

ADVANCED CYBERSECURITY & RESILIENCE IN HUMAN-CENTRIC NETWORKS

Supervisor Name: Prof. Dr. Ana Fernández Vilas

Email: avilas@uvigo.gal

Research Group: Information & Computing Lab

The Information & Computing Lab (Iclab) is a research group with over 12 years of experience that aim to foster experimentation and development at the crossroads of data analysis techniques and ICTs, which serve as key drivers of the emerging digital economy and society. We have four main areas of expertise: (1) decentralized learning, including decentralized federated learning, continual learning and split learning; (2) privacy & security, including Byzantine-robustness, coded decentralized computing and differential privacy; (3) IoT/C2E computing, including Decentralized federated learning over IoT and Cloud-to-Edge computing; and (4) quantum networks, including Quantum Internet, Quantum Key Distribution (QKD) and Quantum security.

Further information can be found at our webpage (<https://iclab.uvigo.gal>): including comprehensive details about publications members, ongoing research projects, and cooperation and knowledge transfer projects.

Keywords: Zero-Trust Networking | Agentic AI Threats | Quantum-Safe Networking | Cyber - Physical Network Resilience

Research Focus:

As 6G evolves, we are transitioning toward AI-native, human-centric ecosystems that fundamentally integrate communications, sensing, and computation (ISAC). In these hyper-connected environments, the semantic integrity and meaning of data become as critical as the physical infrastructure itself. However, the deep integration of distributed Agentic AI and cyber-physical systems introduces a new frontier of complex vulnerabilities. To support next-generation industrial operations and sensitive human-centric services, we must move beyond reactive security and embed end-to-end resilience directly into the network's architectural foundation.

We are seeking MSCA proposals that address these multifaceted challenges through a robust Zero-Trust security framework designed to maintain operational continuity even under sophisticated persistent threats. This research is pivotal for establishing Communication Sovereignty, ensuring that

critical network infrastructures remain autonomous, secure, and under verifiable control. Candidates are encouraged to define their own research trajectory, but we are particularly interested in projects that explore the following strategic areas:

- **Defending AI and ISAC against Agentic Threats:** We need to investigate how to protect semantic communications and human-swarm interactions from autonomous AI-driven attacks. This includes developing proactive defenses against Adversarial Machine Learning (AML), mitigating data poisoning in distributed training datasets, and ensuring the physical-layer security of sensing data against advanced sensor spoofing in critical infrastructures
- **Quantum-Safe Networks & Hybrid Cryptography:** While QKD offers theoretical unconditional security, it faces significant hurdles in key generation rates and scalability for massive deployments. We are looking for hybrid strategies that seamlessly orchestrate QKD with PQC algorithms to create a quantum-safe scalable shield for human-centric networks.
- **Cyber-Physical Resilience:** This area focuses on using AI-driven predictive network slicing not just for resource isolation, but to enforce dynamic security and Quality of Service (QoS) profiles tailored to specific application needs. Furthermore, research should define fail-safe protocols that ensure "graceful degradation" of physical systems during severe cyber-kinetic disruptions, ensuring that human operators remain effectively in-the-loop to prevent catastrophic failures.