Theme
Cybersecurity Resilience Challenges

Topics: Resilience frameworks, Human factors, Adaptive security, Quantum-era risks

Keywords: Threat intelligence, Zero trust architecture, Critical infrastructure protection, Supply chain security, AI-driven cyber defense, Regulatory compliance / data sovereignty

PANEL #1

BARCELONA
2025

Moderator

Prof. Dr. Alexander Lawall, IU International University of Applied Sciences

Panelists

Niklas Lindskog, Ericsson, Sweden

Prof. Dr. Aspen Olmsted, Wentworth Institute of Technology, USA

Co-Founder Ali Recai Yekta, Yekta IT GmbH, Germany

Prof. Dr. Yuichi Kaji, Nagoya University, Japan

Timm Bostelmann, FH Wedel (University of Applied Sciences), Germany

Chair Introduction

Barcelona 2025

Def. (NIST SP 800-172): „The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.“

Alexander Lawall

IU International University of Applied Sciences

Cybersecurity Resilience Challenges

- Why resilience matters: sophisticated threats, interdependent systems, geopolitical risks
- From prevention to resilience: anticipate, detect, withstand, recover, evolve
- Themes: Resilience frameworks, Human factors, Adaptive security, Quantum-era risks

Source: https://www.researchgate.net/publication/344470267/figure/fig1/AS:996912564035585@1614693885639/Cyber-Resilience-Lifecycle.png

Chair Introduction

Barcelona 2025

Key Challenge Domains

- Threat intelligence – predictive vs. reactive
- Zero Trust Architecture – scalable reality or idealized vision?
- Critical Infrastructure Protection – healthcare, energy, transport, etc.
- Supply Chain Security – transparency & SBOMs after SolarWinds/Log4j
- AI-driven Defense – automation, adversarial ML risks
- Regulatory Compliance & Data Sovereignty (EU CRA) – fragmentation vs. protection

Alexander Lawall

IU International University of Applied Sciences

Chair Introduction

Barcelona 2025

(Possible) Discussion Areas

- Are resilience frameworks guiding practice or just compliance tools?
- Can AI ever be trusted as an autonomous defender?
- How urgent is migration to post-quantum cryptography?
- What works better: training, awareness, or cultural transformation?

Alexander Lawall

IU International University of Applied Sciences

Panelist Position

BARCELONA 2025

Niklas Lindskog
Ericsson Research

- Utilizing unintended information leakage for security - Opportunities
  - Devices leak unintended information
    - Regularly used for attacks (both in academia and real world)
      – e.g., breaking crypto keys and reverse-engineering software.
  - How can we turn this drawback into an advantage and strengthen resilience against attacks?
  - Potential sources of information:
    - Power consumption
    - Component activations / utilization
    - Performance counter and events
    - Internal traffic patterns
  - What if we utilize these in combination with conventional security - added value
    - Pros:
      - Can detect patterns hidden from conventional security protection
      - Can already be measured by hardware - or measured by retrofitted components
      - Compatible with user privacy – data is not revealed in process

Panelist Position

BARCELONA 2025

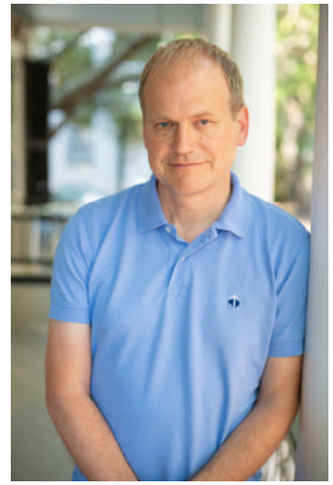
Niklas Lindskog
Ericsson Research

- Utilizing unintended information leakage for security – Challenges and next steps
  - Challenges to be solved:
    - Sampling rate
      - Focus on general patterns rather than single instructions
    - How to handle complex software
      - Collaborate with “classic” virus scanners.
    - Avoid that attacker can utilize unintended information leakage for malicious purposes
      - Capability management
      - Detection of unauthorized monitors
    - Main challenge for large-scale adaptation - how do we know what is desirable behavior?
  - Future devices - From app-based to agentic approach
    - Technological vision – user devices go from app-based to agent-based
      - The device agent(s), not the apps, understands what the user wants to do
    - User creates own work-flows and instructs device with tasks
      - Agents extracts user goals and context.
    - Possibility to go from “is this normal?” to “is this what the user wants?”
      - Determine if measured behavior aligns with user’s goal

Panelist Position

BARCELONA 2025

Cybersecurity resilience challenges and secure software development are fundamentally intertwined because the quality and security of the software itself is a primary determinant of an organization's overall cyber resilience.



Aspen Olmsted, Ph.D
Wentworth Institute of Technology

Panelist Position

BARCELONA 2025

Cyber Resilience Challenge

Pervasive Vulnerabilities (the primary cause of breaches)

Supply Chain Risk (from third-party and open-source components)

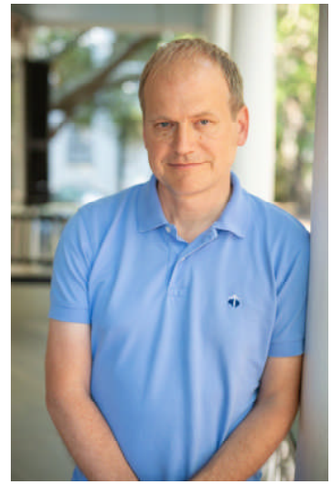
Downtime and Recovery (failure to continue operations after an attack)

Secure Software Development Response (SSDLC)

"Shift Left" Security: Integrating practices like **threat modeling** and **security requirement definition** into the earliest phases (planning/design) to prevent flaws rather than fixing them later.

Software Composition Analysis (SCA): Using tools to automatically scan and manage **Software Bills of Materials (SBOMs)** to identify and patch known vulnerabilities in third-party libraries.

Secure Architecture Design: Implementing **fail-safe** and **self-healing** mechanisms, **redundancy**, and **immutable infrastructure** to ensure the software can quickly restore or continue critical functions.



Aspen Olmsted, Ph.D
Wentworth Institute of Technology

Panelist Position

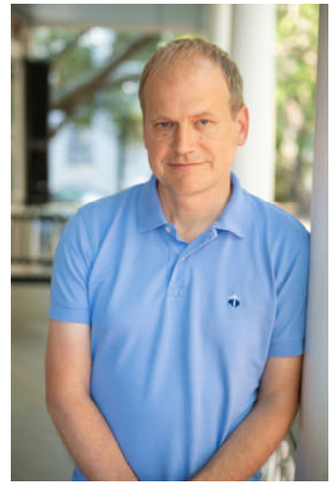
BARCELONA 2025

Evolving Threats (new attack vectors and zero-days)

Delayed Patches and Updates (leaving systems exposed)

Continuous Security Testing: Employing **Static Application Security Testing (SAST)**, **Dynamic Application Security Testing (DAST)**, and **Penetration Testing** to continuously validate the software's security posture against emerging threats.

Secure Deployment & Maintenance: Automating the delivery of **security updates** (patch management) and **secure configuration management** throughout the product's entire lifecycle.



Aspen Olmsted, Ph.D
Wentworth Institute of Technology

Panelist Position

BARCELONA 2025

Effective cyber resilience depends on fundamentals: asset transparency, domain-specific protocol coverage, and strong feature- and detection-engineering beat tool complexity.

Ali Recai Yekta
Yekta IT GmbH

Panelist Position

BARCELONA 2025

Critical Infrastructure Protection

- Asset Inventory: Foundation First
  - Start with Excel/CSV before expensive tools – document assets, criticality, dependencies, protocols. Tool integration later.
- Asset Criticality: Not Everything is Equal
  - Classify by impact (safety, operations, compliance). Focus resources on crown jewels, accept risk on low-impact assets.
- Logging: Quality Over Quantity
  - Log detection-relevant events only. Design logging during architecture phase, not as afterthought. ATT&CK is a good source
- IDS/IPS: IT-IDS != OT-IDS
  - Does it support YOUR OT protocols (Modbus, DNP3, S7, OPC-UA)? Test with real traffic before procurement.
- Signatures: Relevance Over Volume
  - 50 relevant rules beat 10,000 generic ones. Tune ruleset to your infrastructure, disable noise.

Ali Recai Yekta
Yekta IT GmbH

Panelist Position

BARCELONA 2025

AI for Attacker

Realistic Use Cases

- Content Automation: Spear-phishing, deepfakes, social engineering in native languages
- Reconnaissance & Tooling: Script/PoC generation, infrastructure discovery, rapid variant creation

Overhyped Claims

- "Autonomous Attack Campaigns": Real operations require OpSec, context, and human decision-making
- "Stuxnet 2.0 via AI": Advanced OT attacks need domain expertise, supply chain access, physical testing

AI for Defender

Effective Use Cases

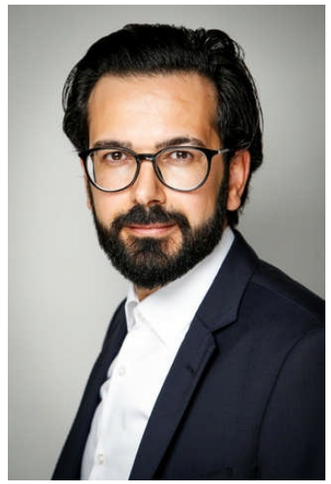
- Network/OT Behavioral Analysis
- SOC Alert Triage: Clustering, deduplication, prioritization

Suboptimal Use Cases

- DoS/DDoS Detection: Threshold/rate-limiting at sensor/firewall level. No ML for full traffic needed
- Known Signatures/TTPs: Rule-based/pattern matching is faster and more robust

Critical Success Factor is Feature Engineering

Web Attacks: HTTP method, path, status, headers/parameters captured?



Ali Recai Yekta
Yekta IT GmbH

Panelist Position

BARCELONA 2025

Yuichi KAJI
Nagoya Univ.
Japan

In my personal view...

long-term resilience = the ability to accommodate changes

- Migration to the cloud outsources classical issues of resilience
- Affected more by changes made in the cloud services
  - deployment of MFA, tighten security of mail services, migration to PQC...
- Raising the security level may make some services unavailable
  - A university is decentralized; nobody knows all the systems on the campus

Panelist Position

BARCELONA 2025

- Challenge One: fragmentation of responsibility
  - Autonomy brings the fragmentation of responsibility and budget
  - Shadow IT everywhere, transfer of people makes it a black-box
  - The responsibility of a single user is increasing
    - A fault of a single user can cause damage to the entire university

Yuichi KAJI
Nagoya Univ.
Japan

- Challenge Two: users' commitment
  - Professors tend to resist changes enforced by others
  - Everybody considers that security is someone else's business
  - Security evangelism for users is essential, but who does that?
    - At least, we need a good relationship with users so that they listen to us

Panelist Position

BARCELONA 2025

Timm Bostelmann
FH Wedel
(University of Applied Sciences)

- Implementing cyber resilience in a company is hard.
  Traditional perimeter security has reached its limits.
  - Human Factors: Most employees are not aware of or inherently interested in cybersecurity. At best, they want to get their job done and leave the rest to the IT Department.
    -> Phishing, Weak Passwords, Shadow IT
  - Complex IT Environments: Legacy systems and fragmentation are the natural state. Creating or keeping an organized structure takes much effort.
  - Resource Constraints: Implementing cyber resilience costs time and money upfront. Not being resilient is free... until it is not.
  - Regulatory Pressure: Even well-meant regulations can hinder cyber resilience if inconsistent or incompatible rules increase complexity.
- Implementing cyber resilience in a society is even harder.
  See all above... manyfold.

THE STAGE IS YOURS