NTNU CCIS and SFI NORCICS Joint Conference 2025
"Future directions of Cyber Security in the light of Disruptive Technologies"

November 18-19th 2025, Hotel Scandic Lerkendal, Trondheim

Presentation of keynotes

Keynote 1:

"Dual-Use Intelligence at the Frontier of Cyber Resilience: a Telecom Perspective"
Speaker: Jeriek Van den Abeele, Research Scientist, Telenor Research & Innovation

Abstract:
Cybersecurity threats are not new to the telecom sector. As one of the Nordics' largest digital service providers, Telenor faces a continuously evolving risk landscape that directly impacts national resilience. The growing interdependence between infrastructure and AI systems expands potential attack surfaces, and generative AI adds a complex layer of dependency and exposure. It facilitates automation and scale on both sides of the security equation -- enabling faster detection and response, while also allowing threat actors to produce targeted phishing content, disinformation, and exploit code at unprecedented speed and volume. This keynote examines both sides of that transformation, from vulnerabilities in small language models and agentic data-exfiltration risks to opportunities for enhanced situational awareness, adaptive defences, and resilient AI deployment in critical infrastructure.

Bio:
Jeriek Van den Abeele joined Telenor as a Research Scientist in 2020. He holds a PhD from the University of Oslo, where he worked at the interface of particle physics and artificial intelligence. At Telenor Research & Innovation, he has contributed to using reinforcement learning for network automation and has provided technical advisory regarding the EU AI Act since its inception. He is currently leading Telenor's involvement in the Horizon Europe project ENFIELD, focusing on Green, Human-centric, and Trustworthy AI research directions. His most recent projects include the development of defences against LLM jailbreak attacks and a large-scale survey analysing AI adoption among employees.

Keynote 2:

“Insights into deploying Private 5G and outlook to making 6G happen”
Speaker: Dirk Trossen, VP Research& Development, Chief scientist Norwaves Networks and Executive Partner DaPaDOT Tech

Abstract:
This talk outlines insights into the deployment of Private 5G networks for verticals, including mission-critical services. Norwaves has gained those insights through several engagements in Norway, ranging public safety, defence, entertainment and medical use cases. The talk will discuss the capabilities needed for those use cases and the plug-and-play nature in providing, building upon the largely softwarised nature of key 5G components. An outlook towards 6G will be provided, too, outlining some of the key capabilities that need attention, foremost the native support for AI capabilities, both at 6G system as well as service and application level.

Bio:
Dr. Dirk Trossen is the Executive Partner of DaPaDOT Tech UG, a SW consulting and development company, also serving as Vice President R&D and Chief Scientist for Norwaves Networks in Norway to develop innovative solutions for private 5G networks. Dirk is also the Secretary General of the Datacom Industry Association, founded in 2024 and assembling currently around 45 members in the Datacom industry and associated vertical industries. Dirk has extensive experience through his 30+ years career in Internet technologies, network architectures, 5G/6G technologies, and network protocols in general, having held previous appointments as Chief Researcher at Huawei, Interdigital Europe, BT, and Nokia, while also experiencing academic insights as Senior Researcher at Cambridge University and Associate Researcher at MIT. He has published more than 90 peer-reviewed publications, holds more than 50 patents, and contributed to several standard organisations like IETF and 3GPP.

Keynote 3:

“It's the law: Some technical things all Security Architects ought to know about CRA, EUCC regulation”

Speaker: Markku-Juhani O. Saarinen, Professor of Practice, Faculty of Information Technology and Communication Sciences, Tampere University

Abstract:

Markku-Juhani O. Saarinen is a Professor of Practice ("työelämäprofessori") and a Docent of Information Security and Cryptography at Tampere University (Finland). He holds a Ph.D. in Information Security from Royal Holloway, University of London (2009). Markku started his career at SSH Communications Security in 1997, helping to design the now-ubiquitous SSH2 secure login protocol, and after several industry positions, moved to academia to pursue his PhD in the mid-2000s. Post-Quantum Cryptography (PQC) has been a research focus since 2015, resulting in numerous publications and a half-dozen patents. In 2018, he was the first employee at PQShield Ltd. (UK), a University of Oxford spin-out focusing on PQC. At PQShield, he architected some of the first commercially successful high-assurance PQC hardware modules before joining Tampere University in 2023. He is currently a member of CENELEC TC 47X (Cyber Resilience Act / Semiconductors) and Chairs the Cryptography SIG at RISC-V International.

Bio:

I am currently Finland's representative to CENELEC TC 4 7X "Semiconductor devices and trusted chips", which is tasked with turning the security requirements of the EU's Cyber Resilience Act (CRA) into electrotechnical standards. These engineering standards are scheduled for release shortly -- I will try to provide the latest information. The CRA and its technical requirements are of great interest to chip makers and designers globally, as compliance will be required to sell electrical goods in the EU market (the comparable U.S. "Cyber Trust Mark" program, being introduced by the FCC, will be only voluntary). Among other things, CRA implies supply chain security measures, fairly strict vulnerability reporting timelines and responsibilities, as well as some concrete security features such as secure firmware updates (EU policy mandates quantum-secure signatures by 2031). For "Critical category" products (e.g., secure elements), CRA compliance often requires a third-party laboratory evaluation with the EU Common Criteria (EUCC) Certification Scheme; passing requires relatively advanced technical protections.

Keynote 4:

"The Evolution of Cyber Operations"
Speaker: Benjamin James Knox, The Norwegian Cyber Defence and Adjunct Associate Professor NTNU CCIS/IIK

Abstract:
The presentation looks at how thinking and conducting cyber operations has evolved within the Defence. This will be framed from a perspective concerning the expansion of cyberspace, and how this fits within the wider action-space of what we now refer to as cognitive warfar

Bio:
Benjamin Knox brings an academic perspective that is founded on thirty years of service in both the British and Norwegian Defence Forces. Ben holds a PhD in cyber and information security from the Norwegian University of Science and Technology (NTNU), and an MSc in Development Management from the Open University (U.K). Ben is research leader for the Norwegian Armed Forces Cyber Defence, and an affiliated researcher at the Norwegian Defence Research Institute (FFI). He holds associate professor positions at the Center for Cyber and Information Security (CCIS), and with the Faculty of Health, Welfare and Organization at Østfold University College, Norway. Ben's research interests lie in the fields of human factors in cyberspace operations, cognitive warfare, cognitive security, governance, leadership and applied cognitive performance.

Keynote 5:

"Cyber threat intelligence and management decision-making behavior: Gathering data through agent-based simulations, cyber exercises and serious games"
Speakers: Erjon Zoto and Grethe Østby, Associate Professors Department of Information Security and Communication Technology NTNU

Abstract:
Information security and the impact from ongoing cyber-attacks has become a fixed item on the main agenda for both public and private organizations in recent years. Coupled with the increasing skills and staff shortage in the related fields, the situation calls for greater attention towards new and creative solutions. In this session, the Information Security Management group will discuss the practical use of games, cyber exercises and other tools for improving the training efforts around cybersecurity, aiming to increase overall security posture and resilience in all levels of society.

Bio:
Grethe Østby & Erjon Zoto are both associate professors at NTNU, Department of Information security and Communication technology, with a special interest in information security management and how cyber-exercises, simulation tools and other types of serious games can support teaching and training activities.

Grethe teaches in the course IMT4115/IIKG6503 Introduction to information security management (master's level) and also supervises some master-students and a phd-student within relevant management responsibilities, and especially on learning artifacts in cyber-security exercises. Grethe will present how recent research has been executed in full-scaled exercises at the Norwegian Cyber Range and also examples of what our excellent master-students' studies.

Erjon teaches Infosec-related courses at the Bachelor level and is supervising several Master students, while also responsible for the experience-based Master program in Information Security. His part will focus on the development and usage of an agent-based simulation tool for modeling the interactions between attack and defense actors in cyberspace, where each agent's behavior is affected by a given strategy towards reaching the final goal.

Keynote 6:

“AI-driven digital forensics: Navigating cybersecurity challenges in the age of disruptive technologies”
Speaker: Dr. Hans Henseler, Senior Scientist Netherlands Forensic Institute, Professor Digital Forensics & E-Discovery Leiden University of Applied Sciences

Abstract:
My presentation will address the central challenge facing digital forensics today: the overwhelming volume of digital evidence that renders manual review ineffective. I will argue that while AI, specifically Large Language Models (LLMs), presents itself as a powerful disruptive technology, its direct application in investigations is fraught with critical cybersecurity and legal risks, such as data privacy violations and the generation of non-verifiable 'hallucinations'.

Drawing on our work with the Hansken digital forensics platform, I will outline an evolutionary path for responsibly integrating this technology:

1. **The Initial Stage:** Moving beyond basic LLMs to a secure **Question & Answer (Q&A) partner** using the Retrieval-Augmented Generation (RAG) architecture. This grounds the AI in case-specific evidence, solving the immediate security and reliability problem.
2. **The Future Direction:** Evolving from a simple Q&A tool to an **'Agentic' Copilot**. This represents the true paradigm shift, where the AI can autonomously use a toolkit of forensic functions to conduct multi-step reasoning. It can deconstruct complex investigative goals into smaller, manageable tasks and actively assist in solving them.

The core of my perspective is that the primary cybersecurity challenge is not just external threats, but the internal challenge of ensuring the **integrity, auditability, and legal admissibility** of evidence derived from these complex AI systems. The presentation will conclude with a framework for a human-AI partnership, where the investigator retains strategic control, ensuring AI is used as a powerful, but always verifiable, tool.

Bio:
Dr J. Henseler is part-time professor of Digital Forensics & E-Discovery at University of Applied Sciences Leiden since 2016. He is also a senior scientist in the Hansken division at the Netherlands Forensic Institute and chairman of the board of directors at DFRWS.

Keynote 7:

“NTNU-HUNT data services: utility, security, and privacy considerations”
Speaker: Arnulf Langhammer, Professor, NTNU ved Medisin og helsevitenskap

Abstract:
Presentation of the HUNT study; data collection, data handling, privacy management and research.

Bio:
He has been working at the HUNT Research Center since 1994. He was the co-project leader for the Osteoporosis Project in HUNT2, and he has also been the project leader for the Osteoporosis Project in HUNT3-4 and the Lung Project in HUNT2, 3, and 4. He was a member of the project group for HUNT3 and HUNT4, led the HUNT3 and HUNT4 questionnaire group, and was the leader of the HUNT database and management from 2007 to December 2023, and during the same period, he was a member of the HUNT leadership group. In addition to this, he has worked as a general practitioner in Steinkjer.