SFI NORCICS and ISTARI Smart Resilience Summit September 3rd 2025

Date: Wednesday, September 3, 2025
Time: 09:30 – 15:00 CEST
Location: Scandic Solli, Oslo
Host: NTNU / SFI NORCICS & ISTARI

Technology alone isn't enough.
Despite technological advances, the number and severity of cyber incidents continue to grow. A broad spectrum approach—however well-intentioned—will fall short in effectively preparing for and mitigating the scale and speed of emerging threats.

As AI transforms both the threat landscape and the defensive toolkit, the need for informed human oversight becomes even more critical. Strategic judgement, contextual understanding, and cross-functional coordination are the differentiators.

What's required now is not simply more tools or broader approaches, but a **disciplined, collaborative, and intelligence-driven strategy** to deliver **Smart Resilience** - that aligns resources with the most pressing risks, integrates insight across silos, and drives real-world resilience with measurable outcomes.

Program:

When	What
09:30 – 10:00	**Check- in & Networking Refreshment Break** Welcome coffee and informal networking to kick off the day
10:00 – 10.05	**Opening Remarks** • Welcome from NTNU and ISTARI; • Overview of the summit's objectives and themes.
1:05 – 10:40	***Smart Resilience in a Hyperconnected World*** • The evolving landscape of cyber threats and the need for integrated resilience strategies;. • Lessons from the cyber frontline; • Case studies on proactive vulnerability identification and mitigation.
10:40 – 11:15	***Third-Party Risk – Smart Efforts for Maximum Impact*** • What does a good 3PR strategy look like? • Practical examples of effective 3PR.
11:15 – 11:55	**Data-driven governance: Seeing the Whole Picture** • How to ensure your controls are actually working while providing risk insight across the organisation?

	• Practical case study of managing data-driven governance in complex organisational structures.
12:00 – 13:00	**Networking Lunch** An opportunity to connect with peers, speakers, and industry experts.
13:05 – 13:40	**Closing the Gap on *OT-IT*** • A strategy exercise to explore the nexus between OT & IT, how they interact and how to get ahead of the challenge.
13:40 – 14:15	***Harnessing AI and Next-Gen Cyber Defense*** • How to enable AI while ensuring proper governance and controls? • Balancing automation with human oversight in threat detection.
14:15 – 14:50	***Engaging with Boards in a NIS2 World*** • Communicating cyber risks and resilience strategies to board members effectively; • How to actively engage board members for a joined-up approach to cyber resilience.
14:50 – 15:00	**Closing Remarks**

Speakers:

Dr Melanie Garson
Director, Research & Insights, ISTARI & Associate Professor in International Security, University College London

Dr Garson is cyber and tech geopolitics policy specialist and public speaker who connects the dots between new and emerging tech and its potential impact on security, foreign policy, diplomacy and the world order. She is an Associate Professor in International Security in the Department of Political Science at University College London where she teaches her flagship course "From Cyberwarfare to Robots: The Future of Conflict in the Digital Age."

She worked for four years as the Cyber Policy and Tech Geopolitics Lead at the Tony Blair Institute for Global Change, and is also a lawyer and mediator. Melanie regularly provides commentary on geopolitics and tech in podcasts, webinars and at major media outlets including Bloomberg, BBC, Sky, CNBC, CNN, Fox News, France 24, and DeutscheWelle.

Jo De Vliegher
Client Partner, ISTARI, former group CIO, Hydro

Jo De Vliegher is a client partner at ISTARI, supporting clients across EMEA in managing digital risk and enhancing cyber resilience. Previously, he was Group CIO at Hydro, a global aluminium and energy company, where he led IT, digitalisation and cybersecurity for 34,000 employees.

Jo oversaw Hydro's cybersecurity programme and led the acclaimed response to the company's 2019 cyber-attack, recognised as a gold standard across the industry.

Lilja Fjeldsted
(CISSP, CISA, CISM) Senior Solution Architect, BlueVoyant

Lilja guides Nordic enterprises in building resilient third-party risk management programs and advanced security operations. With 19+ years of cybersecurity, she pioneered early third-party risk frameworks in the financial sector.

Lilja combines deep technical expertise—including Microsoft Security solution specialization—with strategic advisory experience, helping organizations mature internal/external threat detection and align programs with regulations like NIS2 and DORA.

Ben Dickinson
Founder and CEO, 3VRM

As a Managing Director at 3VRM, Ben designed and led the firm's Supplier Risk Management and Assurance capability, interacting with regulators and peer organisations to develop standards and approaches across various risk topics impacting Third Parties, including: Cyber, Security, Information Management, Resilience, Conduct, Regulatory Compliance, PCI-DSS, Sanctions and Anti-Bribery & Corruption.

Sam Weeks
VP Client Solutions, Prevalent AI

Sam has been pioneering cyber security solutions for over 15 years, with extensive technical and operational computer network operations experience. He was previously General Manager in the UK for Linchpin Labs, the world leader in the privatised intelligence industry, and spent nearly a decade with UK Government leading the design and delivery of cyber offensive technical and operational capability at scale.

Paul Norton
Head of Cyber Strategy & Assurance, Avon

Paul is Head of Cyber Strategy & Assurance at Avon, with over 15 years' cybersecurity experience in global consumer goods and retail sectors. He specialises in governance, risk management and compliance, having developed and executed cyber strategies across diverse markets in Europe, Asia, Australia and the Americas.

His expertise spans enterprise IT transformation, third-party risk and regulatory assurance, making him a respected leader in driving resilience and securing digital operations.

Nicolas Castellon
Director Cybersecurity Services Europe, Sygnia

Nicolas leads Sygnia's incident response, advisory and managed security services in the Nordics, Benelux and Iberian countries. Prior to Sygnia, he led Capgemini Group's Cybersecurity practice in the Nordics, guiding C-suites through multi-year cyber-transformation projects in aerospace, automotive, manufacturing and energy sectors.

Earlier in his career Nicolas worked in research across various Think-Tanks and IOs such as UNDP's Crisis Response Unit in New York City, The Hague Centre for Strategic Studies and Brazil's Getulio Vargas Foundation Center for Technology and Society, co-authoring several widely cited policy papers.

John Gorski
Programme Director, Advisory, ISTARI

John joined ISTARI from Sky, where he served as Head of Cyber Delivery and Programme Director. John has over 15 years of experience leading large transformational programmes; the last eight have been exclusively in cybersecurity.

Among other achievements, John built a global claims team for Goldman Sachs in Bangalore, India, continuing a distinguished tradition of Royal Engineers developing capabilities in Bangalore, helping the city become a global /IT business powerhouse.

Jason Mallinder
Client Partner, ISTARI, former CISO CreditSuisse

Jason is a Client Partner at ISTARI. He is the former Global CISO and Managing Director at Credit Suisse. He was responsible for information security, including cybersecurity and technology risk management, globally. Having joined in 1998, Jason spent 25 years at Credit Suisse and held numerous roles in technology and operational risk during his time there.

Jason is a certified information security manager and certified risk manager. He chaired the Investment Banking Information Security Group in the U.K. and worked closely with the Bank of England and the U.K. government on cross-sector cyber defence development, testing and exercising programs.

Felix Knoll
COO/CRO and Co-Founder, Cranium

David Prince
Principal, Advisory, ISTARI