

Newsletter N. 23  
1-15 Aprile 2023



## Cybersecurity Skills: L'UE muove con decisione i suoi passi

Leonardo Querzoni, Presidente Cyber 4.0 - 20 Aprile 2023

Si parla spesso della necessità di sviluppare un'azione concertata tra mondo accademico e mondo aziendale, per creare un ponte tra studio e lavoro. Nel mondo della cybersecurity questo è tanto più necessario, vista la carenza sistematica di profili e competenze a fronte di una domanda sempre crescente. È questo un contesto su cui si sta muovendo con decisione anche l'Unione Europea, come dimostra la recente istituzione della European Cyber Skills Academy e come dimostrano le molteplici iniziative condotte da ENISA, tra cui cito lo European Cybersecurity Skills Framework, la cui diffusione da questo mese vede Cyber 4.0 impegnato in prima linea, su mandato della stessa Agenzia EU.

FACT.ZERO

## IN EVIDENZA



### Altro che AI, la cybersecurity ha bisogno di giovani. Il premio di Leonardo e Cyber 4.0

Fortune - 18 Aprile 23

Da una parte il cyber crime è diventato, economicamente, una potenza globale. Dall'altra, mancano milioni di persone per contrastarla: se esiste un mondo dove la frase 'il futuro è in mano ai giovani' è priva di retorica, probabilmente è quello della cybersicurezza, affamato di ragazzi da contrapporre a gruppi di criminali informatici sempre più attivi e sempre più efficaci. Settantadue di quei ragazzi, da una rosa iniziale di 500, sono stati riuniti a Roma per i premi finali del Cyber X Mind4future Award organizzato da Leonardo e Cyber 4.0, centro di competenza nazionale sulla cybersecurity promosso dal Ministero delle Imprese e del Made in Italy. Sono stati 10 i premiati, i più bravi in mesi di gare ed esercitazioni di cybersicurezza: partito a dicembre 2022, il percorso ha visto la partecipazione di studenti dalle 8 università socie del Centro Cyber 4.0 (Sapienza, Tor Vergata, Roma Tre, LUISS Guido Carli, Campus Biomedico, Toscana, Cassino e Lazio Meridionale, L'Aquila).

[Vedi altro](#)

Articoli Correlati:

[Adnkronos, Cybersecurity, Leonardo e Cyber 4.0 premiano i vincitori di Cyber X Mind4Future](#)

[Ansa, Frattasi, cybersecurity coinvolge ogni attività umana](#)



### Cybersecurity, Frattasi: "In Italia troppi attacchi sommersi"

Corriere Comunicazioni - 18 Aprile, 23

Tra gli attacchi informatici contro imprese e Pa in Italia c'è una rilevante parte sommersa: alcuni incidenti cyber non sono denunciati, altri restano addirittura invisibili. Lo ha dichiarato Bruno Frattasi, direttore dell'Agenzia per la cybersicurezza nazionale (Acn), intervenuto a Roma in apertura della cerimonia di premiazione dei vincitori di Cyber X Mind4Future, il programma di formazione evoluta ed esperienziale sui temi della sicurezza cibernetica ideato da Leonardo e il centro di competenze Cyber4.0.

[Vedi altro](#)



## Cyber 4.0 nell'Ad Hoc Working Group di ENISA sullo European Cybersecurity Skills Framework

*Cyber 4.0 – 20 Aprile 23*

Il nostro Centro di Competenza viene nominato permanent observer dall'Agenzia Europea di Cybersicurezza. L'ECSF, pubblicato nella sua forma definitiva a Settembre 2022, è lo strumento di riferimento a livello comunitario per la definizione dei profili e delle competenze legate alle professioni di cybersecurity. Il Framework individua 12 profili, definendone ruoli, responsabilità e competenze, oltre che interrelazioni e sinergie. L'Ad Hoc Working Group appena costituito si occuperà di facilitare l'implementazione dell'ECSF, monitorarne l'utilizzo, supportarne la promozione con le rispettive controparti, e fornire assistenza nelle sue possibili revisioni.

[Vedi altro](#)

Articoli Correlati:

[Enisa Ad-Hoc Working Group on the European Cybersecurity Skills Framework \(2023-2025\)](#)



## Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience – 'The Cybersecurity Skills Academy'

*European Commission - April 18, 23*

In 2022, the shortage of cybersecurity professionals in the European Union ranged between 260,000 and 500,000, while the EU's cybersecurity workforce needs were estimated at 883,000 professionals, suggesting a misalignment between the competences available and those required by the labour market. The cybersecurity workforce further suffers from the misconception associated with its technical image, and continues to fail at attracting women, who amount to 20% of cybersecurity graduates and to 19% of information and communications technology (ICT) specialists. [...] To overcome the challenge of addressing cybersecurity skills and closing the labour market gap, the Commission is putting forward a Cybersecurity Skills Academy, as announced by the President of the European Commission in her 2022 State of the Union Letter of Intent, and in the context of the European Year of Skills. The Cybersecurity Skills Academy (in short, 'the Academy') aims at creating a single point of entry and synergies for cybersecurity education and training offers as well as for funding opportunities and specific actions for supporting the development of cybersecurity skills. It will scale up stakeholders' initiatives to reach a critical mass that will make a difference on the labour market, including for defence. Those activities would align along common goals and key performance indicators to seek greater impact.

[Vedi altro](#)



## L'Italia affila le armi contro gli hacker: gestiti oltre 400 attacchi a reti critiche

*Corriere Comunicazioni – 12 Aprile 23*

Si intensifica in Italia la lotta alle attività di cybercrime. Nel corso del 2022 la Sala Operativa del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (Cnaipic) ha gestito, a livello nazionale, 405 attacchi a sistemi informatici di strutture di rilievo strategico, occupandosi inoltre di 77 richieste di cooperazione nel circuito High Tech Crime Emergency e avviando 110 indagini con 51 persone indagate. È quanto emerge dal rapporto stilato in occasione del 17lesimo anniversario della fondazione della Polizia di Stato.

[Vedi altro](#)



## EU proposes \$1.2 billion plan to counter growing cybersecurity threats

Reuters – April 18, 23

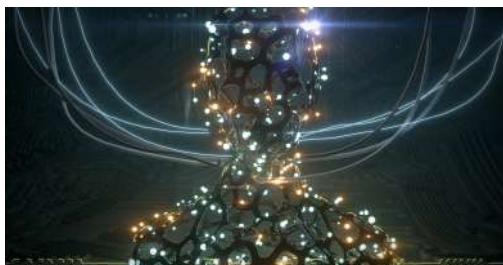
The European Commission on Tuesday announced a 1.1-billion-euro (\$1.2 billion) plan to counter growing cybersecurity threats, underscoring mounting concerns about a series of high-profile hacking incidents. The growing use of cyber warfare in the military conflict between Russia and Ukraine has also triggered alarm. "The EU Cyber Solidarity Act will strengthen solidarity at Union level to better detect, prepare for and respond to significant or large-scale cybersecurity incidents, by creating a European Cybersecurity Shield and a comprehensive Cyber Emergency Mechanism," the EU executive said in a statement. The Shield will be made up of national and cross-border Security Operations Centres which will use state-of-the-art technology, such as artificial intelligence and advanced data analytics, to detect cross-border cyber threats and incidents. [...] The Cyber Solidarity Act will require agreement from EU countries and European Parliament before it can become law.

[Vedi altro](#)

Articoli Correlati:

[European Commission, Cyber: towards stronger EU capabilities for effective operational cooperation, solidarity and resilience](#)

[Ansa, L'Ue lancia il cyber-scudo per la sicurezza informatica](#)



## L'EDPB crea la task force europea su ChatGPT, dopo lo stop italiano: cosa significa

Cybersecurity 360 – 14 Aprile 23

L'EDPB istituisce la task force europea su ChatGPT. Le autorità garanti della privacy dell'Unione europea uniscono le forze per scambiarsi dati sul monitoraggio di OpenAI, dopo il blocco di ChatGPT in seguito all'intervento dell'Authority italiana. Intanto l'organo che raccoglie i Garanti privacy dell'Unione risolve una disputa con Meta in merito all'Art. 65 del GDPR sul trasferimento dei dati da parte della società di Facebook verso gli Stati Uniti.

[Vedi altro](#)



## Cybersecurity, Thales: errore umano causa principale violazioni su cloud (55%)

Industria Italiana – 18 Aprile 23

Aumento degli attacchi ransomware ed errore umano come causa principale delle violazioni sul cloud: sono queste le due principali evidenze emerse dal Thales Data Threat Report, il Rapporto Annuale sulle Minacce Informatiche condotto da Thales su circa 3000 professionisti IT provenienti da organizzazioni pubbliche e private di 18 diversi Paesi, tra cui l'Italia.

[Vedi altro](#)



## How 'Operation Cookie Monster' took down a major dark web marketplace

World Economic Forum – April 14, 23

Genesis Market, one the world's largest illicit online marketplaces, was shut down this month in a police operation that involved over a dozen international law enforcement agencies. Dubbed "Operation Cookie Monster," the crackdown resulted in the seizure of hundreds of thousands of stolen identities and online access credentials that were for sale on the platform. The operation, which also led to over 100 arrests worldwide, was headed by the US FBI and the Dutch National Police and served a major blow to global cybercrime efforts.

[Vedi altro](#)



## The Russia-linked APT29 is behind recent attacks targeting NATO and EU

Security Affairs – April 13, 23

Poland's Military Counterintelligence Service and its Computer Emergency Response Team linked a recent string of attacks targeting NATO and European Union countries to the Russia-linked APT29 group (aka SVR group, Cozy Bear, Nobelium, and The Dukes). APT29 along with APT28 cyber espionage group was involved in the Democratic National Committee hack and the wave of attacks aimed at the 2016 US Presidential Elections.

[Vedi altro](#)

## NUOVE PUBBLICAZIONI

[Cisco, Cisco Cybersecurity Readiness Index 2023: in Italia solo il 7% delle aziende è in grado di difendersi dalle minacce informatiche](#)

[Centre for Strategic and Intelligence Studies \(CSIS\), Space Threat Assessment](#)

[Cybersecurity and Infrastructure Security Agency \(CISA\), Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default](#)

[Gartner, Top Strategic Cybersecurity Trends for 2023](#)

[Sloan Management Review, From ChatGPT to HackGPT: Meeting the Cybersecurity Threat of Generative AI](#)

## PROSSIMI EVENTI

[Cyber 4.0 – Ict Security Magazine – SOCINT, Cybercrime Conference, 11-12 Maggio, Roma](#)

[Cyber 4.0, Roadshow Cyber 4.0 Piemonte, 18 Maggio 2023, Torino](#)

[Cyber 4.0 – Forum Cyber 4.0, 6-7 Giugno, Roma, Aula Magna La Sapienza Università di 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](mailto:comunicazione@cyber40.it)

