



PANEL #1

**LISBON
2025**

NexTech 2025

Dynamics in Social Networks - Scalable Monitoring



PANEL #1

LISBON
2025

Dynamics in Social Networks – Scalable Monitoring

Digital dependency: overreliance on online activities

Digital divide: inequality in information, resources, and opportunities

Empathy erosion: declining understanding of the feelings of others

Aloofness: being distant, reserved, and unwilling to be friendly or involved

Phubbing: neglecting a person in favor of smartphone

Virtual intimacy: profound emotional closeness; AI-powered virtual companions

Cyber-bullying: aggressively dominate, or intimidate others

Digital burnout: mental, emotional, and physical exhaustion



CONTRIBUTORS

LISBON
2025

Moderator

Prof. Dr. Mart Verhoog, IU International University of Applied Sciences, Germany

Panelists

Dr. Erik Hieta-aho, VTT, Technical Research Centre of Finland, Finland

Prof. Dr. Mart Verhoog, IU International University of Applied Sciences, Germany

Prof. Dr. Sung-Ho Kim, Korea Advanced Institute of Science and Technology, South Korea

Dr. Rainer Falk, Siemens AG, Foundational Technologies, Germany

Prof. Dr. Petre Dini, IARIA



Panelist Position

LISBON
2025

Dynamics in Social Networks – Scalable Monitoring

- **Information diffusion: facts and emotions spread**

Explanation: Networks spread not only news, but also moods and stress.

Example: During the pandemic, fear and solidarity hashtags both spread widely.

- **Influence dynamics: empathy loss, phubbing & FOMO**

Explanation: Online influence drives FOMO and weakens empathy, especially among youth.

Example: Teens feel pressure from influencers to stay online constantly; some countries now discuss stricter limits.

- **Community detection: inclusion vs. digital exclusion**

Explanation: Communities online can empower, but also exclude vulnerable groups.

Example: Elderly people or those without broadband access are cut off from key discussions.

- **Anomaly detection: early signals of cyber-bullying & burnout**

Explanation: Monitoring can reveal harmful patterns before they escalate.

Example: Sudden spikes in aggressive language in school forums may signal bullying.

- **Temporal evolution: tipping points once social thresholds are crossed**

Explanation: Social problems often remain hidden until they suddenly erupt.

Example: Digital burnout builds slowly, then leads to sudden dropout or withdrawal.



Mart Verhoog
IU International
University



Panelist Position

LISBON
2025

Opportunities & Risks of Monitoring

- Opportunities

Early-warning for misinformation, hate speech, burnout

Explanation: Monitoring offers predictive insights into unhealthy dynamics.

Example: Tracking rising conspiracy hashtags could trigger early counter-information.

Making social dynamics visible

Explanation: Data can highlight the unseen spread of moods and behaviors.

Example: Platforms could show how optimism or stress clusters travel between groups.

- Risks

Over-surveillance & erosion of trust

Explanation: Excessive monitoring may undermine freedom and privacy.

Example: Employees who feel constantly tracked may disengage and lose trust in their organization.

Who defines what is “normal” vs. “anomalous”?

Explanation: The criteria for anomalies reflect cultural and political choices.

Example: A protest hashtag might be seen as activism in one context, extremism in another.

- Balance Question

Monitoring should strengthen resilience – not deepen mistrust.

Explanation: The goal must be empowerment, not control.

Example: Wellbeing alerts that help users manage screen time without shaming or punishing.



Mart Verhoog
IU International
University



Panelist Position

LISBON
2025

Data source values are up to the users

- Pieces of marginal information
 - More is better for structure learning. But how?
 - Anomaly in marginal information
- Compatibility between knowledge structures
 - Check information discrepancy between data sets
- Questions and learning
 - Raising issues and questions for structure learning
 - Questions crucial for monitoring network status
- Efficient learning
 - All-things input vs selected input
 - How to find key factors for efficient learning and/or monitoring?



Sung-Ho Kim
KAIST
South Korea



Panelist Position

LISBON
2025

Cybersecurity for all – Industry and Individuals

- **New Technologies impact on cybersecurity high**
 - Quantum Computers and technologies
 - AI/ML
- Cybersecurity regulatory support necessary for timely reaction to accelerating technologies.
- **Post-Quantum cryptography** transition substantially impacts industry and critical infrastructure entities.
- AI models and their development accelerating
 - Severe impact on integrity of social media and the internet.



Erik Hieta-aho
VTT
Finland



Panelist Position

LISBON
2025

■ Fight and annihilate malicious coalitions

- Social media users (innocent followers)
- Agents in an agentic (autonomous (?) behavior & hallucinations)
- Hackers (on purpose, bad players), Botnets, etc.
- Well-known example: DDoS

■ Monitor and delay (prevent) percolation points

- Anticipatory percolation points
- Prevention of percolation points
- Detect early igniters of to-be percolation points
- Detect last actors before percolation points

Fighting Fire with Fire: Developing AI-enhanced Methodologies to Combat AI-enhanced Cognitive Threats

https://www.iaria.org/conferences2025/filesIARIACongress25/Keynote_NitinAgarwal_FightingFireWithFire.pdf

Prof. Dr. Nitin Agarwal, Jerry L. Maulden-Entergy Chair and Donaghey Distinguished Professor of Information Science, University of Arkansas - Little Rock & Faculty Fellow, International Computer Science Institute, University of California, Berkeley, USA



Petre Dini
IARIA
USA/EU

■ Improving

Resiliency
Robustness
Predictability
Survivability

■ Mechanisms

Detection
Prevention & mitigation
Escalation control & containment
Social/physical networks analogy



Panelist Position

LISBON
2025

Detection Mechanisms

These aim to **identify critical nodes/edges** before percolation cascades into escalation.

- **Percolation Centrality:** Extends betweenness centrality by measuring how often a node lies on the percolation paths; highlights escalation “hubs.”
- **K-core / K-shell Decomposition:** Identifies tightly connected subgroups that can ignite coalition percolation.
- **Spectral Methods:** Use eigenvalue gaps of adjacency or Laplacian matrices to detect vulnerable clusters.
- **Dynamic Early-Warning Indicators:** Monitor for rising variance, correlation, or lag in activity (critical slowing down); signals that escalation thresholds are near.
- **Community Evolution Tracking:** Detects when benign communities merge into larger, potentially destabilizing coalitions.
- **Multilayer Cross-Monitoring:** Correlates physical (infrastructure load) and social (information diffusion) layers to identify compound percolation risks.



Petre Dini
IARIA
USA/EU

Prevention & Mitigation Mechanisms

These mechanisms are aimed at **breaking or slowing percolation cascades** once hotspots are identified.

- **Edge Rewiring or Weakening:** In social networks, introducing “noise” edges or weakening strong ties to disrupt coalition reinforcement.
- **Immunization Strategies:** Selectively “inoculate” nodes (informationally or with safeguards) based on high percolation centrality.
- **Decoy Communities:** Create attractive but controlled coalitions to absorb and dilute escalation energy.
- **Load Balancing in Physical Networks:** Redistribute flows to prevent cascading overload (analogous to slowing rumor/attack spread in social systems).
- **Temporal Firebreaks:** Slow information propagation using throttling, rate-limits, or moderation to prevent synchronous coalition formation.
- **Adaptive Governance Agents:** Deploy monitoring AI agents that intervene with fact-checking, counter-narratives, or rerouting at early escalation points.



Panelist Position

LISBON
2025

Escalation Control & Containment

If percolation starts, focus shifts to limiting systemic damage..

- **Cascading Failure Dampers:** In physical networks (e.g., power grids), trip-switches or circuit breakers limit the escalation chain.
- **Influence Containment Policies:** Temporarily isolate or de-amplify influential coalition leaders in digital platforms.
- **Layered Defense-in-Depth:** Combine physical resilience (redundancy, segmentation) with social countermeasures (alternative narratives, community support).
- **Feedback Suppression:** Break reinforcing loops in escalation (e.g., social recommendation systems amplifying bad coalitions).



Petre Dini
IARIA
USA/EU

Analogy Across Domains

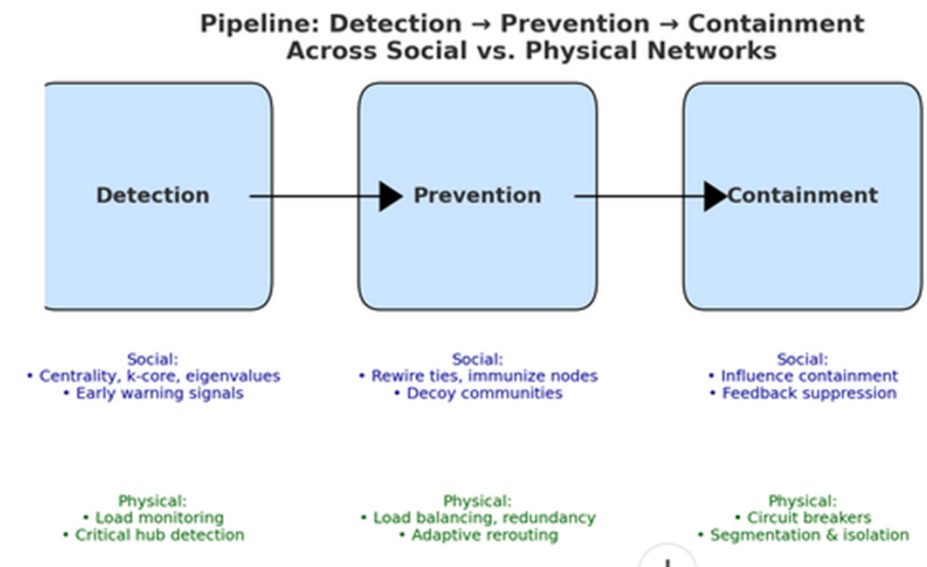
- **Social Networks:** Percolation points are typically opinion leaders or bridge nodes connecting multiple groups.
- **Physical Networks:** They are critical infrastructure hubs or bottleneck links where overload triggers cascades.

The mathematics of percolation is similar, but interventions differ:

- In social systems → information shaping, coalition dilution, influence moderation.
- In physical systems → redundancy, rerouting, controlled shutdowns.

Summary

- Detect early (centrality, eigenvalues, variance)
- Break coalitions (rewire, immunize, dilute)
- and
- Damp escalation (containment, redundancy, suppression)





Panelist Position

LISBON
2025

- **Cybersecurity for Industrial Systems**

- Industrial systems need a security design that address the relevant security objectives and respect side conditions for the specific environment (e.g., lifetime, real-time, functional safety, usability).
- The industrial security standard IEC62443 is applied in different verticals. The responsibilities of the different roles (system operator, integrator, component manufacturer) are distinguished.

- **Cybersecurity Demand**

- Upcoming technologies, including PQ crypto, **AI/ML, AR/VR**, IoT, TSN, 5G/6G, edge computing, virtualization
- **Industrial Metaverse and digital twins – combining the real and the digital worlds**
- Cybersecurity increasingly driven by regulatory requirements
- Usability of security, security by default, security by design, zero trust security



Dr. Rainer Falk
Siemens AG



Open

LISBON
2025

STAGE IS YOURS