne -September 3, 2026

Cyber Resilience Act: cosa cambia dall'11 settembre

In vigore dal 2024, il Cyber Resilience Act prevede severi obblighi di segnalazione dall'11 settembre 2026. Ecco cosa comportano gli obblighi di comunicazione dell'articolo 14

L'11 settembre 2026 è una data chiave per l'applicazione del **Cyber Resilience Act (CRA)**, il Regolamento (UE) 2024/2847 in vigore dal 2024.

L'Articolo 14 rende subito operativi i primi, severi obblighi di segnalazione: da questa data i fabbricanti di prodotti con elementi digitali dovranno **segnalare le vulnerabilità attivamente sfruttate e gli incidenti gravi con impatto sulla sicurezza del prodotto**, secondo **tempistiche stringenti**.

Indice degli argomenti

- Cyber Resilience Act: le novità in vigore dall'11 settembre
 - Cosa cambia dall'11 settembre
- I 3 passaggi del meccanismo
 - Perimetro di applicazione
- La catena di fornitura
 - I multi-livelli del quadro sanzionatorio
- Le linee guida della Commissione europea
- La roadmap: la piena applicazione dal 2027

Cyber Resilience Act: le novità in vigore dall'11 settembre

Il regolamento è entrato in vigore il 10 dicembre 2024 e avrà **piena applicazione dall'11 dicembre 2027**, ma alcune disposizioni sono state anticipate.

L'11 giugno 2026 è entrato in applicazione il capo relativo alla notifica degli organismi di valutazione della conformità; **dall'11 settembre scattano invece gli obblighi di comunicazione dell'articolo 14.**



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 una vulnerabilità viene sfruttata in un prodotto distribuito su larga scala, la rapidità con cui l'informazione circola può diventare parte della risposta all'incidente.

Il CRA non impone di segnalare ogni vulnerabilità scoperta nel codice. **L'articolo 14 riguarda le vulnerabilità attivamente sfruttate** contenute nel prodotto con elementi digitali e **gli incidenti gravi che hanno un impatto sulla sicurezza del prodotto.**

Una falla individuata durante un test o un'attività di ricerca, senza elementi che mostrino un suo sfruttamento effettivo, non determina quindi automaticamente una notifica.

Se emergono invece evidenze che la vulnerabilità è stata utilizzata da un attore malevolo, il fabbricante deve attivare la procedura senza indebito ritardo e comunque entro i termini stabiliti.

Cosa cambia dall'11 settembre

Le comunicazioni confluiranno nella nuova **Single Reporting Platform**, la piattaforma europea istituita e gestita da ENISA.

La notifica viene indirizzata al CSIRT designato come coordinatore nello Stato membro in cui il fabbricante ha il proprio stabilimento principale e, salvo circostanze eccezionali previste dal regolamento, le informazioni vengono rese contemporaneamente disponibili a ENISA.

Il CSIRT che riceve la comunicazione provvede a diffonderla agli altri CSIRT degli Stati membri nei cui territori il prodotto è stato messo a disposizione. Per l'Italia il coordinatore indicato da ENISA è CSIRT Italia dell'Agenzia per la cyber sicurezza nazionale.

La piattaforma sarà operativa proprio dall'11 settembre 2026 e, nella fase iniziale, supporterà le notifiche obbligatorie previste dall'articolo 14. ENISA ha chiarito che il sistema consente una sola comunicazione, evitando di trasmettere separatamente la stessa segnalazione alle autorità dei diversi Paesi interessati.

Se la piattaforma è temporaneamente indisponibile, la notifica deve essere presentata attraverso la SRP una volta ripristinata; se è necessaria una comunicazione immediata, può essere contattato direttamente il CSIRT competente, senza che ciò sostituisca la successiva trasmissione attraverso la piattaforma. (continua...)

<https://www.cybersecurity360.it/legal/cyber-resilience-act-cosa-cambia-dall11-settembre/>

Cybersecurity360 -Luisa Franchina,Tommaso Diddi -10 set 2026

Rapporto Anthropic: l'AI non inventa il cybercrime, lo rende industriale

Il nuovo rapporto Anthropic mostra come l'AI stia riducendo tempi, costi e competenze necessari per condurre operazioni offensive complesse. Cybercrime, frodi, propaganda, sorveglianza e ricerca di vulnerabilità diventano workflow automatizzati e scalabili, gestibili da gruppi sempre più piccoli

L'intelligenza artificiale **non è più soltanto uno strumento usato da un operatore umano per scrivere codice, tradurre un messaggio o cercare informazioni.** Il rapporto dal titolo **"Detecting and countering misuse of AI: September 2026"** pubblicato da Anthropic il 10 settembre 2026 testimonia uno scenario allarmante quanto atteso: **l'AI sta diventando una componente operativa delle azioni offensive** capace di collegare ricognizione, sviluppo di strumenti, intrusione, raccolta dati, propaganda, sorveglianza e frode.

Il documento analizza attività individuate e interrotte tra dicembre 2025 e agosto 2026. Le operazioni riguardano sette aree: cybercrime, influenza, sorveglianza, frodi, ricerca biologica, sviluppo di armi convenzionali e tentativi di estrarre le capacità dei modelli di frontiera.

Anthropic precisa che si tratta dei casi più rilevanti osservati, non di un campione rappresentativo di ogni abuso di Claude. In parole povere, **ci troviamo dinanzi alla punta dell'iceberg.**



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 conclusione più importante non riguarda la comparsa di tecniche completamente nuove. **Il cambiamento è economico e organizzativo:** l'AI riduce il numero di persone, il tempo e le competenze necessarie per condurre operazioni che in passato richiedevano team specializzati.

Indice degli argomenti

- Dall'assistente all'orchestratore
- Cambia la scala delle operazioni di cybercrime
- Sorveglianza e propaganda automatizzate
- Frodi, sistemi d'arma e ricerca biologica
- Distillazione illecita e attacco alla supply chain dell'AI
- La geopolitica impedisce la pausa

Dall'assistente all'orchestratore

Il rapporto descrive l'**uso di Claude oltre la normale interazione conversazionale**. In numerosi casi, gli attori hanno impiegato **framework multi-agente** per eseguire ricognizione, sfruttare vulnerabilità, raccogliere credenziali ed esfiltrare dati, lasciando agli operatori umani soprattutto la selezione dei bersagli e la valutazione dei risultati.

Il caso più rilevante riguarda un gruppo di lingua cinese, identificato come GTG-10007, che avrebbe preso di mira circa 50 organizzazioni nei settori pubblico, energia, sanità, finanza, tecnologia, manifattura e istruzione. L'operazione era organizzata come una vera pipeline: workflow distinti gestivano le varie fasi dell'attacco come ricognizione, ricerca di vulnerabilità, sviluppo del malware, intrusione e raccolta dei dati.

Gli agenti AI mantenevano una memoria persistente con informazioni sui bersagli, credenziali e stato delle operazioni, permettendo di riprendere e coordinare le attività senza ricominciare ogni volta da zero. Più agenti lavoravano in parallelo: alcuni effettuavano scansioni continue, altri analizzavano firmware e binari di dispositivi di sicurezza alla ricerca di vulnerabilità.

Un vero e proprio esercito di esperti che collaboravano per il conseguimento dell'obiettivo comune, ed i risultati confermerebbero l'efficacia della strategia. Secondo Anthropic, una singola catena di ricerca avrebbe individuato oltre una dozzina di possibili **zero-day** in un mese, poi sottoposti a verifica in laboratorio.

L'aspetto più significativo è però la capacità di chiudere automaticamente il ciclo attacco-difesa. Un workflow controllava se gli strumenti malevoli venivano rilevati dagli strumenti di sicurezza; quando individuava una detection, modificava il codice, lo ricompilava per aggirare il rilevamento e lo ridistribuiva.

Si crea così un ciclo continuo: il difensore aggiorna la detection, l'attaccante modifica automaticamente il malware e ripete l'attacco. In questo scenario, le firme statiche rischiano di perdere efficacia perché il codice malevolo può cambiare più rapidamente della capacità del difensore di aggiornarne gli indicatori.(continua...)

<https://www.cybersecurity360.it/nuove-minacce/rapporto-anthropic-lai-non-inventa-il-cybercrime-lo-rende-industriale/>

Cybersecurity360 -Pierluigi Paganini - 14 set 2026

L'affidabilità dell'AI richiede controlli indipendenti e regole comuni. Parla Quattrococchi

Il professore ordinario presso l'Università Sapienza di Roma, dove dirige il Centro di Scienza dei Dati e Complessità per la Società (CDCS), commenta con Formiche.net il dibattito sull'AI: "Servono regole che separino chi genera da chi certifica, limiti tecnici sulle azioni che possono produrre conseguenze reali, accesso indipendente ai modelli e responsabilità umane chiaramente attribuite"



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 dibattito sull'intelligenza artificiale è tornato ad accendersi dopo le dichiarazioni di **Dario Amodei**, ceo di Anthropic, che ha messo in guardia dai rischi estremi legati allo sviluppo della tecnologia, arrivando a chiedere una maggiore cautela al settore. Ne abbiamo parlato con **Walter Quattrociochi**, professore ordinario della Sapienza Università di Roma e direttore del Centro di Scienza dei Dati e Complessità per la Società (CDCS).

Professore, cosa ci dice l'appello di Amodei?

La parte interessante dell'appello di Amodei, per me, non sono le profezie sulla superintelligenza. Quelle restano scenari costruiti su molte ipotesi difficili da quantificare. La parte importante è un'altra: Amodei riconosce che non possiamo lasciare alle aziende il compito di certificare da sole l'affidabilità dei sistemi che costruiscono e propone valutatori indipendenti con accesso molto profondo ai modelli. Questo è un passo nella direzione giusta.

Come possiamo compierlo?

Il punto tecnico è semplice. Un LLM genera sulla base delle regolarità apprese e della compatibilità con il contesto. All'interno di quello stesso processo generativo non possiede un criterio generale che gli consenta di stabilire se ciò che sta producendo sia vero o affidabile. Può essere molto accurato, anche straordinariamente accurato, ma chiedergli di certificare la propria risposta significa ancora interrogare lo stesso tipo di generatore. La verifica deve quindi arrivare da fuori. Per questo, aprire ai ricercatori indipendenti è utile, ma non basta una semplice concessione da parte delle aziende. Servono protocolli comuni, accesso stabile, criteri condivisi e risultati riproducibili. Altrimenti il controllato sceglie anche come deve essere controllato.

Come valutare le risposte a supporto di Amodei dei vari Elon Musk e Sam Altman, con quella del presidente Trump?

Dire "vogliamo essere verificati" è la parte facile. La parte interessante comincia quando il verificatore può arrivare a conclusioni sgradite all'azienda, pubblicarle e continuare ad avere accesso. È lì che vedremo quanto questa apertura sia reale. Trump rappresenta invece perfettamente l'altro lato del problema: la logica della corsa. Se la domanda diventa "chi arriva prima, Stati Uniti o Cina?", ogni forma di cautela viene immediatamente interpretata come perdita di vantaggio competitivo. Trump ha infatti minimizzato gli allarmi insistendo sulla necessità di mantenere il primato americano. Il guaio è che l'affidabilità non si produce accelerando. E non è una proprietà che possiamo semplicemente chiedere al modello di dichiarare. Va costruita attraverso verifiche, limiti operativi, accessi controllati e responsabilità esterne.

C'è chi è convinto che siamo finiti in una lotta di potere tra Big Tech, che giocano con la sicurezza per accrescere il loro status. È d'accordo?

Non serve una teoria del complotto. Basta guardare gli incentivi. Per un'azienda dire "abbiamo costruito un ottimo strumento statistico" è una buona pubblicità. Dire "stiamo costruendo qualcosa di così potente che potrebbe diventare incontrollabile" è una pubblicità ancora migliore. La retorica della potenza e quella del pericolo possono alimentarsi reciprocamente. Questo però non significa che i problemi di sicurezza siano inventati. Significa che proprio perché sono reali non possiamo lasciare alle aziende la definizione del rischio, la misura del rischio e la certificazione della soluzione. Sarebbe come chiedere al produttore di un farmaco di stabilire da solo efficacia, effetti collaterali e autorizzazione alla vendita. Il nodo è sempre lo stesso: se chi produce è anche chi verifica, non abbiamo una verifica indipendente. E c'è un secondo rischio. (continua....)

<https://formiche.net/2026/09/intervista-quattrociochi-dibattito-ai/#content>

Formiche Lorenzo Santucci -14/09/2026

NOTIZIE D'INTERESSE:



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

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

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.