EISS 2026 - Panel Talk Proposal: Quantum-Resilient SATIN and European Digital Sovereignty

Panel: Digital Transformations in the Information Age: Cyber, Digital, and AI

Gürkan Gür
Zürich University of Applied Sciences (ZHAW)
Winterthur, Switzerland

Europe's pursuit of digital sovereignty has become a defining priority amid geopolitical tensions that increasingly threaten the stability and independence of digital infrastructure. Secure connectivity—spanning terrestrial, aerial, and space domains—is now a strategic asset rather than a technical enabler. This proposal positions post-quantum-ready integrated Space–Aerial–Terrestrial Networks (SATIN) as a crucial component of Europe's technological autonomy towards the future. Drawing on emerging work in post-quantum cryptography (PQC) for aerial and space systems, the talk frames SATIN not only as a connectivity substrate but as a geopolitical capability that enhances resilience against external dependencies, supply-chain vulnerabilities, and future quantum-enabled adversaries.

In parallel, Europe faces an increasingly complex landscape of security and defense challenges involving satellites and unmanned aerial systems (UAS). Satellites have become prime targets for cyber intrusion, jamming, spoofing, and interference with telemetry or command links. Their central role in navigation, communication, and surveillance makes them attractive for hybrid disruptions during periods of political instability[1]. Similarly, UASs (aka drones) are being exploited for reconnaissance, critical-infrastructure disruption, and below-threshold attacks.Quantum-safe SATIN architectures directly address the need for secure and resilient communication mechanisms by hardening command-and-control links, improving robustness against signal manipulation, and enabling secure coordination among space and aerial assets, not just for today, but for the future as well.

The talk further argues that European strategic autonomy depends not only on adopting PQC but also on controlling how these mechanisms are realized, evaluated, validated, integrated, and deployed. To achieve sovereignty, Europe must develop software and hardware pipelines, independent testbeds, and simulation environments capable of modeling PQC-induced delays, satellite–UAS interoperability challenges, and multi-layer network performance under stress. Without these capabilities, Europe risks relying on external solutions and validation ecosystems that may not align with its long-term security and industrial priorities.

In conclusion, this panel contribution presents quantum-resilient SATIN as a decisive enabler of European digital future-proof sovereignty, strengthening secure communications, resilient critical infrastructure, and reinforcing Europe's leadership across satellite, drone, and terrestrial networking domains. It invites policymakers, researchers, and industry stakeholders to view SATIN as both a technological and strategic pathway for navigating an increasingly contested digital landscape.

[1]"Russia intercepts key European satellites - Sensitive information at risk as Moscow expands 'hybrid warfare' campaign into space", https://www.telegraph.co.uk/world-news/2026/02/04/russia-intercepts-key-european-satellites/, 04.02.2026