



FORUM CYBER 4.0

I bandi di innovazione di Cyber 4.0

DANIELE VENTURI

COORDINATORE COMITATO SCIENTIFICO E
DI INDIRIZZO CYBER 4.0

PROFESSORE ORDINARIO SAPIENZA
UNIVERSITÀ DI ROMA



CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER



I progetti di innovazione finanziati dal Centro 2021-2023

- **Ricerca Industriale e Sviluppo Sperimentale**
- Alto TRL, breve-media durata
- Premialità per il coinvolgimento di PMI, Organismi di Ricerca, Cyber 4.0
- **2 bandi, cofinanziamento totale 2.2 M€**, intensità variabile sulla base del tipo di attività e la dimensione dell'azienda
- **15 progetti** (2021-2023)
 - 29 aziende coinvolte
 - 80% PMI innovative e start-up
 - Budget totale progetti ca. 7 M€



I progetti di innovazione finanziati dal Centro 2021-2023

**CORE CYBER
SECURITY**

I nuovi bandi 2023-2025

- **5,1 Mln a bando**
- **2 bandi pubblici**, che resteranno aperti per 45 giorni
 - 1 Luglio 2023 – 2,5 Mln
 - Gennaio 2024 – 2,6 Mln
- **Durata 12-18 mesi** – Chiusura inclusa rendicontazione entro Settembre 2025
- **Importi e valore del progetto** – 400k di massimo co-finanziabile per progetto
- **Intensità del contributo variabile** sulla base del tipo di attività e la dimensione dell'azienda

	Micro e piccole imprese	Medie imprese	Grandi imprese
Ricerca Industriale	Fino a 80%	Fino a 60%	Fino a 50%
Sviluppo Sperimentale	Fino a 45%	Fino a 35%	Fino a 25%



Arete Tematiche

- I bandi riguarderanno le seguenti **aree tematiche**:
 - CORE
 - SPACE
 - HEALTH
 - AUTOMOTIVE
- Ciascuna area tematica comprende 3 filoni di ricerca
- Un ringraziamento al Prof. Paolo **Spagnoletti** (LUISS), al Prof. Vincenzo **Tagliaferri** (Tor Vergata), e al Prof. Patrizio **Campisi** (Roma TRE), che hanno contribuito alla definizione delle diverse aree tematiche

- **Intelligenza artificiale.**

- Progetto e sperimentazione di strumenti e metodi basati sull'intelligenza artificiale per lo sviluppo di servizi innovativi per la cybersecurity di imprese e pubbliche amministrazioni, con particolare focus su: cyber intelligence, disinformazione, malware detection, sicurezza e affidabilità delle tecniche di machine learning, business process mining, collezione ed analisi di big data.

- **Blockchain.**

- Sperimentazione della tecnologia blockchain per lo sviluppo di applicazioni industriali distribuite sicure in scenari digitali innovativi che abilitano le interazioni tra cittadini, imprese, pubbliche amministrazioni, e PMI, con particolare focus su: prevenzioni di frodi, tutela della privacy, tokenizzazione ed economia circolare.

- **Crittografia e applicazioni.**

- Progetto e sperimentazione di strumenti e metodi basati sulla crittografia per lo sviluppo di servizi innovativi per la cybersecurity di imprese e pubbliche amministrazioni, con particolare focus su: schemi di cifratura con funzionalità avanzate, sicurezza del software, sicurezza quantistica, cyber intelligence, software testing, vulnerability detection, sicurezza delle reti 5G.

- **Protezione di risorse critiche.**

- Definizione di soluzioni integrate, sviluppo prototipale delle componenti critiche e loro dimostrazione per preservare la disponibilità e l'integrità di elementi critici degli asset spaziali applicati a diversi casi d'uso e tipologie di missioni satellitari, anche con focus su tecniche di classificazione, rilevamento delle anomalie, profilazione del comportamento, e progetto di contromisure in tempo reale.

- **Protocolli di comunicazione satellitari sicuri.**

- Sviluppo e prototipazione di soluzioni crittografiche avanzate, protocolli ed algoritmi specifici per le applicazioni spaziali ed in particolare volte ad incrementare la resilienza dei sistemi di comunicazione contro eavesdropping, jamming e accesso non autorizzato, in diversi scenari applicativi, con sicurezza post-quantum ed anche sfruttando i principi della meccanica quantistica.

- **Sfruttamento dei dati satellitari.**

- Definizione di soluzioni volte all'utilizzo di dati e metadati da sensori spaziali eterogenei per la protezione in tempo reale di asset critici in orbita e a terra (ad esempio infrastrutture critiche), anche attraverso tecniche di intelligenza artificiale e della tecnologia blockchain.

- **Protezione dei dati.**

- Sviluppo ed implementazione di tecnologie volte a preservare la sicurezza e la riservatezza dei dati sensibili in applicazioni di telemedicina digitale avanzate (e.g., digital twins, monitoraggio dei pazienti, etc.), anche attraverso tecniche di intelligenza artificiale e della tecnologia blockchain.

- **Tecnologie sicure per la telemedicina.**

- Sperimentazione e sviluppo di piattaforme tecnologiche hw/sw sicure per l'erogazione di servizi di telemedicina avanzati, con particolare focus su: prevenzione ed il monitoraggio di epidemie (anche attraverso modelli predittivi basati su machine learning), gestione di dispositivi medicali integrati, applicativi software di apprendimento, e gestione del clinical pathway.

- **Anticontraffazione nel settore farmaceutico.**

- Identificazione e sviluppo di soluzioni tecnologiche innovative per l'anticontraffazione e la sicurezza dell'accesso a sistemi e prodotti farmaceutici (dalla produzione, al trasporto, allo stoccaggio, fino alla somministrazione all'utente finale). Le soluzioni dovranno preferibilmente basarsi su piattaforme tecnologiche condivise e scalabili, ed essere compatibili con requisiti di sostenibilità energetica, economica ed ambientale, risultando quindi a basso impatto per un'adozione massiva da parte sia di operatori pubblici che privati.

- **Sicurezza del veicolo.**

- Progettazione e sviluppo di tecnologie volte a preservare la protezione dei veicoli, dei loro occupanti e del traffico circostante, incluse architetture di sicurezza, sistemi di guida autonoma, sensori, attuatori, comunicazioni di bordo, raccolta e analisi di dati finalizzati alla identificazione di possibili minacce, anche attraverso l'utilizzo della tecnologia blockchain.

- **Sicurezza del software e delle stazioni di ricarica.**

- Progettazione e sviluppo di tecnologie volte ad assicurare la sicurezza dei sistemi software installati sui veicoli e delle piattaforme di ricarica, inclusa la certificazione degli aggiornamenti software, l'accuratezza-integrità-resilienza del posizionamento dei veicoli, e la protezione delle stazioni di ricarica dagli attacchi di tipo side channel, anche attraverso l'utilizzo della tecnologia blockchain.

- **Sicurezza della persona.**

- Analisi del comportamento del conducente tramite lo studio di modelli di attenzione e segnali fisiologici (Elettroencefalografia-EEG, Elettrocardiogramma-ECG, etc.), sviluppo di tecniche e algoritmi per la rivelazione di sonnolenza e affaticamento del conducente utilizzando approcci di intelligenza artificiale. Anonimizzazione dei dati relativi.

Colmare il gap tra teoria e pratica!

- **Cifratura con funzionalità avanzate.** Ad esempio:
 - Cifratura omomorfa
 - Cifratura basata su attributi
 - Cifratura funzionale
- **Crittografia in un futuro quantistico.** Ad esempio:
 - Crittografia basata su assunzioni post-quantum
 - Crittografia quantistica
- **Protocolli distribuiti sicuri.** Ad esempio:
 - Prove (interattive) a conoscenza nulla
 - Intersezione privata di insiemi
 - Machine learning e privacy

Thank You!