FORUM 2026
CYBER 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

3-4 GIUGNO 2026

Luiss ROMA / Aula 200

KEY TAKEAWAYS

Con il Patrocinio di:

European Commission

Ministero delle Imprese e del Made in Italy

Ministero degli Affari Esteri e della Cooperazione Internazionale

ACN

Funded by the European Union
NextGenerationEU

Hosted by: LUISS Università di Roma

INDICE

1. IL FORUM CYBER 4.0 2026

Il **Forum Cyber 4.0** è l'evento annuale promosso dal Centro di Competenza nazionale **Cyber 4.0**, nato con l'obiettivo di favorire il confronto tra istituzioni, imprese, università, centri di ricerca e operatori del settore sui principali temi della cybersicurezza e della trasformazione digitale. Giunto nel **2026 alla sua quarta edizione**, il Forum rappresenta oggi uno dei principali momenti di incontro dell'ecosistema italiano della cybersecurity, in linea con la Strategia Nazionale di Cybersicurezza e con il ruolo affidato a Cyber 4.0 dal Ministero delle Imprese e del Made in Italy (MIMIT).

L'edizione **2026** si è svolta il **3 e 4 giugno** presso **l'Aula Chiesa dell'Università Luiss Guido Carli di Roma**, riunendo esperti, rappresentanti delle istituzioni, aziende leader, mondo accademico e stakeholder nazionali e internazionali per due giornate dedicate ad approfondimenti, tavole rotonde e networking. Il programma ha affrontato temi strategici quali la competitività delle filiere industriali, la protezione delle infrastrutture critiche, la digitalizzazione sicura della Pubblica Amministrazione e delle imprese, la cooperazione internazionale e lo sviluppo delle competenze nel settore cyber.

L'interesse verso il Forum è cresciuto costantemente nel corso delle prime quattro edizioni. Nel **2026** sono stati registrati **oltre 650 iscritti**, con circa **440 partecipanti effettivi**, confermando il crescente ruolo dell'iniziativa quale punto di riferimento per la comunità della cybersecurity italiana.

Questa evoluzione riflette il rafforzamento del ruolo di Cyber 4.0 come hub nazionale per l'innovazione, il trasferimento tecnologico e lo sviluppo delle competenze, favorendo il dialogo tra ricerca, industria e istituzioni e contribuendo alla crescita dell'ecosistema italiano della cybersicurezza.

2. SCENARIO CYBER E CONTESTO STRATEGICO

Il Forum conferma che la cybersecurity si colloca ormai al centro della sicurezza nazionale, della competitività industriale e della capacità del Paese di sostenere una trasformazione digitale affidabile. La minaccia non è più confinata alla protezione di dati o sistemi informativi: attraversa filiere produttive, infrastrutture critiche, servizi pubblici, ecosistemi industriali, spazio, domini underwater e processi cognitivi esposti alla manipolazione dell'informazione.

L'evoluzione delle minacce ibride modifica il perimetro della resilienza. Attacchi cyber, sabotaggio fisico, disinformazione, pressione geopolitica e compromissione della supply chain tendono a convergere. In questo scenario, la protezione delle infrastrutture OT, dei cavi sottomarini, dei sistemi satellitari, delle reti energetiche, dei servizi sanitari e degli asset pubblici richiede capacità di simulazione, monitoraggio, intelligence e cooperazione pubblico-privato.

L'intelligenza artificiale agisce come fattore di accelerazione sia della minaccia sia della difesa. Riduce i costi di personalizzazione degli attacchi, aumenta la credibilità delle campagne di phishing e disinformazione, introduce rischi legati ai modelli fondazionali e apre la questione delle infrastrutture cognitive. Al tempo stesso, consente nuove forme di analisi predittiva, supporto decisionale, threat intelligence, automazione difensiva e gestione dinamica degli accessi.

Le tecnologie emergenti ampliano la prospettiva temporale della sicurezza. Quantum computing, AI, sistemi autonomi, 5G privato, dispositivi medicali connessi, automotive, space economy e piattaforme industriali digitalizzate richiedono

un approccio security by design, testing continuo e capacità di validazione prima della messa in produzione. La resilienza si costruisce quindi prima della crisi, attraverso laboratori, piattaforme, formazione e governance.

3. RISULTATI CONCRETI E ASSET DA VALORIZZARE

Il Forum ha rappresentato innanzi tutto l'occasione per evidenziare i risultati concreti prodotti dal Centro, che ha progressivamente trasformato le risorse a disposizione, in particolare quelle provenienti dal PNRR, le partnership istituzionali e la rete associativa in capacità operative, servizi per imprese e PA, piattaforme tecnologiche e iniziative internazionali.

Servizi alle imprese.

Sotto questa componente, Cyber 4.0 ha erogato 11,5 milioni di euro di incentivi, corrispondenti a un valore complessivo di 14,6 milioni di euro di attività. A fronte di quasi 1.000 candidature e oltre 3.600 richieste di servizi, sono state raggiunte oltre 450 imprese e oltre 900 servizi sono stati contrattualizzati ed erogati. La composizione dei beneficiari – 56% piccole imprese, 34% medie e 10% grandi – conferma la capacità del Centro di intervenire in particolare a supporto delle PMI e delle filiere produttive.

Sostegno all'innovazione.

A questa azione si affianca il sostegno all'innovazione, con 20 progetti di ricerca e trasferimento tecnologico finanziati e 4,7 milioni di euro di cofinanziamento allocato in settori strategici quali difesa, automotive, spazio e sanità.

Infrastruttura distribuita.

Parallelamente, Cyber 4.0 ha costruito un'infrastruttura operativa distribuita per attività di test, validazione e supporto di sistema, che comprende il T4 DemoLab dotato di rete privata 5G per la sperimentazione tecnologica, cinque laboratori dedicati alla sicurezza OT, due laboratori sull'intelligenza artificiale, quattro piattaforme di servizio per le imprese e un Cyber Range.

Supporto alla PA.

Il Centro ha inoltre consolidato il proprio contributo alle Pubbliche Amministrazioni, incluse attività a supporto dei comparti strategici della difesa e della sicurezza nazionale. Tra le attività realizzate figurano la formazione sulla NIS2 per 26 atenei pubblici, che ha coinvolto 975 partecipanti, gli assessment su ecosistemi ICT pubblici, il supporto alla definizione di framework e controlli di conformità e le iniziative dedicate ai domini underwater e spaziale.

Il framework di cybersecurity per il dominio spaziale.

In ambito Difesa, Cyber 4.0 ha sviluppato per il Comando per le Operazioni in Rete un framework per la protezione delle infrastrutture spaziali, accompagnato da uno scenario esercitativo realizzato sul Cyber Range della Difesa.

Progetti europei e dimensione internazionale.

La dimensione europea e internazionale completa questo patrimonio di attività. Attraverso il progetto SECURE, Cyber 4.0 contribuisce al percorso di adeguamento delle PMI europee al Cyber Resilience Act e alla gestione di strumenti di finanziamento diretto. Sul piano internazionale, il Centro ha progressivamente incrementato il proprio ruolo di attore nazionale del panorama del capacity building internazionale. In particolare, nel corso del Forum sono state presentate: la call Cyber4Africa nell'ambito dell'AI Hub for Sustainable Development condotto da UNDP, il programma bilaterale Italia-Ghana promosso e finanziato dal MAECI, l'iniziative di cooperazione con la Colombia sviluppata nel

contesto del D4D Hub e le attività di supporto al comparto civile dell'Ucraina sviluppate attraverso il Meccanismo di Tallinn, di cui il Centro è partner.

4. KEY TAKEAWAYS

Le sessioni del Forum hanno restituito alcuni messaggi trasversali sullo scenario della cybersecurity, sull'evoluzione dei rischi e sulle condizioni necessarie per rafforzare la resilienza del sistema Paese. I paragrafi seguenti sintetizzano i principali elementi emersi dal confronto tra istituzioni, imprese, mondo della ricerca ed esperti nazionali e internazionali.

4.1. CYBERSECURITY COME INFRASTRUTTURA DI FIDUCIA, DEMOCRAZIA E SOVRANITÀ

La cybersecurity è ormai una precondizione per la fiducia nei servizi pubblici, nei mercati e nelle relazioni economiche e sociali. Non riguarda soltanto la protezione tecnica di dati e sistemi, ma investe la continuità delle filiere produttive, la tutela dei servizi essenziali, la capacità di prevenire e gestire le crisi e, più in generale, la credibilità del Paese come attore tecnologico affidabile.

Dal Forum emerge quindi **un concetto più ampio di sicurezza digitale, strettamente connesso alla sovranità tecnologica, all'autonomia strategica europea e alla capacità di governare le dipendenze da tecnologie, piattaforme e fornitori esterni**. In questo quadro, la frammentazione delle competenze e la vulnerabilità delle PMI non costituiscono criticità circoscritte alle singole organizzazioni, ma fattori di rischio sistemico, capaci di propagarsi lungo le catene del valore.

La protezione deve inoltre estendersi a infrastrutture e domini nei quali dimensione fisica e digitale sono ormai inseparabili: sistemi OT, reti energetiche e di trasporto, spazio, infrastrutture underwater, piattaforme di intelligenza artificiale e supply chain del software. Investire in cybersecurity significa pertanto rafforzare la capacità complessiva del Paese di innovare, produrre e offrire servizi in modo sicuro e continuativo. La sicurezza non rappresenta soltanto un costo tecnico o un adempimento normativo, ma un investimento nella competitività, nella resilienza democratica e nella sovranità nazionale ed economica.

4.2. CYBER 4.0 COME INFRASTRUTTURA NAZIONALE DISTRIBUITA DI CYBER RESILIENZA

Dal Forum emerge l'esigenza di superare una visione della cybersecurity basata su interventi isolati, favorendo invece la connessione tra competenze, infrastrutture e servizi già disponibili nell'ecosistema nazionale. In questa prospettiva si colloca l'evoluzione di Cyber 4.0: non soltanto erogatore di servizi per imprese e Pubbliche Amministrazioni, ma anche punto di raccordo operativo tra istituzioni, sistema produttivo, ricerca e fornitori di tecnologia, soprattutto nelle attività di prevenzione.

Laboratori, piattaforme, reti tecnologiche e competenze specialistiche messi a disposizione dal Centro possono concorrere a un percorso integrato che comprende analisi del rischio, sperimentazione, compliance, monitoraggio, risposta e continuità operativa. La natura distribuita di questo modello permette di aggregare capacità presenti in organizzazioni e territori diversi, rendendole più facilmente accessibili anche alle realtà meno strutturate.

Questo approccio è particolarmente rilevante negli ambiti in cui le competenze sono rare, gli investimenti iniziali elevati e i benefici prevalentemente collettivi e di lungo periodo, come la sicurezza OT, l'intelligenza artificiale, l'aerospazio, la difesa, il dominio underwater e le tecnologie quantum. In questi settori, la collaborazione tra pubblico, privato e ricerca è necessaria per evitare la frammentazione delle iniziative e

ampliare l'accesso a capacità che difficilmente potrebbero essere sviluppate autonomamente, soprattutto da PMI e amministrazioni.

Gli asset costruiti da Cyber 4.0 sono pertanto da inquadrare come parti di un sistema connesso, capace di sostenere la prevenzione, la sperimentazione e la condivisione delle competenze, contribuendo a rafforzare in modo progressivo la resilienza del sistema Paese.

4.3. DIFESA, SPAZIO E DOMINIO MARITTIMO NEL MANDATO DI CYBER 4.0

Difesa, spazio e dominio marittimo sono ambiti nei quali sicurezza digitale, protezione fisica delle infrastrutture e sicurezza nazionale risultano sempre più interdipendenti. La crescente digitalizzazione dei sistemi spaziali e marittimi, l'estensione delle catene di fornitura e la dipendenza da componenti e servizi esterni ampliano la superficie di attacco e rendono necessario un approccio integrato alla gestione del rischio.

Nel dominio spaziale, il lavoro svolto a **supporto del Comando per le Operazioni in Rete** ha mostrato l'importanza di tradurre gli scenari di minaccia, nel caso specifico in ambito spaziale, in framework di controllo cyber, strumenti di valutazione della maturità ed esercitazioni pratiche. La realizzazione di uno scenario dedicato sul Cyber Range della Difesa ha evidenziato inoltre il valore della simulazione per verificare procedure, responsabilità e capacità di risposta prima che si verifichi una crisi reale.

Una logica analoga riguarda il **dominio marittimo e underwater**, dove cavi sottomarini, infrastrutture energetiche, sistemi portuali, reti di comunicazione e sensoristica distribuita costituiscono un insieme fortemente interconnesso. La protezione di questi asset richiede una conoscenza aggiornata delle infrastrutture, l'analisi congiunta dei rischi fisici e cyber e la definizione di scenari che tengano conto anche del quadro normativo e delle capacità operative disponibili.

Dal Forum emerge la **necessità di rafforzare il confronto tra Difesa, istituzioni, industria e ricerca su temi quali sicurezza delle supply chain, componenti di terze parti e utilizzo dell'open source, digital twin, cyber range e sistemi di monitoraggio**. In domini così complessi, sempre di più la resilienza dipende dalla possibilità di condividere competenze, sperimentare soluzioni e verificare congiuntamente l'efficacia delle misure adottate, attività che sono perfettamente in linea con il mandato costitutivo di Cyber 4.0.

4.4. PNRR: DA INVESTIMENTO STRAORDINARIO A CAPACITÀ PERMANENTE

Il PNRR ha rappresentato un'importante accelerazione per la trasformazione di risorse pubbliche in servizi, progetti di innovazione e infrastrutture operative. I risultati presentati al Forum restituiscono la dimensione dell'intervento: 11,5 milioni di euro di incentivi erogati, 14,6 milioni di euro di valore complessivo dei servizi, 988 candidature, **oltre 450 imprese raggiunte**, più di 3.600 servizi richiesti **e oltre 900 servizi contrattualizzati ed erogati**.

La composizione dei beneficiari – 56% piccole imprese, 34% medie e 10% grandi – conferma la capacità delle misure di raggiungere soprattutto il tessuto delle PMI. A questa linea si aggiungono 20 progetti di ricerca, innovazione e trasferimento tecnologico, sostenuti con 4,7 milioni di euro di cofinanziamento in settori quali difesa, automotive, spazio e sanità.

Dal Forum emerge tuttavia che **il valore del PNRR** non può essere misurato soltanto attraverso le risorse impiegate, il numero di servizi erogati o i soggetti coinvolti. La questione centrale riguarda gli **effetti prodotti: riduzione delle vulnerabilità, crescita delle competenze, adozione di misure di sicurezza, maggiore capacità di risposta agli incidenti e miglioramento della continuità operativa**.

La fase successiva consiste nel consolidare quanto realizzato, assicurando continuità e accessibilità a servizi, laboratori e piattaforme anche oltre l'orizzonte del finanziamento straordinario. Il passaggio da investimento temporaneo a capacità permanente richiede sostenibilità economica, domanda effettiva da parte di imprese e amministrazioni e una misurazione più sistematica dei risultati. È su questa capacità di produrre cambiamenti duraturi, più che sulla sola spesa realizzata, che potrà essere valutato l'impatto complessivo del PNRR.

4.5. LABORATORI E PIATTAFORME COME STRUMENTI DI RESILIENZA

Laboratori e piattaforme assumono valore quando rispondono a bisogni concreti di imprese e Pubbliche Amministrazioni. Non sono quindi semplici dimostratori tecnologici, ma ambienti nei quali verificare la sicurezza prima della messa in produzione, simulare scenari realistici, validare soluzioni e sviluppare competenze difficilmente disponibili all'interno delle singole organizzazioni.
Il patrimonio presentato al Forum comprende il **T4 DemoLab**, una rete privata 5G per la sperimentazione, cinque laboratori dedicati alla sicurezza OT, due laboratori sull'intelligenza artificiale, quattro piattaforme di servizio per le imprese e un Cyber Range. Questi asset coprono ambiti diversi – dall'automotive alla sanità, dai trasporti all'IoT e ai sistemi industriali – e consentono di affrontare in ambienti controllati l'interazione tra sicurezza digitale, continuità operativa e safety.
Le piattaforme di servizio estendono questa capacità anche alle attività continuative di prevenzione, monitoraggio e condivisione delle informazioni. Il SOC as a Service, ISAC4PMI e Spotlight, dedicata all'analisi della disinformazione, rispondono a esigenze che molte organizzazioni, soprattutto di minori dimensioni, difficilmente potrebbero gestire in autonomia.
Dal Forum emerge quindi l'importanza di considerare **laboratori e piattaforme come componenti connesse di un percorso che va dall'analisi del rischio alla sperimentazione, dalla compliance alla detection e alla risposta**. La loro efficacia dipende non tanto dal numero o dal livello tecnologico degli asset disponibili, quanto dalla capacità di renderli accessibili, integrarli nei processi delle organizzazioni e tradurne l'utilizzo in un miglioramento verificabile della resilienza.

4.6. COMPLIANCE COME LEVA INDUSTRIALE: NIS2 E CRA, IL RUOLO DELL'ECSF

La compliance sta diventando uno dei principali fattori di trasformazione del mercato della cybersecurity.

4.6.1. LA NIS2.

- Per i soggetti essenziali e importanti, la NIS2 introduce innanzitutto una responsabilità diretta degli organi di amministrazione e direttivi, chiamati ad approvare le modalità di attuazione delle misure di sicurezza, supervisionarne l'applicazione e partecipare a specifiche attività formative. La gestione del rischio cyber diventa così parte integrante della governance dell'organizzazione e non può essere delegata esclusivamente alle funzioni tecniche.
- Gli obblighi comprendono l'adozione di misure tecniche, operative e organizzative proporzionate al rischio. Queste riguardano, tra l'altro, analisi dei rischi e politiche di sicurezza, gestione degli incidenti, continuità operativa e gestione delle crisi, backup e ripristino, sicurezza della supply chain, sviluppo e manutenzione sicura dei sistemi, gestione e divulgazione delle vulnerabilità, controllo degli accessi, uso della crittografia, autenticazione a più fattori, formazione e pratiche di igiene informatica. Le specifiche di base definite da ACN articolano questi ambiti in 37 misure e 87 requisiti, differenziati in funzione della classificazione del soggetto.

- La NIS2 rafforza inoltre gli obblighi di notifica degli incidenti significativi al CSIRT Italia. Il processo prevede una pre-notifica entro 24 ore dalla conoscenza dell'incidente, una notifica più completa entro 72 ore ed una relazione finale, di norma, entro un mese. L'obbligo non riguarda qualsiasi evento informatico, ma gli incidenti capaci di provocare una grave perturbazione dei servizi o rilevanti conseguenze operative, finanziarie o reputazionali. Per i soggetti inseriti nell'elenco NIS nel 2025, gli obblighi di notifica sono operativi da gennaio 2026, mentre il termine per adottare le misure di sicurezza di base è fissato a ottobre 2026.
- A questi adempimenti si aggiungono la registrazione sulla piattaforma ACN, l'aggiornamento periodico delle informazioni sull'organizzazione e sui servizi forniti, l'individuazione dei referenti previsti e la collaborazione con l'Autorità nelle attività di vigilanza. Il quadro sanzionatorio rafforza ulteriormente la necessità di poter dimostrare non soltanto l'esistenza formale di politiche e procedure, ma la loro effettiva applicazione.

4.6.2. IL CYBER RESILIENCE ACT

- Il Cyber Resilience Act interviene invece sulla sicurezza dei prodotti hardware e software con elementi digitali. Impone ai produttori di integrare la sicurezza fin dalla progettazione, effettuare valutazioni del rischio, gestire e correggere le vulnerabilità, fornire aggiornamenti di sicurezza e conservare la documentazione necessaria a dimostrare la conformità lungo il ciclo di vita del prodotto.
- Gli obblighi di segnalazione delle vulnerabilità attivamente sfruttate e degli incidenti gravi decorreranno dall'11 settembre 2026, mentre i requisiti principali saranno pienamente applicabili dall'11 dicembre 2027.
- In questo quadro, **il progetto europeo SECURE rappresenta un esempio di collegamento tra regolazione e politica industriale**, poiché affianca agli obblighi del Cyber Resilience Act risorse e servizi per accompagnare le PMI nel percorso di adeguamento.

Le difficoltà evidenziate dalle imprese, e confermate anche dalle azioni di supporto erogate da Cyber 4.0, consistono oggi nel tradurre questi quadri normativi in attività concretamente applicabili: comprendere gli obblighi, valutare i gap, definire le priorità, introdurre controlli, formare il personale e produrre evidenze verificabili.
Come evidenziato dagli interventi del Forum, la compliance può però diventare una leva di innovazione, qualità e accesso al mercato, a condizione che venga affrontata come un percorso di maturazione e non come un esercizio burocratico.
In questo contesto, assume rilevanza anche lo **European Cybersecurity Skills Framework**, che consente di collegare gli obblighi alle competenze necessarie per attuarli, rendendo più coerenti formazione, organizzazione interna, selezione dei profili e qualificazione dei fornitori.

4.7. PMI, FILIERE STRATEGICHE E SERVIZI CONDIVISI

La resilienza delle filiere dipende in larga misura dalla capacità di rafforzare la sicurezza delle PMI che ne fanno parte. La crescente interconnessione tra fornitori, piattaforme e operatori essenziali fa sì che una vulnerabilità presente in un'organizzazione di piccole dimensioni possa propagarsi lungo la catena del valore e produrre conseguenze molto più ampie. La sicurezza delle PMI non è quindi soltanto un problema delle singole aziende, ma una componente della resilienza complessiva del sistema produttivo.

I dati presentati al Forum restituiscono un quadro concreto. Tra le circa 400 imprese sottoposte a test, oltre la metà ha mostrato vulnerabilità significative, spesso riconducibili a patch non applicate, configurazioni inadeguate e assenza di piani strutturati di risposta agli incidenti. Si tratta di criticità note e, in molti casi, risolvibili, che tuttavia persistono per la scarsità di competenze interne, la frammentazione degli interventi e la difficoltà di trasformare la consapevolezza del rischio in azioni continuative.
Un ulteriore elemento riguarda la sostenibilità economica. Per molte PMI, il budget annuale destinato alla cybersecurity si colloca indicativamente tra 5.000 e 20.000 euro. Gli interventi sostenuti attraverso le misure pubbliche hanno talvolta raggiunto un valore pari al doppio del budget cyber ordinario dell'impresa. Meno di un terzo delle aziende coinvolte avrebbe realizzato le stesse attività senza incentivi e accompagnamento specialistico. Il dato evidenzia sia l'effetto abilitante del supporto pubblico sia la difficoltà di mantenere nel tempo livelli adeguati di protezione facendo affidamento esclusivamente su interventi straordinari.
Dal Forum emerge pertanto l'esigenza di modelli di servizio proporzionati alle dimensioni, alla maturità e al profilo di rischio delle imprese. Assessment semplificati, interventi correttivi prioritari, formazione, condivisione delle informazioni e servizi gestiti possono ridurre i costi di accesso a competenze e strumenti che una singola PMI difficilmente potrebbe sviluppare al proprio interno.
In questa prospettiva, **strumenti condivisi come il SOC as a Service e ISAC4PMI** possono favorire il passaggio da interventi occasionali a un percorso continuativo di miglioramento. Il loro valore risiede nella possibilità di mettere in comune capacità di monitoraggio, informazioni sulle minacce ed esperienze operative, collegando la sicurezza della singola impresa a quella della filiera nella quale opera.

4.8. AI, OT, QUANTUM E NUOVE SUPERFICI DI ATTACCO

Intelligenza artificiale, sistemi OT e tecnologie quantistiche stanno ampliando le superfici di attacco e modificando le modalità con cui le organizzazioni devono valutare e gestire il rischio. Pur trattandosi di ambiti diversi, condividono alcune caratteristiche: rapida evoluzione, forte interdipendenza con infrastrutture e processi esistenti, competenze ancora limitate e difficoltà nel verificare la sicurezza attraverso strumenti tradizionali.
L'intelligenza artificiale agisce contemporaneamente come moltiplicatore della minaccia e strumento di difesa. Può rendere più rapide, credibili e personalizzate le campagne di phishing e disinformazione, facilitare l'automazione degli attacchi e introdurre nuove vulnerabilità legate ai modelli, ai dati e alle interazioni con sistemi esterni. Al tempo stesso, può sostenere l'analisi predittiva, la threat intelligence, il rilevamento delle anomalie e il lavoro degli analisti. Il punto centrale non è quindi soltanto proteggere i sistemi attraverso l'AI, ma garantire la sicurezza, l'affidabilità e la corretta governance delle soluzioni di AI utilizzate. Proprio in questa direzione operano i due laboratori realizzati da Cyber 4.0 in collaborazione con i soci Luiss e Sapienza.
I sistemi OT presentano una criticità ulteriore, perché collegano il rischio digitale alla continuità dei processi e alla sicurezza fisica di impianti, operatori e utenti. La loro protezione richiede una conoscenza aggiornata degli asset, il controllo degli accessi remoti, la segmentazione delle reti, una gestione delle vulnerabilità basata sul rischio e piani di risposta compatibili con l'esigenza di mantenere operativi i sistemi. Nei settori industriale, sanitario, automotive e dei trasporti, un incidente cyber può infatti produrre conseguenze che vanno oltre la perdita di dati. Cyber 4.0 può mettere a disposizione per test tecnologici, validazioni di sicurezza e analisi in pre-produzione 5 laboratori specializzati sul tema della OT security, realizzati in collaborazione con i propri soci Università di Cassino, Go Infoteam, Università Campus Biomedico, Università di Roma Tor Vergata, BV Tech.
Il quantum computing introduce invece una prospettiva di più lungo periodo, ma richiede decisioni da assumere già oggi. Lo scenario harvest now, decrypt later – nel quale dati cifrati vengono acquisiti per

essere decifrati in futuro – rende particolarmente esposte le informazioni sensibili con una lunga vita utile. La transizione verso soluzioni quantum-safe presuppone la mappatura degli algoritmi crittografici utilizzati, l'individuazione dei dati più esposti e la pianificazione graduale della migrazione.
Dal Forum emerge quindi la necessità di affiancare alla gestione ordinaria della sicurezza una capacità continua di sperimentazione e validazione. **Laboratori dedicati all'AI e ai sistemi OT, Cyber Range e ambienti controllati** consentono di verificare tecnologie, simulare incidenti e analizzare l'interazione tra cybersecurity, safety e continuità operativa. In settori caratterizzati da elevata complessità e rapida innovazione, anticipare il rischio attraverso testing e simulazione diventa parte integrante della resilienza.

4.9. COMPETENZE, FORMAZIONE E CYBER DIPLOMACY

La disponibilità di competenze adeguate rappresenta una condizione essenziale per trasformare investimenti, tecnologie e obblighi normativi in capacità operative. La carenza di profili specialistici rimane un problema rilevante, ma dal Forum emerge anche un'esigenza più ampia: diffondere conoscenze differenziate a tutti i livelli delle organizzazioni, dai vertici responsabili delle decisioni ai team tecnici, fino al personale non specializzato.
La formazione deve quindi essere calibrata sui ruoli e sui contesti di applicazione. Per i vertici, assume particolare rilievo la comprensione del rischio, delle responsabilità introdotte dalla NIS2 e delle conseguenze degli incidenti sulla continuità operativa. Per i profili tecnici servono invece competenze specialistiche e occasioni di esercitazione. Per il personale nel suo complesso, awareness, simulazioni e strumenti di gamification possono contribuire a ridurre i comportamenti a rischio e a consolidare pratiche di sicurezza quotidiane.
Le esperienze presentate al Forum mostrano la portata di questo approccio. Il percorso NIS2 rivolto al sistema universitario ha coinvolto 26 atenei pubblici e 975 partecipanti, con un'attenzione specifica ai livelli apicali. **Per le Pubbliche Amministrazioni sono stati inoltre sviluppati percorsi articolati su più livelli**, comprendenti formazione manageriale, approfondimenti tecnici e sensibilizzazione generale su gestione del rischio, risposta agli incidenti e igiene informatica.
La riflessione avviata con ACN e con i principali operatori del mercato evidenzia inoltre l'esigenza di rendere maggiormente coordinate e riconoscibili le iniziative formative rivolte alle imprese. L'European Cybersecurity Skills Framework può offrire un riferimento comune per collegare contenuti formativi, ruoli professionali, fabbisogni organizzativi e qualificazione delle competenze, riducendo la frammentazione dell'offerta.
La cyber diplomacy amplia ulteriormente il perimetro delle competenze necessarie. La sicurezza digitale è ormai parte delle relazioni internazionali, della cooperazione allo sviluppo, della gestione delle crisi e dei negoziati multilaterali. In questo contesto si inserisce l'intenzione di Cyber 4.0 di lanciare un corso executive in cyber diplomacy, il cui lancio è previsto per ottobre, che mira a rafforzare profili capaci di comprendere insieme aspetti tecnologici, normativi, geopolitici e diplomatici.

4.10. INNOVAZIONE, STARTUP E TRASFERIMENTO TECNOLOGICO VERSO IL MERCATO

Il Forum ha evidenziato come la qualità della ricerca e delle competenze tecniche non sia sufficiente, da sola, a generare innovazione industriale. Il passaggio da un risultato di ricerca o da un prototipo a una soluzione adottabile richiede validazione tecnica, sperimentazione in condizioni realistiche, capacità imprenditoriali, accesso al capitale e apertura ai mercati internazionali.
La cybersecurity offre una domanda in forte crescita: nel 2025 il mercato italiano ha raggiunto un valore di 2,78 miliardi di euro, con un incremento del 12% rispetto all'anno precedente. A questa espansione non corrisponde ancora, tuttavia, un ecosistema di startup e scaleup

comparabile a quello dei principali Paesi europei. Il limite non riguarda soltanto la nascita di nuove imprese, ma soprattutto la capacità di sostenerne la crescita fino al raggiungimento di dimensioni internazionali.

Il divario emerge dai dati complessivi sul venture capital. Nel 2024 le startup italiane hanno raccolto circa 1,5 miliardi di euro, a fronte dei 7,1 miliardi raccolti in Francia, dei 9,4 miliardi in Germania e dei 16,4 miliardi nel Regno Unito. Nel 2025 gli investimenti in equity nelle startup e scaleup hi-tech italiane si sono fermati a 1,46 miliardi, ancora lontani dal massimo di 2,16 miliardi raggiunto nel 2022. Nello stesso periodo, a livello globale, il solo comparto della cybersecurity ha attratto circa 13 miliardi di dollari di venture capital nel 2024. Pur riferendosi a perimetri differenti, questi numeri mostrano con chiarezza la diversa disponibilità di capitale per finanziare la crescita.

Alcune operazioni recenti, come i round da 70 milioni di euro di Exein e da 23 milioni di euro di Cyber Guru, indicano la presenza in Italia di tecnologie e imprese capaci di attrarre investitori internazionali. Restano però casi ancora poco numerosi rispetto alla dimensione del mercato e al potenziale della ricerca nazionale. La fase più critica è spesso quella successiva alla nascita della startup: trasformare il prototipo in prodotto, ottenere le prime referenze industriali, affrontare processi di procurement complessi e finanziare l'espansione commerciale all'estero.

I dati presentati al Forum mostrano un primo contributo del trasferimento tecnologico, con **20 progetti di ricerca e innovazione finanziati e 4,7 milioni di euro di cofinanziamento allocato in settori quali automotive, spazio e sanità**. Per produrre un impatto duraturo, tuttavia, il sostegno alla fase progettuale deve collegarsi più strettamente a testing, validazione, accesso ai clienti, procurement e capitale per la crescita.

Dal Forum emerge quindi che **la competitività italiana non dipenderà soltanto dalla capacità di creare nuove startup, ma dalla possibilità di accompagnarle fino al mercato e sostenerne lo sviluppo su scala europea e globale**. Laboratori, grandi imprese, investitori e amministrazioni possono concorrere a ridurre questa distanza, offrendo ambienti di sperimentazione, primi casi d'uso e percorsi di adozione. Il trasferimento tecnologico diventa così uno strumento di politica industriale: il suo risultato finale non è il prototipo finanziato, ma la nascita di prodotti competitivi, imprese scalabili e capacità tecnologiche che rimangano nel Paese.

4.11. COOPERAZIONE INTERNAZIONALE, CAPACITY BUILDING E DIPLOMAZIA DIGITALE

La dimensione internazionale della cybersecurity ha attraversato in modo trasversale le sessioni del Forum. Minacce, infrastrutture digitali e catene di fornitura non seguono confini nazionali; allo stesso modo, la capacità di prevenirne e gestirne gli effetti dipende sempre più dalla cooperazione tra istituzioni, imprese, organizzazioni internazionali e comunità tecniche.

In questo quadro, il **cyber capacity building assume una funzione che va oltre il trasferimento di conoscenze**. Il rafforzamento delle capacità digitali e di sicurezza dei Paesi partner contribuisce alla stabilità degli ecosistemi connessi, sostiene la cooperazione istituzionale e può favorire l'accesso a nuovi mercati. Formazione, assessment, supporto normativo, sviluppo sicuro delle tecnologie ed esercitazioni diventano così strumenti di politica estera, cooperazione allo sviluppo e diplomazia economica.

Le iniziative presentate al Forum mostrano la diversità degli ambiti di intervento. La call **Cyber4Africa, sviluppata nel contesto dell'AI Hub for Sustainable Development**, sotto la leadership di UNDP, collega il sostegno alle startup africane che utilizzano l'intelligenza artificiale con l'adozione di principi di sicurezza fin dalla progettazione. Il programma bilaterale Italia-Ghana, promosso e finanziato dal MAECI, associa invece dialogo istituzionale, coinvolgimento degli stakeholder e sviluppo di capacità operative. A

queste attività si aggiungono le iniziative rivolte all'America Latina e il supporto alla resilienza cyber del settore civile ucraino.

La **mappatura realizzata tra i soci di Cyber 4.0** – alla quale hanno partecipato cinque università, sette grandi imprese e 22 PMI – evidenzia un interesse già diffuso verso Balcani occidentali, Ucraina, America Latina, Medio Oriente, Africa subsahariana e Indo-Pacifico. Il dato indica la possibilità di collegare più efficacemente le iniziative di capacity building con le competenze della ricerca e dell'industria, mantenendo una chiara distinzione tra obiettivi di cooperazione, interessi istituzionali e possibili ricadute economiche.

L'assunzione da parte dell'Italia della guida del Tallinn Mechanism dal 1° luglio 2026 rappresenta un elemento rilevante nel quadro dell'impegno nazionale a sostegno della resilienza cyber dell'Ucraina. Non determina automaticamente un diverso ruolo per Cyber 4.0, ma si inserisce in un contesto nel quale le competenze e le collaborazioni già sviluppate dal Centro possono contribuire, insieme agli altri attori coinvolti, all'attuazione di iniziative rivolte al settore civile.

Dal Forum emerge forte l'esigenza di considerare la **cooperazione internazionale in ambito cyber non come una successione di progetti separati, ma come un ambito nel quale integrare capacità tecniche, relazioni istituzionali e coinvolgimento del sistema produttivo**.

4.12. GOVERNANCE DI ECOSISTEMA E MISURAZIONE DELL'IMPATTO

La crescita delle attività, degli asset tecnologici e delle collaborazioni di Cyber 4.0 rende sempre più importante **una governance capace di tenere insieme soggetti, strumenti e obiettivi differenti**. Laboratori, piattaforme, servizi alle imprese, progetti di innovazione, formazione e iniziative internazionali producono valore soprattutto quando sono collegati all'interno di una visione coerente e rispondono a bisogni chiaramente identificati.

Dal Forum emerge una necessità di passare dalla gestione di singoli progetti alla capacità di governare un ecosistema. Ciò significa rendere leggibili le relazioni tra competenze dei soci, domanda di imprese e Pubbliche Amministrazioni, infrastrutture disponibili e programmi di finanziamento.

Un ruolo centrale è svolto in questo ambito dalla misurazione dell'impatto. I dati relativi a risorse impiegate, imprese raggiunte, servizi erogati, partecipanti formati e progetti finanziati descrivono l'ampiezza delle attività, ma non sono sufficienti a valutarne pienamente i risultati. Occorre considerare anche i cambiamenti prodotti: vulnerabilità ridotte, misure di sicurezza adottate, competenze consolidate, capacità di risposta migliorate, soluzioni portate sul mercato e servizi diventati continuativi.

La sostenibilità deve rappresentare un'altra dimensione della governance. Gli asset sviluppati attraverso il PNRR e gli altri programmi pubblici possono generare valore nel tempo soltanto se sono mantenuti, aggiornati e collegati a una domanda reale. Questo richiede equilibrio tra finalità pubbliche, accessibilità per PMI e amministrazioni, qualità dei servizi e sostenibilità economica delle infrastrutture.

In ultima battuta, il messaggio del Forum può essere sintetizzato nella considerazione che la credibilità di un ecosistema non dipende dal numero delle iniziative avviate, ma dalla capacità di coordinarle, valutarne gli effetti e comunicarne i risultati in modo trasparente. Una rendicontazione periodica fondata su dati e casi d'uso può rendere più evidente il contributo delle diverse attività alla resilienza del sistema Paese e offrire una base concreta per orientare le scelte future.

5. CONCLUSIONI E ROADMAP

Il Forum Cyber 4.0 2026 restituisce uno scenario nel quale la cybersecurity è ormai parte integrante della sicurezza nazionale, della competitività industriale e della fiducia nei processi di digitalizzazione. Le minacce ibride, la convergenza tra dimensione fisica e digitale e l'evoluzione dell'intelligenza artificiale, dei sistemi OT e delle tecnologie quantistiche richiedono capacità che nessuna organizzazione può sviluppare completamente in autonomia.

In questo quadro, Cyber 4.0 svolge due funzioni complementari: erogare servizi specialistici a imprese e Pubbliche Amministrazioni e operare come raccordo tra istituzioni, sistema produttivo, ricerca e fornitori di tecnologia, mettendo in comune competenze, infrastrutture e informazioni per la prevenzione e l'anticipazione del rischio.

Il PNRR ha consentito di ampliare significativamente la scala dell'intervento, raggiungendo oltre 450 imprese, erogando più di 900 servizi, finanziando 20 progetti di innovazione e costruendo una rete articolata di laboratori e piattaforme.

La priorità del prossimo triennio non sarà, pertanto, moltiplicare gli asset, ma ampliare la portata delle iniziative e trasformare il patrimonio disponibile in capacità permanenti, accessibili e sostenibili.

Una prima fase dovrà rendere più leggibile l'offerta, attraverso una ricognizione unitaria di laboratori, piattaforme, servizi, competenze e progetti che ne chiarisca destinatari, modalità di accesso, capacità, costi operativi e risultati attesi. Su questa base, servizi e infrastrutture potranno essere integrati in programmi costruiti intorno ai bisogni delle organizzazioni e delle filiere, superando la frammentazione tra singoli progetti. Sanità, automotive e manifattura, spazio e difesa, energia e trasporti possono rappresentare i primi ambiti nei quali combinare assessment, testing, formazione, compliance, simulazione e servizi condivisi.

La fase successiva dovrà consolidare e rendere scalabile il modello, verificando quali attività abbiano generato una domanda continuativa, quali possano essere estese a una platea più ampia e quali richiedano ancora un sostegno pubblico in ragione di benefici sistemici non pienamente remunerabili dal mercato. Integrazione, sostenibilità e misurazione dell'impatto costituiscono quindi le tre condizioni decisive della roadmap: occorrerà passare dal conteggio degli output alla verifica dei cambiamenti prodotti in termini di vulnerabilità ridotte, competenze sviluppate, continuità operativa, capacità di risposta e soluzioni portate sul mercato.

La stessa logica dovrà guidare il trasferimento tecnologico, il cui risultato non si esaurisce nel numero dei progetti finanziati, ma si misura nella capacità di trasformare la ricerca in prodotti, accompagnare le startup verso il mercato e favorire la crescita internazionale delle imprese.

Analogamente, la cooperazione internazionale potrà produrre effetti più duraturi collegando obiettivi istituzionali, capacity building, competenze tecniche e coinvolgimento responsabile del sistema produttivo.

La traiettoria che emerge dal Forum è dunque quella di un Centro orientato a consolidare e mettere a sistema quanto costruito, dimostrandone nel tempo la sostenibilità e il contributo concreto alla resilienza del Paese.