

Workshop proposal on Challenges and Opportunities in Digital Resilience – 2025

NIKT (Norwegian ICT Conference for Research and Education), 24 – 26 November 2025

Proposal by Stine Aurora Mikkelsplass, Aleksander Lygren Toppe, Sabarathinam Chockalingam, and Petter Kvalvik – IFE.

Workshop Significance/Relevance to NIKT

The workshop directly aligns with NIKT's role as a national meeting place for ICT research, innovation, and education, and with NISK's focus on ICT security and privacy. By addressing cyber security in practice, supply chain and COTS device challenges, and human-centered digital sovereignty, the workshop bridges research and real-world practice. It creates space for researchers, practitioners, and students to exchange insights on cyber security, resilience, and digital sovereignty, core concerns of the NISK community and highly relevant to the national and international ICT security landscape.

Description of the Workshop Topics

Cybersecurity in practice

- Lessons from the CIN Project
 - The Cyber Innovation Network (CIN) was a collaborative initiative to strengthen cybersecurity competence among Small and Medium-sized Businesses (SMBs) in Norway. Acknowledging the specific challenges faced by SMBs, such as limited resources and expertise in cybersecurity, the CIN project brought together research and industry to bridge the gap between academic research and real-world application. This session shares lessons learned on how knowledge from research and academia was translated into practical tools, enabling SMBs to improve risk management and overall digital security, among other topics. The discussion will also touch on barriers that SMEs often encounter when implementing cybersecurity measures, and how the CIN initiative encouraged collaboration, knowledge sharing, and the use of best practices to help address these challenges.
- Supply Chain and Commercial-Off-The-Shelf (COTS) Products
 - Commercial Off-The-Shelf (COTS) technologies and global supply chains present both opportunities and vulnerabilities for digital resilience. The increasing digitalisation and standardisation of software and hardware products enables the possibility of integrating new technologies into existing infrastructures. However, this integration raises critical questions about

transparency and security—do we truly know what is inside the products we procure? Industry efforts such as Software Bill of Materials (SBOM) and Hardware Bill of Materials (HBOM) aim to clarify product composition and manage complexity, covering aspects like frameworks, software libraries, and licensing. Adopting secure-by-design and privacy-by-design principles is essential for robust resilience.

- The evolving landscape, marked by regulatory measures such as digital security law (NIS2), and the Cyber Resiliency Act, will have a profound impact on both vendors and consumers, reshaping responsibilities and expectations. Software can enter an organisation through various channels—SaaS, PaaS, IaaS, or on-premises solutions—making it crucial to define accountability for security and maintenance. Questions of product ownership versus licensing is crucial, especially amid rapidly shifting geopolitical dynamics, which can result in products being remotely deactivated. This uncertainty underlines the need for organisations to prepare alternative solutions and develop clear exit strategies for their technology investments.

Human-Centered Digital Sovereignty

- Introduction to Human-Centered Digital Sovereignty.
 - How can we make digital consent more human-centered and trustworthy? In this session, we present a pilot study from the SecuRoPS (User-centred Security Framework for Social Robots in Public Space) project with the social robot ARI and citizens in Fredrikstad, exploring how privacy risk levels and security information can be communicated transparently to examine their impact on user trust. We will share key insights and open a discussion on human-centered approaches to transparency, trust, and digital sovereignty.
- Digital Sovereignty in Rail and Road Transport. Lessons learnt from Digital Road Operator Information and Data Strategy (DROIDS) and EU MOTIONAL.
- Discussion on Challenges and Opportunities on Human-Centred Digital Sovereignty.

Workshop Activities, Objectives, and Proposed Schedule for the Day:

Time	Session	Key points
09:00 – 09:10	Welcome & introduction	Overview of workshop objectives and structure. Brief introduction to the day's focus areas.
09:10 – 09:40	Cybersecurity in practice: Lessons from the CIN project	Insights from the Cyber Innovation Network (CIN) on translating academic research into tools for SMEs in Norway, improving skills such as risk management and digital security.
09:40 – 10:30	Supply chain and COTS products	Exploring opportunities and vulnerabilities of Commercial Off-The-Shelf (COTS) technologies and global supply chains, and secure-by-design/privacy-by-design principles. Discussion on regulatory developments, responsibilities in different

		acquisition models, and strategies for resilience amid geopolitical uncertainty.
10:30 – 10:45	Break	
10:45 – 11:45	Human-Centred Digital Sovereignty	Introduction to human-centred digital consent and trust, with findings from the SecuRoPS project, and case studies from rail and road transport (DROIDS, EU MOTIONAL). Open discussion on challenges and opportunities for human-centred digital sovereignty. Key takeaways and next steps.
11:45 – 12:00	Closing remarks	Q&A and key take aways

The workshop will aim be interactive and engage with the participants throughout the presentations.

Names and Backgrounds of the Organisers, Including their Relevance to the Proposed Workshop:

Petter Kvalvik is Head of Department for Business Development and a Senior Scientist at the Institute for Energy Technology (IFE). He holds a Master's degree in Applied Computer Science, a Master of Management in Strategy and Project Portfolio Management, a Master's degree in Safety and Security Critical Systems, and a Bachelor's degree in Business Administration. Petter leads the new research area on Digital Sovereignty, which includes, among other things, federated and autonomous systems, data spaces and data products, data governance, decentralised identities, digital trust, and interoperability. He is responsible for following up on the European data strategy, the European technology stack, the Big Data Value Association, and the annual International Conference on Digital Sovereignty. He also heads the My Digital City programme and the Norwegian FIWARE iHub for IoT. Both initiatives play a vital role in piloting a Norwegian data space for smart communities, involving project participants such as Halden Municipality, Østfold University College, and Smart Innovation Norway.

Aleksander Lygren Toppe has over 20 years' experience in IT and OT consultancy, research, and operations, with a background in Computer Science. He has led initiatives to integrate emerging technologies into safety-critical sectors like nuclear, served as lead developer for logistics solutions in Norwegian oil and gas, and managed IT operations including data lakes, Kubernetes clusters, and IFE Cyber Security Centre. Aleksander has also worked with sensor networks for smart buildings and energy optimisation, and his current focus is on cyber security and resiliency for safety-critical industries and broader societal applications.

Stine Mikkelsplass Aurora is the Head of the Risk and Security department at IFE. She holds a MSc in Applied Computer Science from Østfold University College (HiØ), specialising in cybersecurity. She also holds a BE in computer engineering from HiØ, and a BA in Cultural and Social Studies from the University of Oslo and La Trobe University in

Australia. Stine has previously lectured at Østfold University College, and at IFE she has served as project manager for the OECD Halden Human Technology Organisation (HTO) project *Cybersecurity of black-box solutions and technology*, coordinated IFE's contributions to the research centre SFI Autoship, and led IFE's contribution in the project *Cyber Innovation Network*. She is currently leading the project *Competence building for SMBs – innovations in cyber security training* and has experience in both developing cybersecurity courses, and lecturing, for SMBs.

Sabarathinam Chockalingam is a Senior Researcher in the Department of Risk and Security at the Institute for Energy Technology. Saba has a PhD in Artificial Intelligence and Cyber Security from Delft University of Technology and a Master of Science in Cyber Security and Management from the University of Warwick. He has managed and contributed to national and international research projects related to cyber security such as CPSEC, ERA 4.0, RECYCIN, and SecuRoPS. Finally, he also served as an Organisation and Program Committee member in various international conferences and workshops in addition to being a reviewer and (guest) editor for high-quality journals in the field of his expertise. Notably, Saba is leading the SecuRoPS (*User-centred Security Framework for Social Robots in Public Space*) project, which explores human-centered approaches to digital privacy and trust. This experience enables him to contribute to discussions on *Human-Centered Digital Sovereignty* in the proposed workshop, where he will share insights on how privacy risk levels and security information can be communicated transparently to establish user trust.

Maximum Number of Participants: Maximum 40 participants.

Procedure for Recruitment and Selection of Participants: The workshop is open to all registered conference attendees and will be filled on a first-come, first-served basis until maximum capacity is reached.

Equipment and Supplies Needed to Conduct the Workshop: The workshop requires a projector with screen, Wi-Fi, flipchart/whiteboard with markers, and standard tables/chairs for group discussion. If possible, a microphone and power outlets for participant laptops would also be helpful.