Cybersecurity: Between Spies, Spooks, and Hackers

May 23, 2025

With increasingly sophisticated cyberattacks, the rise of AI-powered cybercrime, and evolving European regulations, digital security has become a global and collective challenge.

In an era where cyberattacks have become part of everyday news, cybersecurity can no longer be seen merely as a technical issue: it is a collective and systemic challenge.

This was the central theme of the event "*Cybersecurity: Between Spies, Spooks, and Hackers*," held at the 2025 Trento Festival of Economics. The panel featured **Silvio Ranise, Director of the Center for Cybersecurity at Fondazione Bruno Kessler and Full Professor at the University of Trento**, along with other leading experts: **Emilio Gisondi, CEO of Tinexta Defence; Yuri Giuseppe Rassega, Head of Cyber Security at Enel; Fabio Scacciavillani, Founder of Nextperience Scf; and Giovanni Andrea Toselli, Chairman and CEO of PwC Italy.**

The discussion, moderated by **Simone Casalini, editor of Il T Quotidiano**, highlighted the ongoing transformations in the digital security landscape—an increasingly sensitive topic that affects every aspect of our lives, from data protection to personal freedom.

Ranise (FBK) pointed out three main challenges that hinder effective protection of digital systems: **the asymmetry between attack and defense, exacerbated by the malicious use of artificial intelligence; the extreme interconnectedness of digital ecosystems; and the complexity of identifying those responsible for cyberattacks.** Addressing these issues requires action on technical, organizational, and human levels.

"It is essential that education in this field begins as early as elementary school, to build a digitally aware culture," Ranise explained during his talk. "At the same time, it is crucial to raise awareness among all workers: cybersecurity is not just a matter for specialists—it is a shared responsibility. *Every click, every email opened, every password chosen can become an entry point for an attack. Companies must invest in continuous training to ensure everyone*

understands the potential risks individual behaviors can pose to the overall security posture of the organization."

The topic is a delicate one, and the speakers brought different experiences and perspectives—all converging toward the same direction: cybersecurity affects people's daily lives, and it is vital to act collectively.

According to **Emilio Gisondi, CEO of Tinexta** Defence—a private company that has entered the field of national security—the way forward is to build **national technological sovereignty,** freeing ourselves from dangerous global dependencies in technology.

Education in data security and usage—for all citizens and especially for younger generations, who still seem relatively unaware of the issue—is key to a safer digital world, said **Giovanni Andrea Toselli, Chairman and CEO of PwC Italia.** This must be accompanied by a **major system-wide effort.** The same systemic approach was advocated by **Yuri Giuseppe Rassega, Head of Cyber Security at Enel**, who suggested it could **secure entire supply chains by optimizing investments.** There is still a long way to go: while awareness among citizens and businesses has grown, it is not yet sufficient—especially since the risk is constant and continues to evolve.

A medium-to-large company can face 50,000 intrusion attempts per day, while a company like **Poste Italiane may experience up to 500,000**, according to **Fabio Scacciavillani, economist and Founder of Nextperience Scf.** The problem, therefore, is vast—and it's a mistake to think it only affects "*others.*"

The event ultimately underscored the complexity of the issue: cybersecurity is not merely a technological challenge, but a social, regulatory, and organizational one—demanding a **collective commitment from public institutions, private companies, research organizations, and citizens alike.**

AUTHORS

- Giovanna Rauzi