Cybersecurity @ LINCS

Francesca Bassi

LINCS retreat 2025

December 17, 2025

Cybersecurity @ LINCS, so far

Fragmented efforts

- Cybersecurity not seen as a structuring theme in the last decade
- Over the years, LINCS has addressed cybersecurity topics
  - Several recent seminars on cybersecurity topics (Side-channel attacks by O. Rioul, DDos attacks by R. Khatoun, Cyber-resilience by R. Dagnas)
  - Workshop in 2025 on AI and Cybersecurity
  - Members actively working in cyber (Joaquin, Gregory, Francesca)
- Efforts have however been sporadic and uncoordinated
- Lack of a unified scientific strategy

Can cybersecurity inspire ambitious research directions @ LINCS?

- Let's discuss together

Dynamic networks & Trust

Distributed and highly dynamic networks

- Modern networking paradigms based on SDN and virtualization
- Networks that connect nodes across different domains: edge computing, IoT, vehicular networks...
- Expanded attack surfaces + trust and authentication challenges across domains

Research challenges

- Define (mathematically) and quantify trust in dynamic networks
- How to establish trust protocols across multiple domains

Post-quantum security

Quantum threats

- Quantum computing threatens asymmetric cryptography
- Migration towards quantum-safe primitives has impact on performance (memory and complexity)
- How to handle migration when networks are made of long-lived devices? (e.g., cars)

Research challenges

- Balance complexity, latency, memory requirements in protocols
- Hybrid schemes (legacy + post-quantum)
- Integrate quantum in the security (resilience of quantum internet)

Cyber-resilience

Failures are inevitable

- Prevention and protective measures target known threats/events, but this cannot prevent the unknown (both attack and defense are dynamic)
- Systems needs to be designed to be adaptive as to recover (and learn)

Research challenges

- How to measure and quantify cyber-resilience
- How the concept of resilience evolves in the light of quantum threat?
- Can we use AI (gen) to increase cyber-resilience?

AI & cybersecurity

AI for security

- Real-time intrusion and anomaly detection: how to do this effectively / while preserving privacy?
- How to defend against adversarial attacks, where attacker nodes have learned a plausible behavior?

Security of AI

- Learning over networks: how to secure the distribution across nodes?
- Trust again: if the AI model is a node in a network, how to ensure it is trustworthy?

Privacy

- Computing over private data (e.g. learning over private data)
- Storing and retrieving private data
- ...