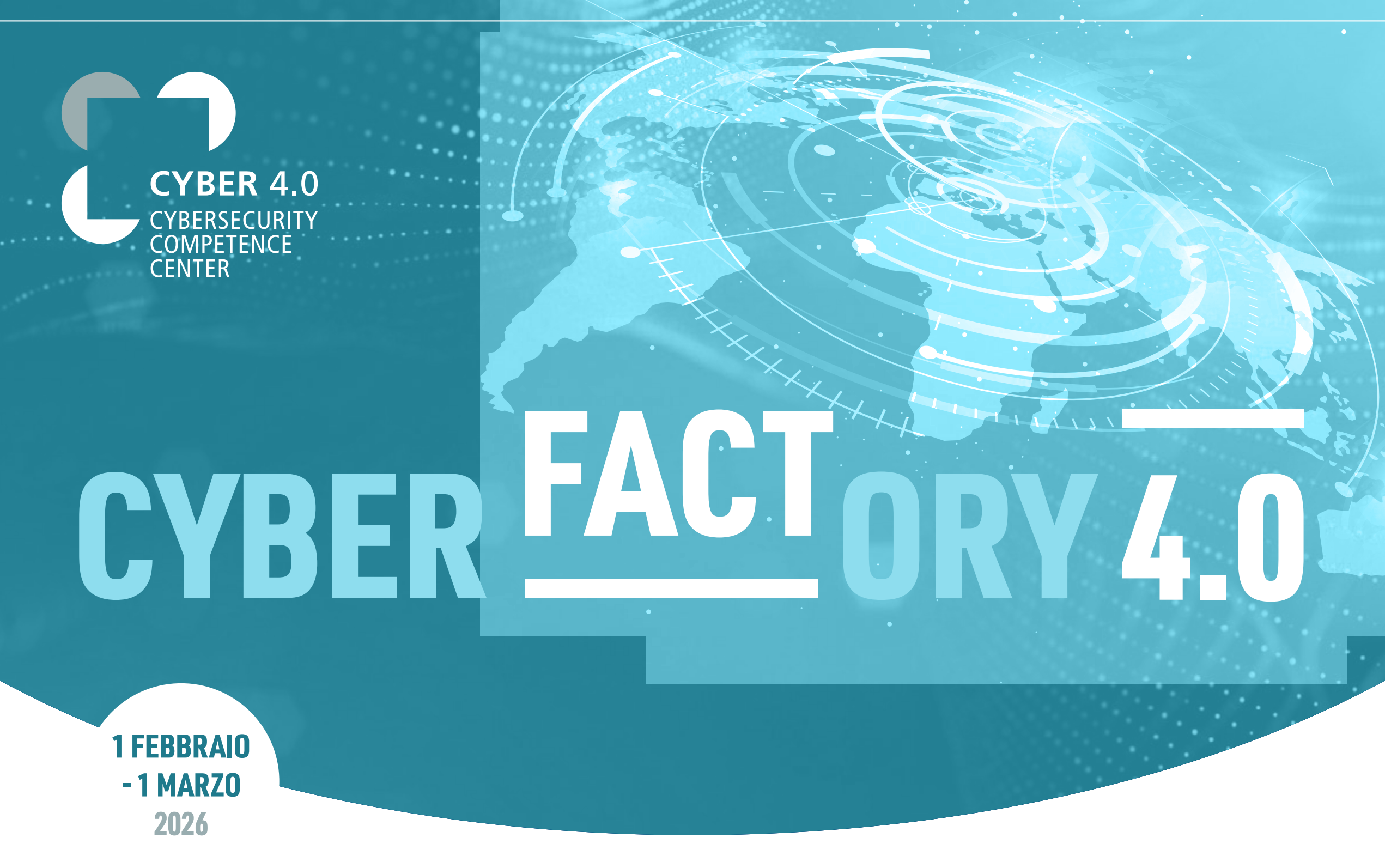


CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

CYBER FACTORY 4.0

1 FEBBRAIO
- 1 MARZO
2026

IN EVIDENZA

3 E 4 GIUGNO 2026

Save the date: Forum Cyber 4.0 2026

Cyber 4.0 annuncia il Forum 2026, appuntamento di riferimento per l'ecosistema nazionale della cybersicurezza e dell'innovazione digitale. L'evento rappresenterà un momento di confronto tra istituzioni, imprese, mondo accademico e stakeholder tecnologici sui principali trend emergenti, sulle sfide regolatorie e sulle opportunità di sviluppo del settore cyber.
Il Forum si inserisce nel percorso di consolidamento del ruolo di Cyber 4.0 come Centro di Competenza nazionale ad alta specializzazione, promuovendo sinergie pubblico-private e favorendo il trasferimento tecnologico verso il sistema produttivo.

LEGGI TUTTO

MIMIT - 10 FEBBRAIO 2026

L'AI Hub protagonista del 'Nairobi AI Forum' organizzato da Italia, Kenya e Undp: annunciati 4 protocolli d'intesa

L'AI Hub per lo Sviluppo Sostenibile è stato protagonista del Nairobi AI Forum, evento organizzato congiuntamente da Italia, Kenya e UNDP. Nel corso dell'iniziativa sono stati annunciati quattro protocolli d'intesa per rafforzare la cooperazione internazionale sull'AI, con attenzione allo sviluppo di competenze, ecosistemi innovativi e capacity building in ambito africano.
L'iniziativa si inserisce nella strategia italiana di diplomazia tecnologica e nella cornice del Piano Mattei, promuovendo un modello di sviluppo condiviso e sostenibile attraverso l'adozione responsabile delle tecnologie AI. In tale contesto, è stata inoltre annunciata la **Cybersecurity Readiness Initiative for African AI Startups**, che vedrà il coinvolgimento del Competence Center Cyber 4.0, in collaborazione con l'AI Hub, per il lancio di una call dedicata al rafforzamento della cybersicurezza delle startup africane operanti nel settore dell'intelligenza artificiale.

LEGGI TUTTO

Articoli Correlati:

1. The Standard, Kenya, Italy hand 130 African startup keys to AI revolution, February 18, 2026
2. Ministry of Enterprises and Made in Italy, Nairobi AI Forum 2026 Drives AI, Adoption and Impact, February 10, 2026
3. Industria Italiana, Cybersicurezza e AI: nasce Cyber4Africa, il programma di Cyber4.0 per formare 120 start-up africane. Con AI Hub, Mimit e Cisco, 12 Febbraio 2026
4. Cyber 4.0, AI via a Nairobi Cyber4Africa, il programma per rafforzare la cybersicurezza delle startup africane di intelligenza artificiale, 10 Febbraio 2026

CYBER 4.0

IL PARLAMENTO MAGAZINE - 6 FEBBRAIO 2026

La sicurezza dell'AI è un progetto democratico

La ridenominazione dell'AI Safety Institute britannico in AI Security Institute riporta al centro il tema della "sicurezza" dell'intelligenza artificiale e della distinzione, nel mondo anglosassone, tra **safety** e **security**: la prima riguarda la prevenzione degli effetti indesiderati che un sistema può generare su persone e organizzazioni; la seconda attiene alla protezione del sistema stesso da minacce esterne. In Italia, l'assenza di una distinzione terminologica chiara rischia di tradursi in ambiguità regolatorie e progettuali.
Garantire sistemi AI affidabili richiede un approccio integrato che agisca sulla data governance, sulla valutazione preventiva del rischio e sull'adozione di logiche di **safety e security by design**.

LEGGI TUTTO

ACN - 3 FEBBRAIO 2026

Progetto SECURE, al via il primo bando per sostenere le PMI nell'attuazione del Cyber Resilience Act

È stato lanciato il primo bando del progetto europeo SECURE, coordinato dall'Agenzia per la Cybersicurezza Nazionale. Il bando mette a disposizione **5 milioni di euro** di finanziamenti a cascata, con contributi fino a **30.000 euro per progetto** per micro, piccole e medie imprese che producono, importano o distribuiscono prodotti con elementi digitali. Le PMI potranno adeguarsi ai requisiti del **Cyber Resilience Act**, migliorare la cybersicurezza lungo l'intero ciclo di vita dei prodotti e accedere a formazione specialistica. Scadenza candidature: **29 marzo 2026**.

LEGGI TUTTO

IL PARLAMENTO MAGAZINE - 5 FEBBRAIO 2026

Cyber capacity building e governance digitale: una risposta strategica alle sfide del cyberspazio

Le strategie nazionali ed europee di cyber capacity building rispondono alla convergenza tecnologica tra intelligenza artificiale, reti 5G e quantum computing in un contesto geopolitico caratterizzato da crescenti tensioni ibride. La governance digitale resiliente richiede modelli multidominio capaci di garantire interoperabilità cross-layer e capacità di risposta coordinate.
Formazione specialistica avanzata, piattaforme di cooperazione pubblico-privato e meccanismi di interoperabilità tra settori costituiscono investimenti strategici imprescindibili per lo sviluppo scalabile delle capacità cyber a livello nazionale ed europeo.

LEGGI TUTTO

QUOTIDIANO NAZIONALE - 26 GENNAIO 2026

Cyber 4.0 in missione per la Farnesina

Cyber 4.0 rafforza il proprio ruolo istituzionale attraverso missioni internazionali che promuovono il modello italiano di competence hub nella cybersecurity. Le attività di diplomazia cyber trasferiscono know-how tecnologico avanzato e consolidano partnership strategiche con ecosistemi innovativi europei e globali.
Tale posizionamento strategico contribuisce a consolidare l'Italia come attore di riferimento nel panorama europeo della sicurezza digitale e delle competenze tecnologiche critiche.

LEGGI TUTTO

CYBER 4.0 - 2 FEBBRAIO 2026

Al via 5GSESAMO, il progetto finanziato dall'UE per reti 5G avanzate

Il progetto europeo 5GSESAMO sviluppa reti 5G avanzate con sicurezza integrata nativa nei protocolli di rete core, garantendo protezione end-to-end contro minacce avanzate su infrastrutture telecom critiche. L'iniziativa implementa standard di sicurezza armonizzati a livello europeo per la prossima generazione di connettività.
Partnership pubblico-privato multinazionali accelerano il deployment operativo di capacità di rete resilienti, conformi ai requisiti normativi europei e pronte per scenari operativi complessi.

LEGGI TUTTO

CYBER 4.0 - 30 GENNAIO 2026

Progetto CYBORG - Sistemi di comunicazione sicura a bordo veicolo basati su blockchain

CYBORG sviluppa sistemi di comunicazione sicura a bordo veicolo basati su blockchain per garantire integrità e confidenzialità dei dati in scenari IoT automotive ad alta criticità. I protocolli crittografici distribuiti mitigano rischi di manipolazione, intercettazione e attacchi denial-of-service in contesti di mobilità connessa.
I risultati del progetto trovano applicazione diretta in smart mobility, veicoli autonomi e sistemi di trasporto intelligente con requisiti di sicurezza elevati.

LEGGI TUTTO

CYBER 4.0 - 13 FEBBRAIO 2026

Progetto WISE PACK - Protezione dei prodotti farmaceutici tramite sensori wireless integrati nel packaging

WISE PACK integra sensori wireless nel packaging farmaceutico per prevenire contraffazioni e garantire tracciabilità completa lungo l'intera filiera produttiva e distributiva. Il sistema implementa autenticazione digitale avanzata e monitoraggio real-time delle condizioni ambientali di conservazione.
La tecnologia risulta scalabile per l'applicazione ad altri settori ad alta criticità della supply chain come aerospazio, energia e componentistica strategica.

LEGGI TUTTO

CYBER 4.0 - 27 FEBBRAIO 2026

CyberGuardEV - Sicurezza avanzata per le infrastrutture di ricarica dei veicoli elettrici

CyberGuardEV sviluppa soluzioni di sicurezza avanzata per le infrastrutture di ricarica dei veicoli elettrici, proteggendo stazioni di ricarica da minacce cyber remote e attacchi automatizzati. Protocolli di autenticazione multi-fattore, segmentazione di rete e monitoraggio continuo garantiscono integrità operativa.
L'iniziativa rappresenta un elemento critico per l'espansione su scala nazionale della mobilità elettrica sostenibile e l'integrazione con le reti elettriche intelligenti.

LEGGI TUTTO

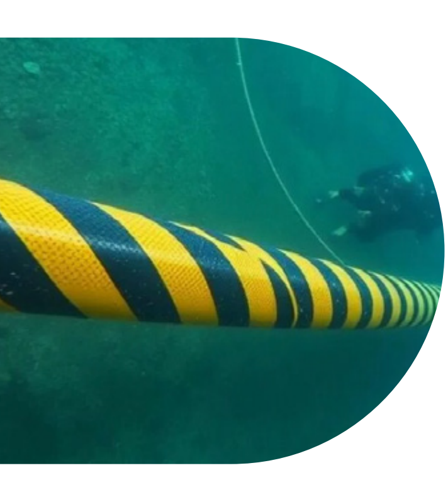
IN ITALIA

MINISTERO DELLA DIFESA - 26 FEBBRAIO 2026

Strategia della Difesa in materia di Intelligenza Artificiale

Il Ministero della Difesa presenta la strategia nazionale per l'integrazione dell'intelligenza artificiale nei sistemi di difesa, con particolare attenzione a interoperabilità operativa, resilienza cyber e sviluppo del tessuto industriale nazionale della sicurezza.
Il documento definisce priorità tecnologiche, quadro normativo e governance per l'adozione responsabile delle tecnologie AI in ambito militare, con focus su capacità decisionali aumentate e protezione delle piattaforme critiche.

LEGGI TUTTO



RED HOT CYBER - 25 FEBBRAIO 2026

I cavi sottomarini non sono un problema di telecomunicazioni: sono una questione di sicurezza europea.

I cavi sottomarini di telecomunicazione rappresentano una vulnerabilità strategica sistemica per la connettività digitale europea e la sovranità infrastrutturale del continente. La loro protezione richiede approccio integrato fisico-digitale contro minacce statali e non convenzionali.
L'analisi evidenzia la necessità urgente di una strategia europea coordinata per la cybersecurity marittima e la resilienza delle infrastrutture transoceaniche critiche.

LEGGI TUTTO

REPORT DIFESA - 18 FEBBAIO 2026

Security Summit Clusit 2026: CLUSIT RIUNISCE A MILANO L'ECOSISTEMA DELLA CYBERSECURITY

ClusIT riunisce a Milano l'intero ecosistema italiano della cybersecurity per il Security Summit 2026, evento di riferimento nazionale per l'analisi del threat landscape e le strategie di resilienza organizzativa.
L'appuntamento diventa piattaforma di coordinamento strategico tra istituzioni, imprese specializzate e centri di ricerca per la definizione delle priorità operative nazionali.

LEGGI TUTTO

POLIZIA DI STATO - 20 FEBBRAIO 2026

Roma: Polizia di Stato e Rete fondazioni Its insieme per la formazione sulla cybersicurezza

La Polizia Postale conduce un'operazione nazionale di contrasto alle reti criminali dedicate a frodi digitali e diffusione di malware, identificando e neutralizzando catene operative transnazionali. L'intervento produce risultati significativi in termini di prevenzione e repressione del cybercrime.
L'attività investigativa coordinata dimostra l'efficacia delle capacità operative nazionali contro le minacce informatiche evolute.

LEGGI TUTTO

LA STAMPA - 5 FEBBRAIO 2026

Aerei civili, lo spettro dei cyberattacchi

Una ricerca indipendente ha identificato vulnerabilità critiche nei sistemi TCAS degli aerei civili, potenzialmente sfruttabili per attacchi cyber che compromettono la sicurezza aerea sistemica. L'esposizione dei protocolli di comunicazione avionica rappresenta un rischio operativo concreto.
La scoperta richiede interventi urgenti di retrofit e hardening delle piattaforme avioniche su scala globale.

LEGGI TUTTO

NEWS INTERNAZIONALI

BANKINFOSECURITY - MARCH 1, 2026

Western cybersecurity experts brace for Iranian reprisal

Western cybersecurity professionals anticipate Iranian retaliatory cyberattacks following recent U.S. and Israeli strikes against Iranian leadership and infrastructure. Experts warn of heightened risks to critical infrastructure, financial institutions and government networks across allied nations.
Iranian-linked APT groups APT42 and APT33, associated with IRGC and MOIS, are expected to activate wiper malware campaigns, DDoS operations and targeted disruptions against U.S., Israeli and European targets. The decentralized command structure post-strikes may accelerate proxy hacktivist activities.

LEGGI TUTTO

REUTERS - FEBRUARY 25, 2026

Exclusive: US orders diplomats to fight data sovereignty initiatives

The U.S. State Department directs diplomatic personnel to actively oppose data sovereignty measures deemed restrictive to global digital commerce. The policy positions cross-border data flows as critical public goods essential to American economic and security interests.
Bilateral trade negotiations and digital economy partnerships face significant implications from this assertive posture.

LEGGI TUTTO

SEENEWS - FEBRUARY 27, 2026

Romania, Moldova, Ukraine sign MoU for cybersecurity alliance

The three nations establish regional cybersecurity cooperation framework through Memorandum of Understanding. Intelligence sharing, joint exercises and regulatory harmonization target hybrid threats in Black Sea region.
Coordinated response addresses escalating hostile activities in strategic maritime domain.

LEGGI TUTTO

INTERPOL - FEBRUARY 18, 2026

Major operation in Africa targeting online scams nets 651 arrests

Continental operation dismantles romance scam, BEC and crypto-fraud networks across multiple countries. USD 4.3 million recovered through coordinated law enforcement actions targeting transnational criminal infrastructure.
Operation demonstrates effectiveness of multinational cybercrime disruption strategies.

LEGGI TUTTO

TECHSTORY - FEBRUARY 28, 2026

Apple's iPhone and iPad Join the Ranks of NATO-Approved Hardware

Apple mobile devices achieve official NATO certification for secure allied communications. Validation enables deployment in military and intelligence operations across NATO member states.
Standardization accelerates mobile platform integration in multinational operations.

LEGGI TUTTO

The ENISA Cybersecurity Exercise Methodology

ENISA - FEBRUARY 16, 2026

Cybersecurity preparedness: DIY - build your own cybersecurity exercise

ENISA publishes practical framework with customizable templates for organizational cybersecurity exercises. Methodology supports tabletop scenarios, red/blue team operations and technical drills across maturity levels.
Implementation toolkit enhances operational readiness across EU organizations.

LEGGI TUTTO

TALLINN MECHANISM PLATFORM - FEBRUARY 13, 2026

Tallinn Mechanism provides a secure and well-coordinated framework through which support can be delivered effectively and responsibly - interview with EU CyberNet

NATO cyber assistance coordination platform operationalizes technical support, intelligence sharing and capacity building for Allies under cyber pressure. Framework implements Article 4 mutual defense consultation procedures.
Essential enabler for collective cyber defense response mechanisms.

LEGGI TUTTO

POLITICO - FEBRUARY 13, 2026

Europe needs offensive cyber power, says EU tech chief

Commission Chief Technology Officer calls for EU development of proactive cyber capabilities. Position marks strategic shift from reactive defense posture to active deterrence framework.
Debate centers on rules of engagement, command-control architecture and operational thresholds.

LEGGI TUTTO

Nuove Pubblicazioni

- Submarine Cable Security Toolbox and Cable Projects of European Interest, February 5, 2026
- European Commission, EU Cyber Census 2025, February 20, 2026
- Ministero della Difesa, IA e Difesa 2026, Febbraio 2026
- European Commission, Commission presents action plan to counter drone threats, February 11, 2026
- CERT-EU, Cyber Threat Intelligence Framework, February 13, 2026
- Science, The science and practice of proportionality in AI risk evaluations, Schellaert et al., February 13, 2026

Cyber FACTory 4.0 è una newsletter con cadenza bisettimanale.
Le notizie sono selezionate per attinenza alle attuali aree di interesse di Cyber 4.0 e non rappresentano posizioni ufficiali del Centro di Competenza.
Ricevi questo contenuto in quanto hai preso parte alle attività del Centro.
Per ulteriori informazioni, contributi, iscrizioni o rimozioni da questa lista di distribuzione, contattare: **comunicazione@cyber40.it**

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER