



CYBER 4.0, 28 SETTEMBRE 2026

Il trasferimento tecnologico che funziona: al MIMIT i dati sull'attività dei competence center italiani

Il 28 settembre, nella Sala degli Arazzi del Ministero delle Imprese e del Made in Italy, si è tenuta la presentazione della ricerca condotta dal CNR e dall'Università di Padova sull'impatto generato dai Centri di Competenza finanziati con risorse del Piano Nazionale di Ripresa e Resilienza. Hanno aperto l'evento il Viceministro Valentino Valentini e il Capo di Dipartimento Marco Calabrò. Nel corso dell'incontro è stato firmato l'Atto Costitutivo dell'Associazione Competence Center Italia.



LEGGI TUTTO

Articoli Correlati:

- [Innovation Post, Il futuro del trasferimento tecnologico e il ruolo dei Competence Center dopo il PNRR, 28 Settembre 2026](#)
- [Industria Italiana, Mimit, dai Competence Center 320 milioni di progetti, 4.700 servizi alle imprese e 57mila persone formate, 24 Settembre 2026](#)

ACN, 1 OTTOBRE 2026

È online la seconda open call del progetto europeo Secure coordinato da ACN

Il nuovo bando per il finanziamento del progetto **SECURE** – Strengthening EU SMEs Cyber Resilience mette a disposizione delle imprese europee 11,5 milioni di euro per realizzare interventi volti a migliorare la sicurezza dei prodotti con elementi digitali e accompagnare le imprese nel percorso di adeguamento ai requisiti introdotti dal Cyber Resilience Act (CRA). Il finanziamento coprirà il 50% dei costi ammissibili, fino a un contributo massimo di 30.000 euro per impresa.



LEGGI TUTTO

CYBER 4.0

CYBER 4.0, 22 SETTEMBRE 2026

Cyber Capacity Building Italia-Ghana: al via a Roma la study visit della delegazione ghanese

Il programma bilaterale di Cyber Capacity Building tra Italia e Ghana, implementato da Cyber 4.0 nell'ambito della cooperazione con il Ministero degli Affari Esteri e della Cooperazione Internazionale (MAECI) e la Cyber Security Authority (CSA) del Ghana, entra in una nuova fase con l'avvio della study visit della delegazione interistituzionale ghanese, composta da rappresentanti della Cyber Security Authority, della magistratura, delle Forze Armate, del Ghana Immigration Service e del Ministero degli Esteri.

LEGGI TUTTO

Articoli Correlati:

- [ACN, ACN welcomes a delegation of Ghanaian government officials: cybersecurity and international cooperation at the heart of the visit, September 24, 2026](#)

CYBER 4.0, 30 SETTEMBRE 2026

Cognitive warfare: disinformazione, social engineering e minacce cyber

La cybersecurity non riguarda soltanto la protezione di sistemi, reti e dati. Sempre più spesso, le minacce possono sfruttare anche il **modo in cui le persone interpretano le informazioni, attribuiscono fiducia a una fonte e prendono decisioni**, facendo leva su dinamiche che non dipendono necessariamente da una vulnerabilità tecnica. **È su questi temi che si è concentrato** "Cognitive warfare: disinformazione, social engineering e minacce cyber", quarto appuntamento del ciclo di seminari sulla cybersecurity promosso dal **Ministero delle Imprese e del Made in Italy**, in collaborazione con **Cyber 4.0** e la **Scuola Superiore di Specializzazione in Telecomunicazioni**.

LEGGI TUTTO



IN ITALIA

ACN, 18 SETTEMBRE 2026

Le novità per i soggetti NIS

La riunione plenaria del Tavolo di attuazione della NIS dell'Agenzia per la cybersicurezza nazionale, con le Autorità di settore e i rappresentanti regionali, ha approfondito le determinazioni del Direttore generale di ACN. È stato disposto **l'aggiornamento dell'elenco dei soggetti NIS**, che riguarda oltre 2000 registrazioni tardive e circa 2000 istruttorie di revisione, analizzate da ACN da maggio a luglio. L'attività fa parte del percorso collaborativo di attuazione dell'Autorità nazionale NIS portato avanti da ACN per assicurare il presidio efficace del tessuto produttivo del Paese.

LEGGI TUTTO



INNOVATION POST, 24 SETTEMBRE 2026

Crescono i cyber attacchi alle aziende manifatturiere. In Italia un attacco su 5 colpisce l'industria

Gli attacchi al settore manifatturiero sono in crescita del 30% nel mondo. E anche in Italia la situazione è critica: il 18,6% degli attacchi colpisce la manifattura. Le aziende hanno fatto progressi nei controlli di base, ma restano criticità su inventario, vulnerability assessment e budget OT. I numeri resi noti al Security Summit OT di Clusit.

LEGGI TUTTO



ANSA, 30 SETTEMBRE 2026

Aziende italiane prime vittime di attacchi ransomware, l'87% paga il riscatto

L'intelligenza artificiale è sempre più un'arma a doppio taglio per le imprese italiane. Se da un lato i software generativi permettono di velocizzare molte operazioni, automatizzando i flussi di lavoro, dall'altro si alza il rischio di concedere troppe informazioni agli "agenti", i programmi che svolgono attività in autonomia, senza un intervento umano. Quando non c'è sufficiente controllo, le IA possono cadere nella trappola degli hacker, e l'intera azienda ne paga le conseguenze. Stando ai più recenti dati degli esperti di sicurezza informatica dei Rubrik Zero Labs, il 49,5% delle imprese italiane ha subito un attacco di tipo ransomware nell'ultimo anno, superando la media globale del 39%. Di queste, ben l'87% decide di pagare un riscatto a seguito di un blocco dei computer causato dai virus che limitano l'accesso a dati e interi sistemi.

LEGGI TUTTO

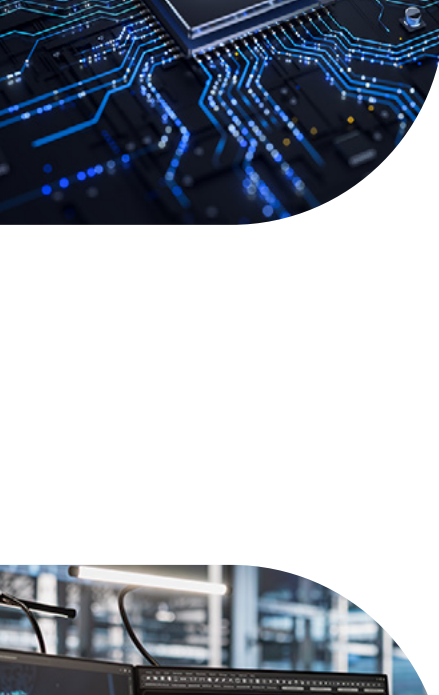


GPDP, 28 SETTEMBRE 2026

Sanzione di 403 milioni a Google, intervento del Garante privacy italiano con la Dpc irlandese

Google è stato condannato a una multa di 403 milioni di euro comminata dall'Autorità irlandese per la protezione dei dati, per aver violato le norme europee (Gdpr) sull'utilizzo dei dati di geolocalizzazione dei propri utenti. Il provvedimento è frutto della collaborazione dell'Autorità italiana Garante della Privacy con la Commissione irlandese per la protezione dei dati (Dpc), l'ente che vigila su Google a livello europeo poiché la sede della società Google Ireland Ltd. si trova a Dublino.

LEGGI TUTTO



POLIZIA POSTALE, 25 SETTEMBRE 2026

Siti clone e intelligenza artificiale: attenzione alle truffe

È sempre più diffuso l'utilizzo di strumenti di Intelligenza Artificiale per finalità di frode: audio che replicano la voce di familiari, video deepfake che, ad esempio, possono copiare volti di personaggi famosi, messaggi di phishing potenziati, privi di errori grammaticali e adatti al profilo della vittima. I sistemi di IA consentono di creare falsi siti, graficamente identici o molto simili a quelli originali, che riproducono loghi, immagini, testi di aziende, istituti di credito, enti e servizi online. L'obiettivo è indurre l'utente a inserire credenziali di accesso, dati personali, informazioni bancarie o altri dati sensibili. I siti clone possono essere raggiunti attraverso link contenuti in e-mail, SMS, messaggi sui social network o applicazioni di messaggistica, ma possono anche comparire tra i risultati di una ricerca online.

LEGGI TUTTO



ANSA, SETTEMBRE 2026

L'italiana Paradigma tra le 10 startup europee ammesse alla Next Frontier AI Challenge

La startup italiana Paradigma è stata scelta tra le 10 Società europee della Next Frontier AI Challenge, il programma dell'agenzia federale tedesca per l'innovazione Spring che conta su 125 milioni di euro di fondi con l'obiettivo di colmare il divario tra Europa e Stati Uniti sull'intelligenza artificiale di frontiera. La startup romana, che è entrata nella prima fase della selezione che gli attribuisce tre milioni di fondi, si è proposta con il proprio progetto che punta ad insegnare alle macchine a fare ricerca scientifica autonomamente, di fatto utilizzando l'intelligenza artificiale per accelerare il modo in cui la ricerca viene condotta, dalla formulazione delle ipotesi fino alla validazione sperimentale.

LEGGI TUTTO

ICT SECURITY MAGAZINE, 30 SETTEMBRE 2026

Responsabilità e rischio nei sistemi di IA: il ruolo del contratto tra AI Act e NIS2

Nel percorso di analisi dedicato alla governance giuridica dell'Intelligenza Artificiale e alla progressiva costruzione del quadro regolatorio europeo, si è evidenziato come il diritto sia chiamato a confrontarsi con una crescente complessità tecnologica e con nuove forme di distribuzione del rischio. In questo contesto, emerge con particolare evidenza un nodo ancora solo parzialmente esplorato dalla dottrina e dalla regolazione.

LEGGI TUTTO



NEWS INTERNAZIONALI

ENISA, SEPTEMBER 22, 2026

Exploring the evolution of the cyber threat landscape: How dependencies weaken our digital resilience

The 2026 ENISA Threat Landscape confirms that cyber dependencies expand the attack surface and require a new level of vigilance to effectively prevent and mitigate the impact of cyber incidents.

LEGGI TUTTO



UNIDIR, SEPTEMBER 18, 2026

From Cyberspace to AI: Translating Norms of Responsible State Behaviour in Cyberspace to AI in the Military Domain

This publication examines what lessons the international community can draw from the development of voluntary norms of responsible State behaviour in information and communications technology (ICT) security for future discussions on AI in the military domain. It argues that norms in ICT security should not be transferred directly to military AI but can serve as useful signposts when adapted to AI's distinctive characteristics, including its dependence on data and autonomous functions.

LEGGI TUTTO

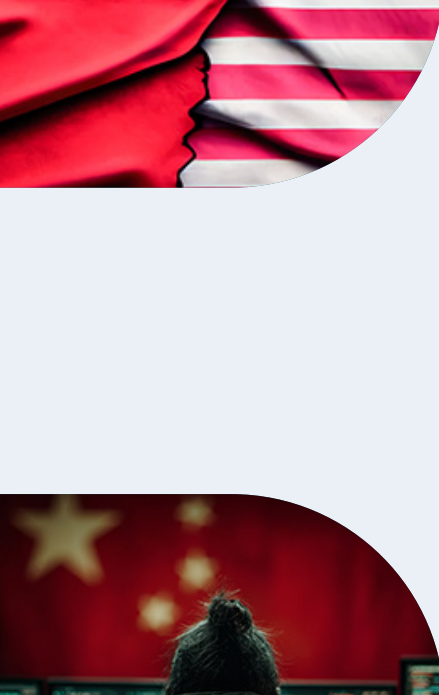


NBC NEWS, SEPTEMBER 21, 2026

20 nations call for new global body to oversee AI ahead of U.N. General Assembly

Leaders and representatives from 20 countries released a statement Monday afternoon calling for increased oversight of advanced AI systems. The statement, posted by the president of Finland, declares that the rapid pace of AI development and recent episodes of AI systems' sidestepping safety protocols demand concerted international coordination.

LEGGI TUTTO



EURONEWS, SEPTEMBER 30, 2026

Top AI and tech firms sign 'morally binding' accord to 'self-police' development after meeting at White House

The accord comes amid massive global pressure from civilians and lawmakers alike to regulate the industry as reports of the technology breaking out of its confines continue to pile. Last week OpenAI revealed that its agent had hacked into an Australian government website during its testing phase.

LEGGI TUTTO



THE GLOBAL EYE, 24 SETTEMBRE 2026

Il vertice Trump - Xi Jinping : un "momento Reykjavik" per la governance dell'IA?

"Governare l'IA" non può restare una formula generica. Significa stabilire in concreto entro quale cornice di responsabilità e di potere essa debba operare; quali limiti debbano vincolarne l'impiego; quali controlli debbano accompagnarne l'uso; quali garanzie debbano essere riconosciute agli individui e agli Stati. L'intelligenza artificiale non è un settore normativo tra gli altri: è un'infrastruttura trasversale che incide sulla formazione delle decisioni, sull'uso della forza, sulla distribuzione delle risorse e sulla qualità stessa dei processi democratici.

LEGGI TUTTO



POLITICO, SEPTEMBER 22, 2026

Chinese hackers targeted shipping in at least seven EU countries, cyber agency reports

A notorious Chinese hacking group carried out cyberattacks against European maritime organizations at a "sustained tempo" throughout 2025, the EU's cyber agency said on Tuesday. Mustang Panda, a China-based cyber-espionage group that U.S. justice department officials accuse of being sponsored by the Chinese government, hit shipping-related organizations with "continuous campaigns impacting at least seven EU member states," EU agency ENISA said in its annual report outlining the cyber threats facing the bloc.

LEGGI TUTTO



LAC4, SEPTEMBER 29, 2026

CyberWeek@LAC4 2026 Agenda Announced! Stronger Together: Shielding the Digital Future of Latin America and the Caribbean

"LAC4's annual flagship event brings together cybersecurity professionals to strengthen practical operational capabilities and advance cross-regional cyber resilience. With a focus on technical expertise and operational experience, CyberWeek@LAC4 2026 provides a space for cybersecurity practitioners and policymakers to exchange knowledge, share lessons learned and explore practical approaches to addressing evolving cyber threats. Ultimately, it's an event about bringing people together, building trust, sharing experiences and turning connections into cooperation. By strengthening these relationships and learning from each other, we build the foundations for more resilient societies." – Liina Areng, LAC4 Director.

LEGGI TUTTO



REUTERS, SEPTEMBER 29 2026

OpenAI shelves new AI model release over safety concerns

OpenAI has scrapped the release of GPT-6.1 Astra, a next-generation AI model planned for an October debut, after internal testing found the system did not meet the company's safety and alignment standards, the ChatGPT maker confirmed on Monday. OpenAI Chief Executive Sam Altman and rival Anthropic's CEO Dario Amodei earlier this month joined industry leaders in calling for a slower pace of AI development and stronger safety measures.

LEGGI TUTTO



INTERPOL, SEPTEMBER 18, 2026

Counter-terrorism operation leverages artificial intelligence to identify 126 terrorism suspects

A first-of-its-kind operation to disrupt terrorist networks in the digital domain has harnessed artificial intelligence to identify suspected terrorists. Operation Shams II (1 – 5 June 2026), coordinated by INTERPOL, brought together 28 specialized officers and experts from 11 countries. During the five days of coordinated action, held in Tunis, Tunisia, law enforcement officers extracted 108,076 facial images from visual content published by jihadist groups.

LEGGI TUTTO

Nuove Pubblicazioni

[ACN, Online, l'Operational summary di ACN con i dati e gli indicatori della minaccia cyber in Italia, 28 settembre 2026](#)

[United Nations, Thematic Brief of the Independent International Scientific Panel on AI, September 2026](#)

[National Security Agency, Post-Quantum Cryptography Resource Hub](#)

[Poste Italiane, Poste Italiane: al via il mese europeo della Cybersecurity, 1 Ottobre 2026](#)

Eventi

[Regione Lazio, "Safe Mobility Hack: Bootcamp & Hackaton", 10-12 ottobre 2026, Spazio Attivo Roma Casilina, Via Casilina, 3/T, Roma](#)

[Innovation, "NIS2: della compliance ai finanziamenti", 21 ottobre 2026, Seminario Interdiocesano "Regina Apostolorum", Via Louis Braille, 26, Catania](#)

[MIMIT, SSSCIT e Cyber 4.0, "Post-quantum cryptography: standard, innovazioni e difesa digitale", 21 ottobre 2026, webinar online](#)

[Assolombarda, L'Architettura della Resilienza – Governance e Prodotto: interdipendenze tra NIS2 e CRA 28 ottobre Milano, Assolombarda Auditorium Giorgio Squinzi - 10.00 – 16.00](#)

[Roadshow dell'AI Hub for Sustainable Development, 3 novembre, Roma, sede Luiss di viale Pola](#)

[ENISA, European Cybersecurity Skills Conference 2026, Larnaca Cyprus, Nov 04 to 05, 2026 from 9:00 AM to 5:00 PM](#)