FONDAZIONE BRUNO KESSLER
MAGAZINE

A workshop on FBK's Cybersecurity

April 10, 2026

Two days of discussions on technical challenges and future perspectives of the Center, spanning artificial intelligence, interconnected ecosystems, and stakeholder collaboration.

Two days of intensive work brought together the Fondazione Bruno Kessler Center for Cybersecurity for an internal workshop dedicated not only to scientific and strategic alignment but also to sharing new research insights and best practices for managing project activities. The objective was twofold: to share and consolidate active lines of research and to focus on future directions in a rapidly evolving technological and geopolitical context.

The Center, established in 2021, has experienced significant growth and has recently structured its activities into four research units dedicated to **applied cryptography, digital identity, secure software development, and artificial intelligence for cybersecurity**: *Applied Cryptography* (ALEPH), Security & Trust (ST), *Secure Code Lifecycle for Applications and Networking* (SaFEWaRe)HYPERLINK "https://safeware.fbk.eu/", and Distributed AI for Dependable Cybersecurity (DAISY).This structure reflects a vertical organization around the main scientific areas, but during the workshop the increasingly cross-cutting nature of activities clearly emerged, also highlighted in a poster session.

In addition to established research areas, the work has expanded to the secure design of complex digital ecosystems, including aspects of secure-by-design development and the deployment of reliable systems. Particular attention was paid to risk management and, specifically, to *threat modeling* as an operational tool to anticipate vulnerabilities and attack scenarios. At the same time, progress in the application of large language models (LLMs) in areas such as privacy, security, and compliance was discussed, along with issues related to the reliable development and integration of artificial intelligence techniques.

Among the technical topics addressed were the security of AI agents, the analysis of energy consumption associated with protection mechanisms, and the role of side-channel attacks. The need emerged to maintain strong alignment between fundamental research and emerging challenges, avoiding drift driven by technological hype and instead prioritizing the identification of structural criticalities.

The workshop also stressed the importance of collaboration. The Center operates through several joint labs at the national level, including one with **the national mint, the Istituto Poligrafico e Zecca dello Stato,** and collaborates with organizations such as **pagoPA**. At the regional level, joint initiatives such as the Cleanse laboratory with **Dedagroup** have strengthened technology transfer and engagement with industrial use cases.

A significant portion of the discussion focused on the stakeholder landscape.
The multiplicity of actors involved in cyberspace—academia, public institutions, the private sector, and standardization bodies—and the need for structured cooperation mechanisms that can be catalyzed by research organizations such as FBK were emphasized. In particular, the importance of sharing cyber threat intelligence, developing best practices, and coordinating security policies was emphasized, with the aim of moving beyond a purely defensive approach to cybersecurity and promoting the resilience of digital ecosystems.

"The increase in interconnection between systems has introduced new dependencies and risks of cascading attacks, as seen in the integration between energy infrastructure and payment systems that enable electric vehicle charging. Artificial intelligence plays an ambivalent role: on one hand, it enables techniques to identify and mitigate increasingly sophisticated anomalies; on the other, it allows attackers to identify vulnerabilities and develop exploitation strategies at a much higher speed than in the past," **Silvio Ranise, Director of the FBK Center for Cybersecurity and Full Professor of Computer Science at the University of Trento, xplained**. He continued: "*This creates an even greater urgency to move from a defensive approach to one based on resilience, capable of minimizing the impact of attacks—which are increasingly likely—and restoring normal operations as quickly as possible. Quantum computing is emerging as an additional disruptive factor, as it could undermine the protection offered by widely used cryptographic primitives such as RSA within a few years. This will require transforming the cryptographic infrastructure that ensures the confidentiality and integrity of everyday Internet transactions—a vast engineering and organizational effort requiring time, resources, and expertise from all stakeholders. The Center's role is not only to identify technical challenges and solutions but also to raise awareness among stakeholders so they develop risk awareness, adopt appropriate security controls, and better manage human risk, fostering a widespread and shared culture of security, including across supply chains."*

Within the European framework, the relevance of the **European Cybersecurity Competence Centre (ECCC) was discussed,** particularly its role in coordinating investments in research, technologies, and industrial development, strengthening the competitiveness of the European sector, and supporting the large-scale adoption of solutions developed in Europe. Through the network of National Coordination Centres—with the Agenzia per la Cybersicurezza Nazionale serving as the Italian node—the ECCC facilitates cooperation among industry, academia, and public institutions, also managing dedicated funding programs such as the Digital Europe

Programme and Horizon Europe.

At the operational level, several guiding principles for the development of cybersecurity solutions emerged. The need to design services that **can be easily integrated into existing infrastructure was reiterated, taking into account real-world constraints and ensuring reliability.** The expansion of the attack surface was recognized as a structural factor to be addressed through resilience-oriented approaches rather than reactive ones.

Another key point concerned the **balance between security and resources:** protection mechanisms carry computational and energy costs and can affect performance, making a deliberate and optimized approach essential. In the field of AI, it was emphasized that language models do not constitute standalone solutions; their use requires contextual integration into software architectures and robust validation strategies. The definition of reliable ground truth was identified as one of the key open challenges.

The workshop thus consolidated a clear development path: strengthening the integration between fundamental research and applications, maintaining a practical focus on real-world problems and operating conditions, in a context characterized by the continuous and rapid coevolution of technologies and threats.

PERMALINK

https://magazine.fbk.eu/en/news/a-workshop-on-fbks-cybersecurity/

TAGS

- #ai agents
- #aleph
- #artificialintelligence
- #crittografia applicata
- #cyber attacks
- #cybersecurity
- #cyberspace
- #cyberspazio
- #daisy
- #dedagroup
- #digital identity
- #ipzs
- #jointLab
- #llm
- #pagopa
- #safeware
- #secure-by-design
- #security
- #ST
- #threat modeling

AUTHORS

- Giovanna Rauzi