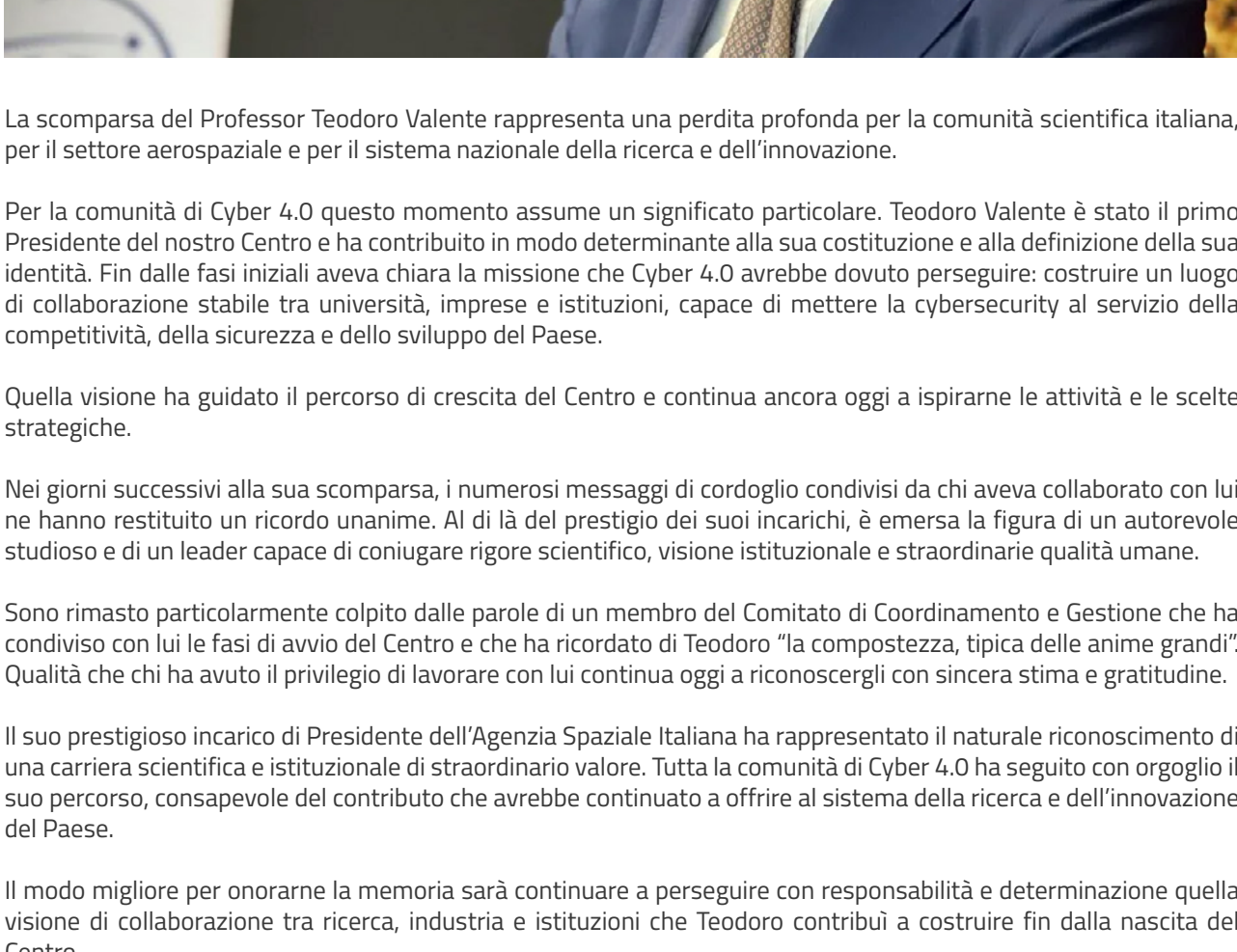




# CYBERFACTORY 4.0

1-31  
LUGLIO  
2026

## In memoria del Professor Teodoro Valente



La scomparsa del Professor Teodoro Valente rappresenta una perdita profonda per la comunità scientifica italiana, per il settore aerospaziale e per il sistema nazionale della ricerca e dell'innovazione.

Per la comunità di Cyber 4.0 questo momento assume un significato particolare. Teodoro Valente è stato il primo Presidente del nostro Centro e ha contribuito in modo determinante alla sua costituzione e alla definizione della sua identità. Fin dalle fasi iniziali aveva chiara la missione che Cyber 4.0 avrebbe dovuto perseguire: costruire un luogo di collaborazione stabile tra università, imprese e istituzioni, capace di mettere la cybersecurity al servizio della competitività, della sicurezza e dello sviluppo del Paese.

Quella visione ha guidato il percorso di crescita del Centro e continua ancora oggi a ispirarne le attività e le scelte strategiche.

Nei giorni successivi alla sua scomparsa, i numerosi messaggi di cordoglio condivisi da chi aveva collaborato con lui ne hanno restituito un ricordo unanime. Al di là del prestigio dei suoi incarichi, è emersa la figura di un autorevole studioso e di un leader capace di coniugare rigore scientifico, visione istituzionale e straordinarie qualità umane.

Sono rimasto particolarmente colpito dalle parole di un membro del Comitato di Coordinamento e Gestione che ha condiviso con lui le fasi di nascita e che ha ricordato di Teodoro "la compostezza, tipica delle anime grandi". Qualità che chi ha avuto il privilegio di lavorare con lui continua oggi a riconoscergli con sincera stima e gratitudine.

Il suo prestigioso incarico di Presidente dell'Agenzia Spaziale Italiana ha rappresentato il naturale riconoscimento di una carriera scientifica e istituzionale di straordinario valore. Tutta la comunità di Cyber 4.0 ha seguito con orgoglio il suo percorso, consapevole del contributo che avrebbe continuato a offrire al sistema della ricerca e dell'innovazione del Paese.

Il modo migliore per onorarne la memoria sarà continuare a perseguire con responsabilità e determinazione quella visione di collaborazione tra ricerca, industria e istituzioni che Teodoro contribuì a costruire fin dalla nascita del Centro.

A nome dei Soci, degli Organi, del Direttore e di tutto il personale di Cyber 4.0 desidero esprimere cordoglio e vicinanza alla sua famiglia, ai suoi cari e a tutti coloro che hanno condiviso con lui il percorso accademico, scientifico e istituzionale.

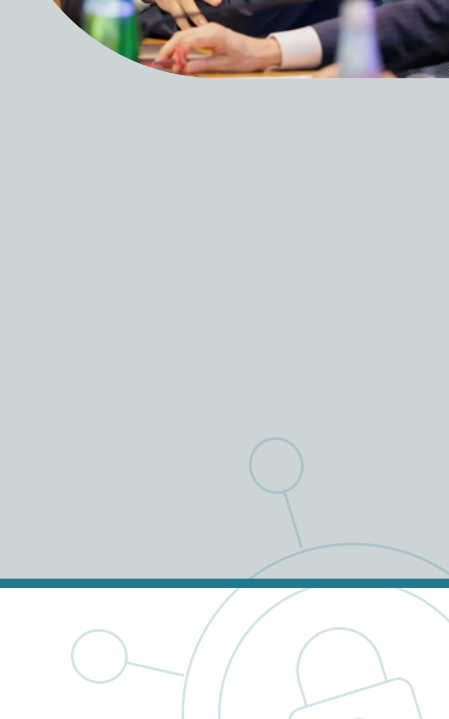
Il Presidente di Cyber 4.0  
Paolo Spagnoletti

## IN EVIDENZA

INNOVATION POST, 28 LUGLIO 2026

### Dalle regole all'azione: la nuova fase della cooperazione globale sulla cybersicurezza

A New York le Nazioni Unite hanno avviato il primo incontro del Global Mechanism on ICTs, il nuovo organismo permanente per la sicurezza digitale internazionale. Dal contrasto al ransomware e all'uso malevolo dell'AI fino alla protezione delle infrastrutture critiche, la sfida passa ora all'adozione di tutele concrete.



LEGGI TUTTO

#### Articoli Correlati:

- Delegation of the European Union to the United Nations in New York, EU Statement – UN Global Mechanism on ICTs in international security: First Substantive Session Key EU messages for Agenda item on Capacity building, July 23, 2026
- Eu Cyber Direct, The permanent turn of the UN Global Mechanism on ICT Security Five shifts in Cyber Diplomacy, and What They Will Require, July 30, 2026
- United Nations Office for Disarmament Affairs, Joint Multistakeholder Statement on the Objectives to the Participation of Stakeholders in plenary meetings and review conferences of the UN Global Mechanism

## CYBER 4.0



CYBER 4.0, 30 LUGLIO 2026

### Cybersecurity; quali prospettive e sfide per il futuro? Scopri cosa è emerso dal Forum Cyber 4.0 2026

Attraverso le sessioni e i contributi dei relatori sono emersi gli **orientamenti fondamentali per guidare istituzioni e imprese**, offrendo un'analisi approfondita delle priorità strategiche, delle competenze necessarie e delle sfide normative che definiranno l'ecosistema cyber nei prossimi anni. Per approfondire i contenuti emersi durante il Forum, **consulta i Key Takeaways** realizzati da Cyber 4.0, che riassumono i principali **temi affrontati, le evidenze emerse e gli spunti di riflessione** condivisi nel corso dell'evento.

LEGGI TUTTO

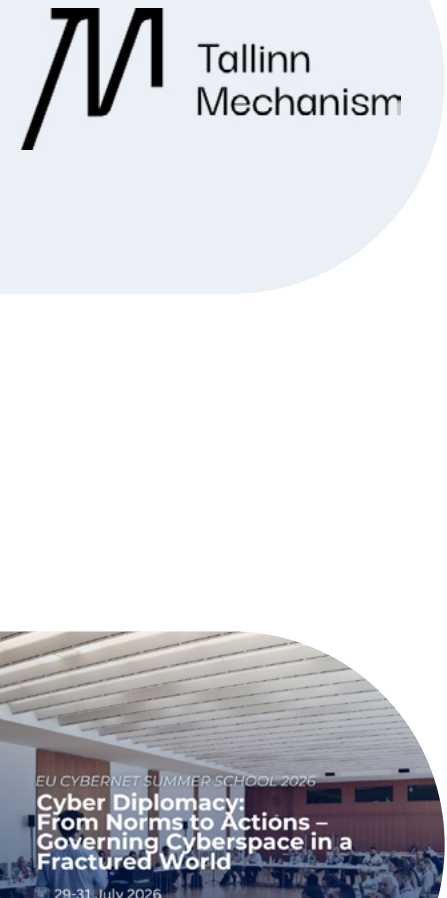


RETE 8, 2 AGOSTO 2026

### Pescara: nasce l'OT Cybersecurity LAB, il primo polo del Centro Italia

Inaugurato all'Aurum di Pescara l'OT Cybersecurity LAB, laboratorio nato dalla collaborazione tra Gruppo Infoteam e Cyber 4.0, per la protezione di apparati elettromedicali e sistemi industriali, in linea con le direttive europee NIS2 e Cyber Resilience Act.

LEGGI TUTTO



CYBER 4.0, 25 GIUGNO 2026

### AI, ricerca e formazione: come cambiano università e competenze nel nuovo scenario tecnologico?

In occasione del We Make Future 2026 di Bologna, Paolo Spagnoletti, Presidente di Cyber 4.0, è intervenuto al panel "AI, ricerca e formazione: come cambiano università e competenze nel nuovo scenario tecnologico". L'incontro ha approfondito l'impatto dell'intelligenza artificiale sul ruolo delle università, con particolare attenzione all'evoluzione dei modelli di ricerca, dei percorsi formativi e delle competenze richieste dal mercato, ponendo al centro del dibattito il contributo degli atenei alla costruzione di ecosistemi dell'innovazione sempre più integrati con imprese e istituzioni.

LEGGI TUTTO

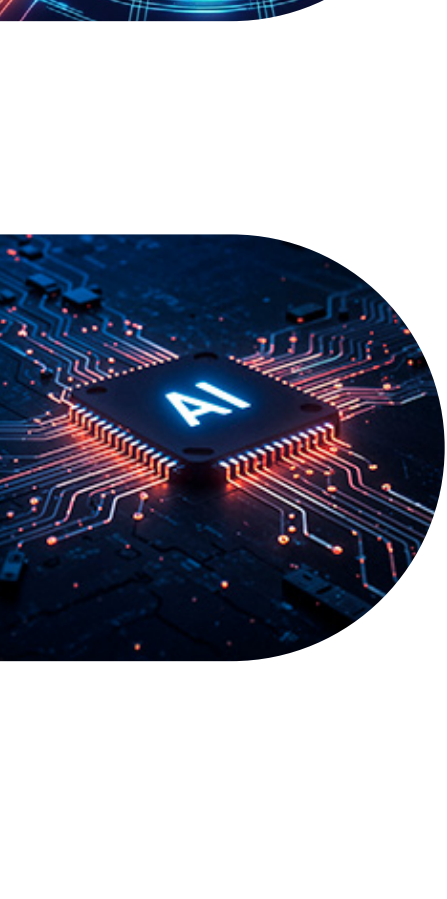


IL SOLE 24 ORE, 3 LUGLIO 2026

### La mappa dei progetti del Piano Mattei

[...]Sul versante delle infrastrutture e dell'innovazione digitale, l'AI Hub for Sustainable Development, istituito nell'ambito della Presidenza italiana del G7, è finanziato dal Ministero delle Imprese e del Made in Italy (MIMIT) con 14,9 milioni di euro su tre anni e attuato con il supporto tecnico di UNDP. Dal lancio del 20 giugno 2025, l'Hub è passato dalla fase di co-progettazione all'attuazione operativa, registrando 376 manifestazioni di interesse per il Compute & Talent e 135 candidature per l'AI Infrastructure Builder Programme. In tale quadro si inseriscono il programma Cyber4Africa, sviluppato con Cyber 4.0 e Cisco Kenya, le collaborazioni con l'Agenzia Spaziale Italiana e i 7 partenariati industriali e scientifici formalizzati nel giugno 2026 presso il Tecnopolo DAMA di Bologna.

LEGGI TUTTO



CYBER 4.0, 2 LUGLIO 2026

### L'Italia assume la leadership del Tallinn Mechanism: nuovo impulso all'impegno internazionale di Cyber 4.0

Dal 1° luglio 2026 l'Italia assume il ruolo di Leading Nation del Tallinn Mechanism, il quadro internazionale che coordina il sostegno alla resilienza cibernetica dell'Ucraina, raccogliendo il testimone dal Regno Unito. Il passaggio di leadership rafforza la proiezione internazionale dell'Italia nel settore della cybersicurezza, nel cui ecosistema rientra il Centro di competenza Cyber 4.0. Il tema è stato infatti richiamato anche nel corso della sessione dedicata all'interno del Forum Cyber 4.0, dove Niccolò Costantini del Ministero degli Affari Esteri e della Cooperazione Internazionale ha illustrato il contributo italiano all'iniziativa.

LEGGI TUTTO



CYBER 4.0, 28 LUGLIO 2026

### Dalle norme all'azione: a Firenze la EU CyberNet Summer School 2026 sulla cyber diplomacy

Nel corso degli ultimi due decenni sono stati progressivamente definiti principi e norme volontarie per orientare il comportamento responsabile degli Stati nel cyberspazio. La loro attuazione, tuttavia, resta disomogenea: per molti Paesi, tradurre gli impegni assunti in politiche nazionali, procedure e strumenti operativi richiede competenze specialistiche, coordinamento tra amministrazioni e capacità istituzionali ancora da rafforzare. È a partire da questa esigenza che, dal 29 al 31 luglio, l'European University Institute di Firenze ospiterà la EU CyberNet Summer School 2026, dedicata al tema Cyber Diplomacy: From Norms to Actions – Governing Cyberspace in a Fractured World. L'iniziativa è organizzata da EU CyberNet in collaborazione con EU Cyber Direct–EUISS, il Servizio europeo per l'azione esterna, l'European University Institute e Cyber 4.0.

LEGGI TUTTO

#### Articoli Correlati:

From Policy to Action: The EU CyberNet Summer School 2026 on Cyber Diplomacy in Florence, July 28, 2026

## IN ITALIA

ACN, 24 LUGLIO 2026

### Aggiornate le FAQ ACN sulle misure di sicurezza per la supply chain dei soggetti NIS

Per supportare i soggetti NIS nell'adozione delle misure di sicurezza a protezione della loro supply chain, la FAQ MSB.13 indica le quattro fasi del relativo processo (valutazione del rischio associato alla fornitura; identificazione dei requisiti di sicurezza; enforcement dei requisiti e loro verifica).

LEGGI TUTTO



MILANO FINANZA, 20 LUGLIO 2026

### AI, Bankitalia mette in guardia le piccole banche sui modelli come Mythos. E chiede un piano d'azione entro fine anno

La Banca d'Italia mette in guardia le piccole e medie banche sui modelli avanzati dell'AI, come Mythos di Anthropic. Gli istituti meno significativi (Lsi o Less Significant Institutions), vigilati direttamente da Via Nazionale, dovranno preparare entro il 31 dicembre «una relazione che rappresenti il livello attuale di resilienza e l'adeguatezza dei presidi esistenti, individui le principali carenze e le relative priorità di intervento nonché definisca un piano di lavoro con l'indicazione delle azioni, dei tempi e degli investimenti necessari».

LEGGI TUTTO



CYBERSECURITY ITALIA, 22 LUGLIO 2026

### Due modelli di OpenAI violano Hugging Face senza intervento umano. L'AI cyber fuori controllo?

L'attacco cyber 'in piena autonomia' contro Hugging Face crea scenari senza precedenti, con un impatto diretto sulla percezione di sicurezza informatica. Un cyberattacco senza intervento umano durante un test da parte di una "combinazione di più modelli di AI". Non è più teoria o un'ipotesi di studio ma è quanto accaduto a Hugging Face, nell'incidente che è capitato a OpenAI.

LEGGI TUTTO

## NEWS INTERNAZIONALI



CORRIERE DELLA SERA LOGIN, 1 LUGLIO 2026

### L'Onu sull'intelligenza artificiale: «Le capacità dei modelli superano la comprensione scientifica e la capacità dei governi»

Con le attuali misure di sicurezza l'Europa non riesce a stare al passo con la crescita dell'intelligenza artificiale. A mettere in guardia le istituzioni del nostro continente è l'Independent International Scientific Panel on AI, il gruppo di esperti e scienziati dell'Onu nato per colmare il divario di conoscenze sull'AI e valutare l'impatto della tecnologia sull'economia e la società. Il Panel ha pubblicato il Preliminary Report: un rapporto nel quale viene presentata la prima valutazione scientifica globale e indipendente delle opportunità, dei rischi e degli impatti dell'intelligenza artificiale. Si tratta di un lavoro preliminare, che fornisce la base di dati per informare la politica globale in vista di un successivo rapporto completo, la cui pubblicazione è prevista per il 2027.

LEGGI TUTTO

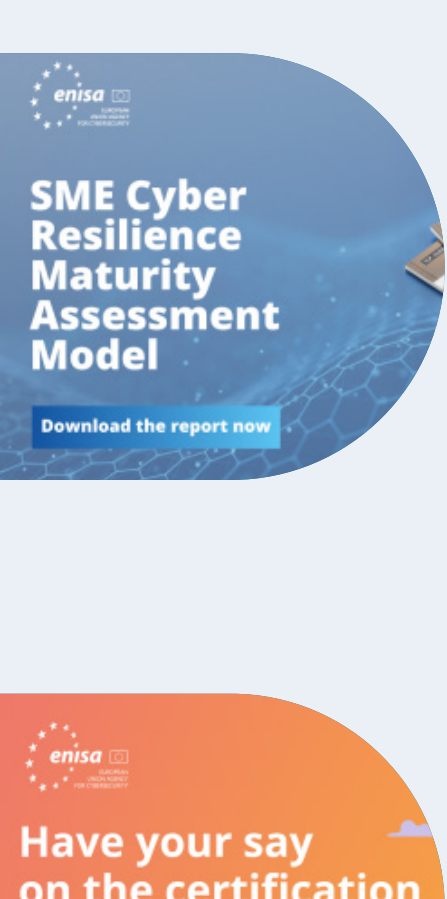


EUROPEAN COMMISSION, JULY 7, 2026

### Commission presents EU Action Plan on Cybersecurity and Artificial Intelligence

The European Commission has presented an Action Plan for a structured response to address the risks and harness the opportunities of advanced artificial intelligence (AI) models for cybersecurity. New advanced AI models are redefining cybersecurity. AI can be misused to identify vulnerabilities, automate attacks and increase the scale and speed of cyber incidents at an unprecedented speed.

LEGGI TUTTO



ENISA, JULY 7, 2026

### ENISA's view on Cybersecurity in the Frontier AI Era

This publication provides national competent authorities in Member States and EU policymakers, defenders, and service providers with an initial set of recommendations to support them in their respective roles towards developing the necessary operational capabilities to face machine-speed threats.

LEGGI TUTTO



EUROPEAN COMMISSION, JULY 27, 2026

### Commission publishes new guidance to support timely Cyber Resilience Act implementation

In a clear demonstration of its commitment to simplification and timely implementation, the Commission today published practical guidance to help manufacturers, developers, and businesses of all sizes meet their obligations under the Cyber Resilience Act.

LEGGI TUTTO

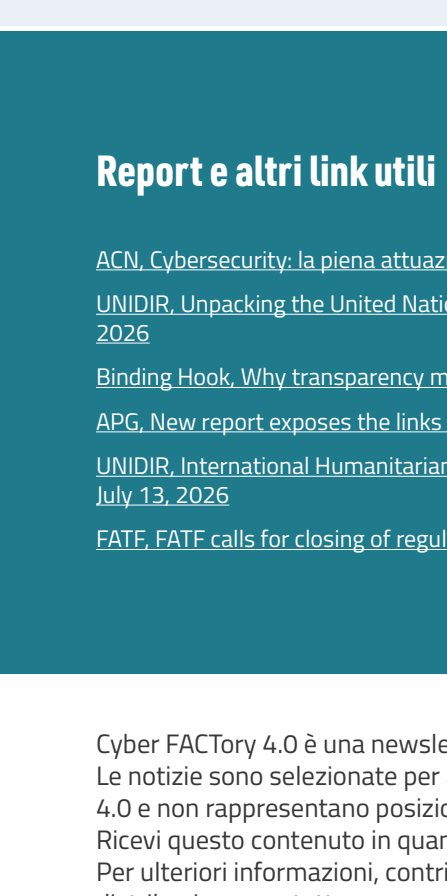


ENISA, JULY 13, 2026

### Where do SMEs stand in preparing for the Cyber Resilience Act?

The EU Agency for Cybersecurity (ENISA) publishes the Micro, Small and Medium-sized enterprises (SME) Cyber Resilience Maturity Assessment Model, a simple and practical guidance for SMEs to support them assess their current status, identify improvements and strengthen their cyber resilience practices.

LEGGI TUTTO

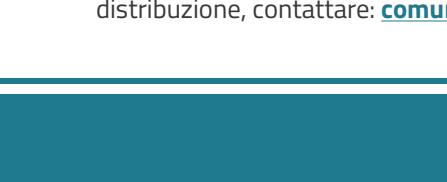


ENISA, JULY 24, 2026

### Have your say on the certification of EU Managed Security Services

ENISA is launching a public consultation on the draft candidate cybersecurity certification scheme on EU Managed Security Services (EUMSS), following its work with the dedicated Ad Hoc Working Group.

LEGGI TUTTO



ENISA, JULY 24, 2026

### AI Office publishes frontier AI expert findings on EU competitiveness, sovereignty and security

ENISA is launching a public consultation on the draft candidate cybersecurity certification scheme on EU Managed Security Services (EUMSS), following its work with the dedicated Ad Hoc Working Group.

LEGGI TUTTO



COUNCIL OF THE EUROPEAN UNION, JULY 13, 2026

### Russian cyber-attacks and destabilising activities: Council sanctions nine individuals and four entities

The Council today decided to impose restrictive measures on nine Russian individuals and four entities forming part of Russia's cyber ecosystem, responsible for and involved in carrying out, enabling and facilitating cyber-attacks against the EU, its member states and international partners.

LEGGI TUTTO



#### Articoli Correlati:

Binding Hook, The evidence paradox behind bulletproof hosting, July 27, 2026

Europa Today, Chat Control, l'Ue ha davvero aperto al controllo delle nostre conversazioni online?, 16 Luglio 2026

## Report e altri link utili

- ACN, Cybersecurity: la piena attuazione della NIS2 rafforza la capacità di rilevare gli incidenti e la resilienza del sistema Paese, 24 Luglio 2026
- UNIDIR, Unpacking the United Nations Open-Ended Working Group on ICT in the Context of International Security (2021–2025), June 24, 2026
- Binding Hook, Why transparency must be the foundation of trust in tech-driven global order, July 24, 2026
- APG, New report exposes the links between cyber scam hubs and human trafficking, July 7, 2026
- UNIDIR, International Humanitarian Law and Cyber Operations: (Consequences of) Divergent National Interpretations of "Attack" and "Data", July 13, 2026
- FATF, FATF calls for closing of regulatory gaps as virtual asset illicit finance risks become more complex, July 16, 2026