

Un workshop sulla Cybersecurity di FBK

10 Aprile 2026

Due giorni di confronto su sfide tecniche e prospettive future del Centro: tra intelligenza artificiale, ecosistemi interconnessi e cooperazione tra stakeholder.

Due giornate di lavoro intenso hanno riunito il [Centro per la Cybersecurity](#) della Fondazione Bruno Kessler per un workshop interno dedicato non solo all'allineamento scientifico e strategico ma anche alla condivisione di nuovi spunti di ricerca e buone pratiche per la gestione delle attività progettuali. L'obiettivo è stato duplice: condividere e consolidare le linee di ricerca attive e mettere a fuoco le direttrici future in un contesto tecnologico e geopolitico in rapida evoluzione.

Il Centro, istituito nel 2021, ha registrato una crescita significativa e recentemente strutturato le proprie attività in quattro unità di ricerca dedicate a **crittografia applicata, identità digitale, sviluppo sicuro del software e intelligenza artificiale per la cybersicurezza** nelle Unità di ricerca *Applied Cryptography* ([ALEPH](#)), *Security & Trust* ([ST](#)), *Secure Code Lifecycle for Applications and Networking* ([SaFEWaRe](#)) e *Distributed AI for dependable cyberSecurity* ([DAISY](#)). Questa articolazione riflette un'organizzazione verticale sui principali ambiti scientifici, ma nel corso del workshop è emersa con chiarezza la natura sempre più trasversale delle attività, raccontate anche in una poster session.

Accanto ai filoni consolidati, il lavoro si è infatti esteso alla progettazione sicura di ecosistemi digitali complessi, includendo aspetti di secure-by-design, sviluppo e deployment di sistemi affidabili. Un'attenzione specifica è stata dedicata al risk management e, in particolare, al *threat modeling* come strumento operativo per anticipare vulnerabilità e scenari di attacco.

Parallelamente, sono stati discussi i progressi nell'applicazione dei modelli linguistici (LLM) in ambiti quali privacy, sicurezza e compliance, insieme alle problematiche legate allo sviluppo affidabile e all'integrazione di tecniche di intelligenza artificiale.

Tra i temi tecnici affrontati, hanno trovato spazio anche la sicurezza degli agenti AI, l'analisi dei consumi energetici associati ai meccanismi di protezione e il ruolo degli attacchi side-channel. È emersa l'esigenza di mantenere un forte allineamento tra ricerca fondamentale e problemi emergenti, evitando derive legate all'hype tecnologico e privilegiando l'individuazione di criticità strutturali.

Il workshop ha inoltre evidenziato il ruolo delle collaborazioni. Il Centro opera attraverso diversi joint lab a livello nazionale, tra cui quello con **l'Istituto Poligrafico e Zecca dello Stato**, e collaborazioni con attori come **pagoPA**. A livello territoriale, iniziative congiunte come il laboratorio Cleanse con **Dedagroup** hanno rafforzato il trasferimento tecnologico e il confronto con casi d'uso industriali.

Un'ampia parte della discussione è stata dedicata al panorama degli stakeholder. È stata riconosciuta la molteplicità degli attori coinvolti nel cyberspazio — accademia, istituzioni pubbliche, settore privato e organismi di standardizzazione — e la necessità di meccanismi di cooperazione strutturati che possono essere catalizzati da enti di ricerca come FBK. In particolare, è stata sottolineata l'importanza della condivisione di informazioni sulle minacce cyber (cyber threat intelligence), dello sviluppo di best practice e del coordinamento nelle politiche di sicurezza al fine di andare oltre un approccio difensivo alla cybersecurity e promuovere la resilienza degli ecosistemi digitali.

“L'aumento dell'interconnessione tra sistemi ha introdotto nuove dipendenze e rischi di propagazione a cascata degli attacchi, come nel caso dell'integrazione tra infrastrutture energetiche e sistemi di pagamento per permettere la ricarica delle batterie dei veicoli elettrici. L'intelligenza artificiale ha un ruolo ambivalente: da una parte permette la creazione di tecniche per identificare e mitigare anomalie sempre più sofisticate e dall'altra offre la possibilità agli attaccanti di individuare vulnerabilità e definire strategie per sfruttarle ad una velocità molto maggiore rispetto al passato.” ha spiegato **Silvio Ranise direttore del Centro Cybersecurity di FBK e professore ordinario di Informatica all'Università di Trento**. Continuando: *“Questo impone con ancor maggiore urgenza di passare da un approccio difensivo ad uno basato sulla resilienza capace di minimizzare l'impatto degli attacchi (sempre più probabili) e di ristabilire la normale operatività di servizi ed applicazioni nel minor tempo possibile. Il quantum computing si profila come un ulteriore fattore di rottura rispetto allo status quo della cybersecurity in quanto promette di azzerare il livello di protezione offerto da alcune primitive crittografiche comunemente usate (come ad esempio RSA) entro pochi anni e questo richiede di cambiare l'infrastruttura crittografica che garantisce la riservatezza e l'integrità delle transazioni che avvengono ogni giorno su Internet: uno sforzo ingegneristico ed organizzativo enorme che richiede tempo, risorse e competenze da parte di tutti gli stakeholder coinvolti. Il ruolo del Centro non è solo quello di identificare i problemi tecnici e le relative soluzioni ma anche di sensibilizzare tutti gli stakeholder coinvolti affinché sviluppino consapevolezza dei rischi, adottino i controlli di sicurezza opportuni e gestiscano al meglio il “rischio umano” connesso ovvero costruiscano una cultura della sicurezza diffusa e condivisa non solo all'interno della singola organizzazione ma anche rispetto a fornitori di servizi e librerie sviluppate da terze parti (la cosiddetta sicurezza della supply chain)”*.

Nel quadro europeo, è stata discussa la rilevanza dell'**European Cyber Security**

Competence Centre (ECCC), con il suo ruolo nel coordinare investimenti in ricerca, tecnologie e sviluppo industriale, rafforzare la competitività del settore europeo e sostenere l'adozione su larga scala di soluzioni sviluppate in Europa. Attraverso la rete dei National Coordination Centres — con l'Agenzia per la Cybersicurezza Nazionale come nodo italiano — l'ECCC facilita la cooperazione tra industria, accademia e istituzioni pubbliche, gestendo anche programmi di finanziamento dedicati come il Digital Europe Programme e Horizon Europe.

Sul piano operativo, sono emersi alcuni principi guida per lo sviluppo di soluzioni di cybersicurezza. È stata ribadita la necessità di progettare servizi **facilmente integrabili nelle infrastrutture esistenti, tenendo conto di vincoli reali e garantendo proprietà di affidabilità**.

L'espansione della superficie di attacco è stata considerata un elemento strutturale, da affrontare con tecniche per la resilienza piuttosto che con approcci reattivi.

Un ulteriore punto ha riguardato il **bilanciamento tra sicurezza e risorse**: i meccanismi di protezione hanno un costo computazionale ed energetico e possono incidere sulle prestazioni, rendendo necessario un approccio consapevole e ottimizzato. In ambito AI, è stato sottolineato come i modelli linguistici non costituiscano soluzioni autonome: il loro utilizzo richiede integrazione contestuale nelle architetture software e robuste strategie di validazione. La definizione di ground truth affidabili è stata identificata come una delle criticità aperte.

Il workshop ha quindi consolidato una linea di sviluppo chiara: rafforzare l'integrazione tra ricerca di base ed applicazioni, mantenendo un orientamento concreto ai problemi e alle condizioni operative reali, in un contesto caratterizzato da una continua e rapida coevoluzione tra tecnologie e minacce.

LINK

<https://magazine.fbk.eu/it/news/un-workshop-sulla-cybersecurity-di-fbk/>

TAG

- #ai agents
- #aleph
- #crittografia applicata
- #cyberattacchi
- #cybersicurezza
- #cyberspazio
- #daisy
- #dedagroup
- #identità digitale
- #intelligenza artificiale
- #ipzs
- #jointLab
- #llm
- #pagopa

- #safeware
- #secure-by-design
- #sicurezza
- #ST
- #threat modeling

AUTORI

- Giovanna Rauzi