

CYBERFACTORY 4.0

16-30
GIUGNO
2025

IN EVIDENZA

HERMES BAY, 15 GIUGNO 2025

Cybersecurity e Resilienza Digitale: Un Dialogo con il Professor Paolo Spagnoletti di Cyber 4.0

In un'epoca in cui digitalizzazione e sicurezza sono due facce della stessa medaglia, comprendere il ruolo dei centri di competenza nazionali e delle strategie di resilienza è fondamentale per leggere il futuro del Paese. Per questo motivo, è stato intervistato il **Professor Paolo Spagnoletti**. Oltre a dirigere il corso di laurea in Economia e Management e numerosi programmi executive su innovazione digitale e governance, Paolo Spagnoletti è presidente di **Cyber 4.0**, il Competence Center nazionale per la cybersecurity.



[LEGGI TUTTO](#)

FORTUNE, 1 LUGLIO 2025

Difendere l'Umano contro il 'taylorismo digitale' nell'era dell'AI

L'AI accelera la logica della standardizzazione, ripresentando il problema di integrare l'efficienza con il rispetto del lavoro umano. Alle soglie della quinta rivoluzione industriale, un'epoca che promette di valorizzare l'integrazione tra persone e tecnologie intelligenti, riemerge una sfida antica. Si ripresenta, con nuova urgenza, un dilemma che ha segnato gli inizi del Novecento: come bilanciare la ricerca dell'efficienza con il rispetto del lavoro umano, un nodo cruciale già affrontato ai tempi del taylorismo.



[LEGGI TUTTO](#)

MITT, 16 GIUGNO 2025

Presentato a Roma l'AI Hub: Italia e UNDP insieme per il futuro dell'Africa

È stato presentato presso la sede dell'Associazione della Stampa Estera a Roma l'AI Hub for Sustainable Development. La piattaforma, che è stata inaugurata il 20 giugno a Roma, è promossa, nell'ambito della Presidenza Italiana del G7, dal Mimit e dal Programma delle Nazioni Unite per lo Sviluppo (UNDP), in collaborazione con i partner africani coinvolti nel Piano Mattei e riflette gli obiettivi della strategia della Commissione Europea Global Gateway e di quella dell'Unione Africana sull'Intelligenza Artificiale.



[LEGGI TUTTO](#)

Articoli Correlati:

[UNDP, The G7 endorsed AI Hub for Sustainable Development officially opens in Rome, announcing trailblazing collaborations to advance Africa's economic progress, June 17, 2025](#)

CYBER 4.0

CONFARTIGIANATO, 20 GIUGNO 2025

La sicurezza informatica è investimento strategico per le PMPI

La sicurezza informatica non va considerato un costo per le imprese, ma un'opportunità, un investimento per proteggere il patrimonio prezioso dei dati aziendali ed aumentare la competitività sul mercato. Non c'è tempo da perdere: tutte le imprese, anche quelle di piccola dimensione, sono a rischio di attacchi informatici e devono adottare strumenti e sistemi efficaci per proteggersi, adeguandosi alle normative sempre più stringenti in tema di cybersecurity. Ma le norme, per essere efficaci, devono essere applicabili: È il messaggio lanciato da Fabrizio Peresson, Presidente di Confartigianato ICT, nel corso dell'evento "La cybersecurity a misura di Pmipi" che il 19 e il 20 giugno Confartigianato ha dedicato al tema della sicurezza informatica con la partecipazione di rappresentanti delle istituzioni nazionali ed europee, degli enti di normazione, di esperti ed esponenti di grandi aziende.

[LEGGI TUTTO](#)

CYBER 4.0, 19 GIUGNO 2025

Cyber 4.0 collabora alla challenge TIM per digitalizzare le infrastrutture del Paese

Una nuova sfida volta a integrare tecnologie avanzate come l'AI e l'IoT per monitorare, analizzare e rendere ancora più sicure le reti energetiche, idriche e stradali. L'iniziativa è realizzata in collaborazione con Arduino, Cyber 4.0, eFM, EIT Digital, Intesa Sanpaolo Innovation Center, Osservatori 5G & Digital Connected Industry e Internet of Things del Politecnico di Milano, SOCTEC Italia e il supporto di Alaiam.

[LEGGI TUTTO](#)

Articoli Correlati:

[Il Tempo, AI via il concorso per modernizzare le infrastrutture del Paese, 20 Giugno 2025](#)

REALTÀ INDUSTRIALE, 20 GIUGNO 2025

Il Progetto Confin Hub: Digitalizzazione e Cybersecurity per le Imprese Friulane

Confindustria Udine annuncia l'avvio operativo del Progetto Confin Hub (Confindustria Innovation HUB), una delle più rilevanti iniziative italiane nel campo della digitalizzazione d'impresa, promossa a livello nazionale da Confindustria e finanziata attraverso le risorse del PNRR. Il Cyber Assessment ha l'obiettivo di accrescere la consapevolezza delle aziende sul tema della sicurezza informatica, fornendo una fotografia concreta e dettagliata del livello di maturità in ambito cyber, secondo standard di riferimento nazionali e internazionali quali il Framework Nazionale per la Cybersecurity e la Data Protection (FNCS) e la norma ISO/IEC 27001. Lo strumento è stato realizzato in collaborazione con i Competence Center Cyber 4.0 e Start 4.0, e consente di identificare il livello di esposizione ai rischi informatici, proponendo successivamente le azioni correttive. In accordo con l'azienda, e sempre nell'ambito del servizio, è inoltre possibile programmare, nella fase di restituzione del report, un'attività formativa di base rivolta ai dipendenti aziendali sul tema della cybersecurity.

[LEGGI TUTTO](#)

IL MESSAGGERO, 23 GIUGNO 2025

Dall'analisi dei dati ai flussi, imprese del Lazio e politiche dell'IA

Le imprese della regione Lazio sviluppano, più di altre, le politiche dell'intelligenza artificiale. Lo dicono i numeri: il 9,4% di loro usa l'IA per almeno una delle sette tecnologie, il 7,7% le applica per almeno due, il 3,6% le sviluppa per tre su sette. Quest'ultima è una percentuale che si attesta al 3,7%. A dirlo è uno studio realizzato dall'Istat e presentato nel corso della recente assemblea annuale di Federmanager che si è tenuta a Roma. All'evento ha partecipato anche il Presidente di Cyber 4.0, Paolo Spagnoletti.

[LEGGI TUTTO](#)

IN ITALIA

CYBERSECURITY 360, 20 GIUGNO 2025

16 miliardi di password esposte: no, non è il più grande data breach della storia. Ecco perché

La presunta "madre di tutte le violazioni" con 16 miliardi di credenziali non è un nuovo data breach, ma una raccolta di password già compromesse da infostealer e precedenti violazioni. Analisi tecnica del fenomeno e consigli per proteggere i propri account.

[LEGGI TUTTO](#)

TECH EU, JUNE 19, 2025

Italy's tech ecosystem: Innovation, growth, and emerging opportunities

The Italian tech ecosystem in 2024 showed strong performance, with companies raising over €1.3 billion, despite a slight decrease from €1.4 billion in 2023. This drop, however, reflects the overall stability of the ecosystem, as evidenced by the impressive €504 million raised in the Q1 2025 alone.

[LEGGI TUTTO](#)

AGENZIA PER LA CYBERSICUREZZA NAZIONALE, 25 GIUGNO 2025

Cybersecurity nell'UE: ENISA dà un voto di 62,65 su 100 nel primo Cybersecurity Index

L'Agenzia dell'Unione europea per la cybersecurity (ENISA) ha pubblicato il primo Cybersecurity Index, assegnando all'UE un punteggio medio di 62,65 su 100. L'indice valuta la maturità e la resilienza dei singoli Paesi in ambito cyber, evidenziando progressi significativi ma anche la necessità di rafforzare la cooperazione e le capacità nazionali per affrontare le minacce informatiche in modo coordinato.

[LEGGI TUTTO](#)

AGENZIA PER LA CYBERSICUREZZA NAZIONALE, 27 GIUGNO 2025

Napoli, inaugurato Megaride, il nuovo supercalcolatore dedicato alla cybersicurezza e infrastruttura per ricerca e innovazione

Il 27 giugno è stato inaugurato nel polo tecnologico della Federico II di Napoli il supercomputer **Megaride**, frutto della collaborazione tra ACN, MUR, ICSC e Cineca. Dotato di 28.000 CPU e 340 GPU, in sinergia con "Leonardo", mira a potenziare la ricerca scientifica, l'IA e la cybersecurity nazionale ed europea. Grazie a un finanziamento di circa 50 milioni, l'infrastruttura supporta HyperSOC – sistema ACN per il monitoraggio delle minacce.

[LEGGI TUTTO](#)

NEWS INTERNAZIONALI

EUROPEAN COMMISSION, JUNE 25, 2025

EU Space Act

The EU Space Act is a legislative initiative by the European Commission that introduces a harmonised framework for space activities across the Union. The proposal, launched on 25 June 2025, aims to ensure safety, resilience, and environmental sustainability, while boosting the competitiveness of the EU space sector.

[LEGGI TUTTO](#)

EUROPEAN COUNCIL, JUNE 6, 2025

EU adopts blueprint to better manage European cyber crises and incidents

The EU cyber blueprint is an **important guideline for member states to enhance their preparedness, detection capabilities and response to cyber security incidents**, while building on the foundations laid by the 2017 cybersecurity blueprint and taking on board important recently adopted legislation such as the NIS2 directive and the cyber solidarity act.

[LEGGI TUTTO](#)

ENISA, JUNE 26, 2025

The EU Agency for Cybersecurity (ENISA) publishes a technical guideline for the security measures of the NIS2 Implementing Regulation to assist digital infrastructures and managed service providers

The NIS2 Directive sets out requirements for cybersecurity risk management measures in 18 critical sectors, such as digital infrastructures, energy, transport or health, which have to be transposed into national law. For the NIS2 Digital Infrastructure and the ICT service management sectors these cybersecurity requirements are further elaborated at EU level, by the Commission Implementing regulation 2024/2690 of 17 October 2024. ENISA now publishes a technical guidance to support companies in these sectors with the implementation of this regulation.

[LEGGI TUTTO](#)

Articoli Correlati:

[ENISA, Cybersecurity Roles and skills for NIS2 Essential and Important Entities, June 2025](#)

DIGWATCH, JUNE 18, 2025

Breaking down the OEWG's legacy: Hits, misses, and unfinished business

The open-ended working groups (OEWGs) are a type of format present in the UN that is typically considered the most open, as the name suggests. It means that all UN member and observer states, intergovernmental organisations, and non-governmental organisations with the UN Economic and Social Council (ECOSOC) consultative status may attend public meetings of the working group. Yet, decisions are made by the UN member states. There are various OEWGs at the UN. Here, we are addressing the one dealing with cybersecurity.

[LEGGI TUTTO](#)

EUROPEAN COMMISSION, JUNE 23, 2025

EU reinforces its cybersecurity with post-quantum cryptography

The EU Member States, supported by the Commission, issued a roadmap and timeline to start using a more complex form of cybersecurity, the so-called post-quantum cryptography. Designed with complex algorithms, this is a key milestone to deflect advanced cyber threats.

[LEGGI TUTTO](#)

WORLD ECONOMIC FORUM, JUNE 18, 2025

AI agents: the new frontier of cybercrime business must confront

The concept of Advanced Persistent Threats (APTs) has been recognized since as early as 2011 as a threat model in cybersecurity. APTs refer to highly skilled and well-resourced adversaries who infiltrate corporate systems with stealth and persistence, often motivated by strategic objectives like intellectual property theft, financial gain or sabotage. These attacks typically unfold over months or years, adapting to defenses and evading detection.

[LEGGI TUTTO](#)

EUROPOL, JUNE 16 2025

Europe-wide takedown hits longest-standing dark web drug market

Between 11 and 13 June, a series of coordinated actions took place across Germany, the Netherlands, Romania, Spain, Sweden, targeting the platform's administrators, moderators, key vendors, and technical infrastructure. Around 300 officers were deployed to carry out enforcement actions and secure critical evidence. Archtyd Market operated as a drug marketplace for over five years, amassing more than 600 000 users worldwide with a total transaction volume of at least EUR 250 million. With over 17 000 listings, it is one of the few darknet markets that allowed the sale of fentanyl and other highly potent synthetic opioids, contributing to the growing threat posed by these substances in Europe and beyond.

[LEGGI TUTTO](#)

CYBERSECURITY 360, 20 GIUGNO 2025

Israele-Iran: cyber conflitto e Guerra 4.0. Altro che consapevolezza: è il tempo del fare

Israele ha recentemente sferrato un attacco informatico alla Bank Sepah, una delle più antiche istituzioni finanziarie iraniane, storicamente legata ai Pasdaran. Non si tratta di un bersaglio simbolico, ma di una struttura strategica: colpirla significa interferire direttamente con l'apparato militare, economico e politico dell'Iran. L'attacco, avvenuto con modalità non ancora del tutto pubbliche, ha avuto un impatto serio: interruzione dei servizi bancari, caos interno, ed esposizione di una vulnerabilità sistemica in un'infrastruttura considerata critica. Inutile dire che, dietro l'operazione, ci sia molto più di un semplice exploit: c'è un messaggio strategico, forte e chiaro.

[LEGGI TUTTO](#)

CYBERSECURITY ITALIA, 1 LUGLIO 2025

L'Europa e il Sud-Est asiatico cercano accordi per proteggere i cavi sottomarini dai sabotaggi

La rete mondiale di cavi sottomarini si estende per circa 1,4 milioni di chilometri e trasporta oltre il 95% del traffico internet intercontinentale. Nonostante la sua importanza, rimane esposta a danni accidentali – come quelli causati dalle ancore delle navi – e ad azioni intenzionali. I recenti episodi verificatisi nel Mar Baltico e nel Mar Rosso hanno dimostrato la vulnerabilità di questa infrastruttura, spingendo i governi ad avviare nuove iniziative di cooperazione internazionale per incrementarne la protezione.

[LEGGI TUTTO](#)

Nuove Pubblicazioni

- [ENISA, Consolidated Annual Activity Report 2024, June 30, 2025](#)
- [ENISA, NIS2 Technical Implementation Guidance, June 26, 2025](#)
- [Europol, Major developments and trends on terrorism in Europe in 2024, June 26, 2025](#)
- [Europol, Understanding and mitigating bias to harness AI responsibly, June 27, 2025](#)
- [Interpol, African Cyberthreat Assessment, June 23, 2025](#)
- [Cybersecurity 360, Attacchi ransomware 2025, in Italia sempre più aziende pagano i riscatti: le cifre in gioco, 25 Giugno 2025](#)
- [Bitdefender, 2025 Cybersecurity Assessment Report, June 2025](#)
- [Thales, 2025 Data Threat Report, May 27, 2025](#)
- [Sophos, the state of ransomware 2025, June 24, 2025](#)

Prossimi Eventi

- [Teleconsys Secure Innovation, Secure Innovation Summit 2025, 10 luglio 2025, dalle ore 15.30, Oligiata Golf Club, Roma](#)
- [Osservatorio su Innovazione e Competenze delle Filiere Tecnologiche e Piccola Industria Erosinone, Focus Group Defence Economy, 17 luglio 2025, dalle ore 16.30, Sede Luiss, Guido Carli, Viale Romania 32, Roma](#)

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

