

# FORUM 2025 CYBER 4.0



## L'AGENDA DEL FORUM

4-5 GIUGNO 2025  
ROMA TRE Aula Magna Rettorato

Con il patrocinio di:



Sotto l'alto patrocinio  
del Parlamento europeo



Ministero delle Imprese  
e del Made in Italy



Finanziato  
dall'Unione europea  
NextGenerationEU

Hosted by:



Roma Tre

# 04 GIU

## SESSIONE ISTITUZIONALE

08h30 - 09h00

WELCOME E REGISTRAZIONE

09h00 - 09h40

SALUTI DI INDIRIZZO DEI LAVORI / WELCOME  
ADDRESS

### Massimiliano FIORUCCI

Magnifico Rettore, Università degli Studi Roma Tre

### Bruno FRATTASI

Direttore Generale, Agenzia per la Cybersicurezza Nazionale (ACN)

APERTURA UFFICIALE DELL'EVENTO / OFFICIAL  
OPENING

### Eva SPINA

Capo del Dipartimento per il digitale, la connettività e le nuove tecnologie,  
Ministero delle Imprese e del Made in Italy (MIMIT)

Introduce e coordina:

### Paolo SPAGNOLETTI

Presidente Cyber 4.0

<p>09h00 - 09h40</p>	<p><b>CYBER 4.0: CAPACITÀ, COMPETENZE, COOPERAZIONE, CONCRETEZZA</b></p> <p>Attività, progetti, iniziative di Cyber 4.0. Cosa è stato raggiunto, quali sono i piani di sviluppo nel prossimo futuro, costruendo sull'azione di promozione dell'innovazione e delle competenze in materia di cybersecurity fin qui realizzata.</p> <p>An overview of Cyber 4.0's activities, projects and initiatives. What has been achieved, the challenges, the opportunities and the perspective evolution. Drawing a line on the results of the Center, a public-private partnership on cybersecurity promoted by the Ministry of Enterprises and Made in Italy, with competencies and innovation in its DNA.</p> <p><b>Matteo LUCCHETTI</b> Direttore Operativo Cyber 4.0</p>
<p>10h00 - 10h15</p>	<p><b>THE EU ACTION TO SUPPORT INNOVATION AND PROMOTE INDUSTRIAL POLICIES IN THE AREA OF CYBERSECURITY</b></p> <p>Le iniziative strategiche dell'Unione Europea per promuovere l'innovazione e sviluppare politiche industriali nel campo della cybersicurezza e il ruolo dell'ECCC: i programmi europei, i meccanismi di finanziamento e i quadri normativi pensati per sostenere la ricerca, rafforzare la resilienza e stimolare la crescita di un ecosistema della cybersicurezza solido e competitivo.</p> <p>The role of the European Cybersecurity Competence Center and the Network of the NCCs as a pivot in the definition and implementation of the communitarian policies to enhance competitiveness of the cyber industry in EU, foster technological autonomy and strengthen capacities of public and private organizations.</p> <p><b>Luca TAGLIARETTI</b> Executive Director, European Cybersecurity Competence Center (ECCC)</p>

10h15 - 11h00

## IMPRESE E ISTITUZIONI A CONFRONTO: IL QUADRO NORMATIVO IN MATERIA DI CYBERSECURITY, IL CONTESTO GEOPOLITICO E LE PROSPETTIVE DI SVILUPPO

Il contesto globale, il quadro regolamentare, la risposta delle istituzioni, gli impatti sulle imprese: la cybersicurezza è centrale nel dibattito sullo sviluppo delle capacità nazionali, in un contesto segnato da rapide evoluzioni normative e tensioni geopolitiche. La sessione offre un'occasione di confronto su sfide e prospettive di sviluppo per il settore della cybersecurity.

The global context, the regulatory framework, the institutional response, and the impact on businesses: cybersecurity lies at the heart of the debate on the development of national capabilities, in a landscape marked by rapid regulatory changes and geopolitical tensions. This session provides an opportunity for dialogue on the challenges and future prospects for the cybersecurity sector.

### **Luca NICOLETTI**

Direttore Servizio programmi industriali, tecnologici di ricerca e formazione, Agenzia per la Cybersicurezza Nazionale (ACN)

### **Eva SPINA**

Capo del Dipartimento per il digitale, la connettività e le nuove tecnologie, Ministero delle Imprese e del Made in Italy (MIMIT)

### **Michele VECCHIONE**

Head Cyber Security Offering, TIM Enterprise

Moderatore:

### **Leonardo QUERZONI**

Prorettore alle Tecnologie Digitali e alla Cybersecurity, Sapienza Università di Roma

11h00 - 11h30

COFFEE BREAK E VISITA STAND

11h30 - 11h45

## TRANSIZIONE DIGITALE, QUALI POLITICHE PER LE IMPRESE ITALIANE. IL RUOLO DEI CENTRI DI COMPETENZA NAZIONALI

Politiche attivate a livello nazionale per accompagnare le imprese nel percorso di innovazione digitale, con un focus sul ruolo chiave dei Centri di Competenza. Esperienze, strumenti e opportunità di supporto nel coordinamento tra istituzioni, imprese e attori dell'ecosistema dell'innovazione.

National policies launched to support companies in their digital innovation journey, with a focus on the key role of Competence Centers. Experiences, tools, and support opportunities aimed at fostering coordination between institutions, businesses, and innovation ecosystem stakeholders.

### **Marco CALABRÒ**

Capo del Dipartimento per le politiche per le imprese, Ministero delle Imprese e del Made in Italy

11h45 - 11h55

## LA STRATEGIA NAZIONALE DI CYBERSICUREZZA: RISULTATI E SFIDE NEI NUOVI EQUILIBRI INTERNAZIONALI

La Strategia Nazionale di Cybersicurezza 2022-2026 a tre anni dal lancio: il modello di governance, gli obiettivi raggiunti e le sfide ancora aperte. Un'occasione per riflettere sul percorso compiuto e sulle priorità per il quadro strategico post-2026 alla luce dei nuovi orientamenti UE e del contesto geopolitico in evoluzione.

The National Cybersecurity Strategy three years after its launch: governance model, achieved objectives, and future challenges. An opportunity to reflect on the progress made and to identify priorities for the post-2026 strategic framework, in light of recent EU guidance and the evolving geopolitical landscape.

### **Agostino SPERANDEO**

Capo Divisione Strategia e politiche di cybersicurezza nazionale, Agenzia per la Cybersicurezza Nazionale

11h45 - 11h55

## FROM POLICY TO PRACTICE: TRANSLATING EU CYBERSECURITY POLICIES INTO NATIONAL ACTION

Man mano che l'Unione Europea intensifica la propria agenda in materia di cybersicurezza attraverso iniziative strategiche come la Direttiva NIS2, il Cyber Resilience Act e la Strategia di cybersecurity, garantire un'attuazione efficace a livello nazionale diventa al contempo una sfida e una priorità. ENISA supporta gli Stati membri nella traduzione delle politiche europee di cybersicurezza in realtà operative, attraverso strumenti di monitoraggio, attività di rafforzamento delle capacità e collaborazioni transfrontaliere.

The National Cybersecurity Strategy three years after its launch: governance model, achieved objectives, and future challenges. An opportunity to reflect on the progress made and to identify priorities for the post-2026 strategic framework, in light of recent EU guidance and the evolving geopolitical landscape.

### **Erika MAGONARA**

Head of Sector for the Policy Monitoring and Analyses Unit, European Union Agency for Cybersecurity (ENISA)

12h10 - 12h25

## LO SPAZIO CIBERNETICO COME DOMINIO STRATEGICO: MINACCE GLOBALI E RESILIENZA DIGITALE

Il dominio cibernetico, riconosciuto dalla NATO come ambito operativo strategico, è al centro di un contesto globale segnato da minacce ibride e sfide tecnologiche. L'intervento illustrerà la visione dell'Alleanza per rafforzare la resilienza digitale, le capacità nazionali e la cooperazione multilivello, promuovendo il dialogo tra istituzioni, settore privato e ricerca.

Recognized by NATO as a strategic operational domain, cyberspace is at the forefront of a global context shaped by hybrid threats and technological challenges. This intervention will present the Alliance's vision to strengthen digital resilience, enhance national cyber capabilities, and foster multilevel cooperation through dialogue between institutions, the private sector, and the research community.

### **Mario BECCIA**

Deputy Chief Information Officer for Cybersecurity, NATO

12h25 - 13h15

## STRATEGIES AND COOPERATION IN CYBERSPACE, BUILDING CAPACITIES FOR A SECURE DIGITAL SOCIETY

Con la crescente portata e complessità delle minacce informatiche, costruire una società digitale sicura richiede strategie coordinate e una forte cooperazione internazionale. Questa sessione esplorerà gli approcci al rafforzamento delle capacità nel cyberspazio, mettendo in evidenza le buone pratiche, le iniziative transfrontaliere e il ruolo delle partnership pubblico-privato. La discussione si concentrerà su come la collaborazione possa rafforzare la resilienza, promuovere la fiducia e sostenere lo sviluppo di capacità efficaci di cybersicurezza a livello nazionale e globale.

As cyber threats grow in scale and complexity, building a secure digital society requires coordinated strategies and strong international cooperation. This session will explore approaches to capacity building in cyberspace, highlighting best practices, cross-border initiatives, and the role of public-private partnerships. The discussion will focus on how collaborative efforts can enhance resilience, promote trust, and support the development of effective cybersecurity capabilities at national and global levels.

### **Diego BRASIOLI**

Special Envoy of the Minister of Foreign Affairs and International Cooperation for cybersecurity

### **Matteo Emilio BONFANTI**

Capo Divisione Relazioni, cooperazione e policy internazionali, Agenzia per la Cybersicurezza Nazionale (ACN)

### **Albert ANTWI-BOASIAKO**

Former Director General, Cybersecurity Authority of Ghana

### **Liina ARENG**

Director, EU CyberNet Project

### **David VAN DUREN**

Director, Global Forum for Cyber Expertise Secretariat

Moderator:

### **Matteo LUCCHETTI,**

Direttore Operativo Cyber 4.0

13h00 - 14h00

LUNCH E VISITA STAND

## CYBER SECURITY

### SFIDE E OPPORTUNITÀ PER IMPRESE E PA

14h00 - 14h15

#### CYBERSECURITY, MERCATI E CAPITALIZZAZIONE

Megatrend di cybersecurity in un mercato che cambia, i driver di valore economico, gli impatti sulla capitalizzazione delle imprese. Quale rapporto tra sicurezza, fiducia degli investitori e competitività aziendale, tra gestione del rischio cyber e dinamiche di investimento nel settore.

Cybersecurity megatrends in a changing marketplace, the economic drivers, the impact on corporate capitalization. What is the relationship between security, investor confidence, and business competitiveness?

##### **Umberto ROSINI**

Responsabile ICT, CdP Venture Capital Sgr

14h15 - 14h30

#### THE STATE OF CYBERSECURITY IN EUROPE. TRENDS, THREATS AND STRATEGIES

Una panoramica sullo stato attuale della cybersicurezza in Europa, con un'analisi dei principali trend, delle minacce emergenti e delle risposte strategiche a livello dell'UE. Un approfondimento sugli sviluppi recenti, il quadro normativo e le iniziative di cooperazione.

An overview of the current state of cybersecurity in Europe, examining key trends, emerging threats, and strategic responses at EU level. An analysis of recent developments, regulatory frameworks and collaborative initiatives.

##### **Lorenzo MANNELLI**

Director-General Directorate-General for Information Technologies and Cybersecurity (ITEC), European Parliament

14h30 - 15h15

## STRENGTHENING CYBER RESILIENCE OF EU SMES – THE SECURE PROJECT

Il progetto SECURE, coordinato dall'Agenzia per la Cybersicurezza Nazionale (ACN) e con la partecipazione di Cyber 4.0, ha l'obiettivo di rafforzare la postura cyber delle PMI europee e supportarle nell'adeguamento al Cyber Resilience Act, la cui piena applicazione è prevista per il 2027. SECURE prevede la creazione di una piattaforma per il finanziamento a cascata (Financial Support for Third Parties - FSTP) e offrirà risorse finanziarie e competenze tecniche alle piccole e medie imprese in tutta l'UE, grazie a uno dei budget più elevati mai destinati a progetti di cybersicurezza.

The SECURE project, coordinated by the Italian National Cybersecurity Agency (ACN) and partnered by Cyber 4.0, aims to enhance the cyber resilience of European SMEs and support them in complying with the Cyber Resilience Act, due to be fully applied in 2027. SECURE will establish a platform for cascading funding (Financial Support for Third Parties - FSTP) and provide financial and technical capabilities to small and medium sized businesses across all EU, with one of the highest budgets ever allocated for cybersecurity projects.

### **Andrea MARGHERI**

Capo Divisione Progetti Industriali e tecnologici, ACN

### **Paweł K. KOSTKIEWICZ**

Director for Certification, NASK

### **Alberto GARINEI**

Chief Scientific Officer, IdeaRe

Moderator

### **Alessandro CALABRESE**

Head Advisory and Training, Cyber 4.0

15h15 - 15h45

COFFEE BREAK E VISITA STAND

15h45 - 16h00

## INCENTIVI E RISORSE DI CYBER 4.0 PER SUPPORTARE IMPRESE E PA

Le opportunità offerte da Cyber 4.0 a supporto di imprese e pubbliche amministrazioni per favorire la transizione digitale, promuovere formazione avanzata e favorire l'adozione di soluzioni di cybersicurezza nei processi produttivi e nei servizi pubblici. La sessione offrirà inoltre spunti pratici e casi d'uso per comprendere come accedere concretamente al supporto di Cyber 4.0.

The opportunities offered by Cyber 4.0 to support businesses and public administrations in driving digital transition, promoting advanced training, and encouraging the adoption of cybersecurity solutions in production processes and public services. The session will also provide practical insights and use cases to understand how to effectively access the support offered by Cyber 4.0.

### **Filippo SILVESTRI**

Chief Business Development Officer, Cyber 4.0

## PMI TRA GESTIONE DEL RISCHIO CYBER E SICUREZZA DELLA SUPPLY CHAIN. METODOLOGIE DI ANALISI, STRUMENTI OPERATIVI E OPPORTUNITÀ DI SVILUPPO

Sempre più PMI sono chiamate a gestire la cyber sicurezza come leva strategica di competitività, sia come attori di supply chain complesse che come categoria maggiormente esposta al rischio di attacchi cyber. Quali metodologie esistono per l'analisi della propria postura, quali strumenti operativi sono disponibili e quali sono le best practice per rafforzare la sicurezza dei propri asset, tra opportunità di sviluppo, soluzioni scalabili e incentivi in erogazione.

More and more SMEs are being called to manage cybersecurity as a strategic lever for competitiveness, both as players in complex supply chains and as a category most exposed to the risk of cyberattacks. What methodologies exist for analyzing their cybersecurity posture, what operational tools are available, and what are the best practices for strengthening the security of their assets, among development opportunities, scalable solutions, and available incentives?

### **Claudio TELMON**

Board of Directors, CLUSIT

### **Mariella FERRARO**

Direttore Operativo, Campania Digital Innovation Hub

### **Antonio TRUGLIO**

Direttore Digital Innovation Hub Lazio

### **Mario Gaetano DI DIO**

Direttore Generale, Netgroup

### **Stefano BORDI**

Executive VP, Di.Gi. Academy

Moderatore:

### **Alessandro CALABRESE**

Head of Advisory and Training, Cyber 4.0

16h45 - 17h30	<p><b>PUBBLICA AMMINISTRAZIONE E CYBER SICUREZZA: RAFFORZARE LA PROTEZIONE E GARANTIRE LA CONTINUITÀ DEI SERVIZI ESSENZIALI</b></p> <p>Le sfide della PA tra evoluzione normativa e transizione digitale in atto, dalla protezione delle infrastrutture di servizio ai cittadini, incluse le azioni di prevenzione messe in atto per il Giubileo 2025, alle iniziative di awareness per il personale.</p> <p>The challenges of the public administration amid evolving regulations and ongoing digital transition, from protecting service infrastructures for citizens, including the preventive measures being implemented for the 2025 Jubilee, to awareness initiatives for staff.</p> <p><b>Giorgio AGRIFOGLIO</b> Dirigente Trasformazione Digitale, Direzione Generale per la Digitalizzazione, Ministero delle Infrastrutture e dei Trasporti</p> <p><b>Francesco LIPPOLIS</b> Partner, BIP</p> <p><b>Roger CATALDI</b> CISO Almaviva</p> <p>Moderatore: <b>Filippo SILVESTRI</b> Chief Business Development Officer, Cyber 4.0</p>
17h30	FINE GIORNATA - End of the day

9h00 - 9h45

### CYBERSECURITY E DIFESA DEL PAESE: INVESTIMENTI, STRATEGIE E PROSPETTIVE NEL BREVE-MEDIO PERIODO

Un focus sull'evoluzione del contesto pubblico di cyber security per la difesa del Paese, le linee di sviluppo europee e le politiche nazionali di rafforzamento delle capacità. Verrà inoltre approfondito il tema del dual use di tecnologie e competenze, esplorando le interrelazioni sempre più strette tra ambito militare e settore civile, e il ruolo della cooperazione pubblico-privata nello sviluppo di un ecosistema integrato di cybersecurity.

A focus on the evolving public cybersecurity landscape for national defense, European development frameworks, and national policies aimed at strengthening capabilities. The session will also delve into the dual use of technologies and expertise, exploring the increasingly close interconnections between the military and civilian sectors, and the role of public-private cooperation in building an integrated cybersecurity ecosystem.

#### **Daniele ALÌ**

Group Chief Information Security Officer, Fincantieri

#### **Emanuele GALTIERI**

CEO, Cy4Gate

#### **Fabio COCURULLO**

VP Innovation Projects, Grants and Collaborations, Leonardo

Moderatore

#### **Luisa FRANCHINA**

CEO, Hermes Bay

9h45 – 10h00

## IL DOMINIO CYBER E LA NECESSITÀ DI UN EQUILIBRIO STRATEGICO

La crescente interdipendenza tecnologica impone una revisione dei paradigmi tradizionali di sicurezza e difesa, evidenziando il rischio di escalation incontrollate e vulnerabilità sistemiche. L'intervento propone la costruzione di un equilibrio strategico nel dominio cyber, basato su deterrenza credibile, cooperazione internazionale e rafforzamento della resilienza nazionale, per garantire stabilità e sicurezza in un contesto sempre più complesso e dinamico

The growing technological interdependence requires a revision of traditional security and defense paradigms, highlighting the risk of uncontrolled escalations and systemic vulnerabilities. The intervention proposes the construction of a strategic balance in the cyber domain, based on credible deterrence, international cooperation, and the strengthening of national resilience, to ensure stability and security in an increasingly complex environment.

### **Gen. Vincenzo CAMPORINI**

Già Capo di Stato Maggiore dell'Aeronautica e della Difesa

10h00 – 10h15

## SPAZIO E CYBERSECURITY: NUOVE FRONTIERE PER LA SICUREZZA NAZIONALE E IL RUOLO STRATEGICO DELL'AGENZIA SPAZIALE ITALIANA

Nel contesto di una crescente interdipendenza tra tecnologie spaziali e sicurezza cyber, il settore spazio assume un ruolo strategico nella protezione delle infrastrutture critiche e nella difesa degli interessi nazionali. L'intervento offrirà una panoramica sui recenti sviluppi promossi a livello nazionale, evidenziando l'impulso dell'ASI nel rafforzamento delle capacità spaziali italiane.

In the context of a growing interdependence between space technologies and cybersecurity, the space sector plays a strategic role in protecting critical infrastructure and defending national interests. The address will provide an overview of recent developments promoted at the national level, highlighting the renewed momentum of the Italian Space Agency (ASI) in strengthening Italy's space capabilities.

### **Teodoro VALENTE**

Presidente, Agenzia Spaziale Italiana (ASI)

10h15 - 11h00

## QUANTUM E POST-QUANTUM: LE SFIDE DI SICUREZZA E LE OPPORTUNITÀ DI SVILUPPO

I nuovi scenari di sicurezza e innovazione del quantum computing: da un lato la minaccia di compromettere i sistemi crittografici, dall'altro le opportunità per lo sviluppo di comunicazioni sicure e capacità computazionali senza precedenti. In questo contesto è centrale la collaborazione tra centri di ricerca, università, istituzioni pubbliche, mondo privato, anche nel contesto di poli tecnologici dedicati. Quali prospettive concrete nel breve-medio periodo?

The new security and innovation scenarios of quantum computing: on one hand, the threat of compromising current cryptographic systems; on the other, the opportunities for developing secure communications and unprecedented computational capabilities. In this context, collaboration among research centers, universities, public institutions, and the private sector—also within dedicated technology hubs—is key. What are the concrete prospects in the short to medium term?

### **Paolo CONFORTO**

Head of Network, Security and Ground Operations, Thales Alenia Space

### **Massimo BERNASCHI**

Director of Technology, Consiglio Nazionale delle Ricerche (CNR)

### **Ivan VISCONTI**

Professore Ordinario di Informatica, DIAG, Sapienza Università di Roma

### **Angelo GIULIANA**

Direttore Generale, Meditech

Moderatrice:

### **Patrizia LICATA**

Freelance Journalist CorCom-Digital360

11h00 - 11h30

## COFFEE BREAK E VISITA STAND

11h30 - 12h10

## ALLEATI E AVVERSARI: INTELLIGENZA ARTIFICIALE E CYBERSECURITY REALE

L'Intelligenza Artificiale è oggi al centro della trasformazione digitale, anche in ambito cybersecurity: potente alleato nella rilevazione delle minacce, ma anche nuovo vettore di rischio quando utilizzata per scopi malevoli. Un duplice ruolo, tra strumenti difensivi sempre più sofisticati e attacchi automatizzati difficili da intercettare, che ha implicazioni sempre più concrete in un contesto geopolitico instabile, dove disinformazione, manipolazione algoritmica e governance dei dati sensibili diventano sfide strategiche.

Artificial Intelligence is now at the heart of digital transformation, including in the field of cybersecurity: a powerful ally in threat detection, but also a new vector of risk when used for malicious purposes. This dual role—between increasingly sophisticated defensive tools and hard-to-detect automated attacks—has growing real-world implications in an unstable geopolitical context, where disinformation, algorithmic manipulation, and the governance of sensitive data have become strategic challenges.

### **Raffaele MARCHETTI**

Full Professor, International Relations, Università Luiss

### **Fabrizio SILVESTRI**

Full Professor and the coordinator of the Ph.D. in Data Science, Università Sapienza

### **Roberto DE FINIS**

Direttore Generale, Sistemi & Automazione

### **Mirko LEANZA**

CISO e responsabile della BU Cybersecurity & Governance, Telecomsys

Moderatrice:

### **Patrizia LICATA**

Freelance Journalist CorCom-Digital360

12h10 - 12h50

## OLTRE IL PERIMETRO: SICUREZZA OT NELL'ERA DELLA CONVERGENZA DIGITALE

La convergenza digitale espande la superficie d'attacco e rende più complessa la protezione di sistemi fisici, industriali e non, che integrano componenti digitali. A questo si associa una crescente necessità di compliance a normative sempre più rigorose, come il CRA o la NIS2. Quali i trend emergenti, le soluzioni di sicurezza e le strategie di resilienza in questo contesto sempre più connesso e vulnerabile?

Digital convergence expands the attack surface and makes the protection of physical systems, both industrial and non-industrial, that integrate digital components more complex. This is accompanied by a growing need for compliance with increasingly stringent regulations, such as the CRA or NIS2. What are the emerging trends, security solutions, and resilience strategies in this increasingly connected and vulnerable environment?

### **Stefano PANZIERI**

Professore Ordinario, Dipartimento di Ingegneria civile, informatica e delle tecnologie aeronautiche, Università Roma Tre

### **Luca FARAMONDI**

PhD Assistant Professor, Coordinatore Scientifico Master I Livello in Cybersecurity Management, Università Campus Biomedico di Roma

### **Domenico CAPRIGLIONE**

Professore Ordinario di Misure Elettriche ed Eletttroniche - Dipartimento di Ingegneria Elettrica e dell'Informazione - Università degli Studi di Cassino e del Lazio Meridionale

### **Alessio ACETI**

CEO, HWG Sababa

Moderatrice:

### **Patrizia LICATA**

Freelance Journalist CorCom-Digital360

12h50 - 13h30

## RETURN ON SECURITY INVESTMENT (ROSI): MISURARE L'IMPATTO DELLA CYBERSECURITY NEL PUBBLICO E NEL PRIVATO

Sarà presentato un framework pensato per guidare le decisioni strategiche, misurare i benefici degli interventi di sicurezza e valutarne l'impatto complessivo nel medio-lungo periodo. Attraverso casi d'uso, strumenti di analisi e metriche applicabili, saranno presentati approcci concreti per integrare la cybersecurity nei modelli di valore organizzativi, favorendo una cultura della sicurezza come leva di efficienza, resilienza e competitività.

A framework will be presented to guide strategic decision-making, measure the benefits of security initiatives, and assess their overall impact in the medium to long term. Through use cases, analytical tools, and applicable metrics, concrete approaches will be shared to integrate cybersecurity into organizational value models, promoting a culture of security as a driver of efficiency, resilience, and competitiveness.

### **Liviana LOTTI**

Agenzia per la Cybersicurezza Nazionale (ACN)

### **Yuri RASSEGA**

CISO, Enel e Presidente AssoCISO

### **Alvise BIFFI**

CEO, Secure Network BV Tech e Vice Presidente Assolombarda

Moderatore:

### **Paolo SPAGNOLETTI**

Presidente, Cyber 4.0

13h30 - 14h30

## NETWORKING LUNCH

## COMPETENCIES AND INNOVATION

14h30 - 15h15

### CYBER COMPETENCE GAP, QUALCOSA È CAMBIATO

Le competenze cyber rappresentano la prima linea di difesa per le imprese. Quali sono i metodi più innovativi per la formazione del personale, quali profili servono di più e come si applica il framework europeo sulle competenze cyber, quali iniziative per formare giovani talenti?

Cyber skills represent the first line of defense for businesses. What are the most innovative methods for employee training, what profiles are most in demand, how is the European framework for cyber skills applied, and what initiatives are in place to train young talents?

#### L'analisi di Cyber 4.0

##### **Antonio CAPOBIANCO**

CEO, Fata Informatica

##### **Mattia SICILIANO**

Adjunct Professor of Cybersecurity e Co-Director del Corporate Cybersecurity HUB, Luiss

##### **Piero FIORETTI**

CEO, Versy

##### **Lorenzo SCATENA**

Segretario Generale, Fondazione Amaldi

Moderator:

##### **Alessandro CALABRESE**

Head Advisory and Training, Cyber 4.0

15h15 - 16h00

## CYBERSECURITY È INNOVAZIONE: UNO SGUARDO AL FUTURO

Idee, pitch, call for action, problemi, soluzioni, risposte, iniziative, progetti, programmi.

Ideas, pitches, calls for action, problems, solutions, responses, initiatives, projects, programs.

**Italian Game, Arianna RUFINI, Ufficio di Gabinetto MIMIT**

**Il progetto ESII - Early Security Incident Investigation, Cristian LUCCI, CEO Sharelock**

**Open Innovation Challenge, AI & Cybersecurity, Maria Angela ILARI, LaziInnova**

**Le iniziative della Fondazione Piemonte Innova, Luca MANCINO, Innovation Manager, Fondazione Piemonte Innova**

**A Scuola Connessi, Laura TEODONNO e Claudio PROIETTI, Hermes Bay**

Moderatore:

**Matteo LUCCHETTI**

Direttore Operativo Cyber 4.0

16h00 - 16h30

## KEY TAKEWAYS DEL FORUM CYBER 4.0

**Raffaele BOCCARDO**

CEO BV Tech

**Vincenzo TAGLIAFERRI**

Professore Emerito, Università Tor Vergata

Modera e conclude:

**Paolo SPAGNOLETTI**

Presidente Cyber 4.0