Cybersecurity and Workplace Innovation

(SFI: Norwegian Centre for Cybersecurity in Critical Sectors)

Professor Halvor Holtskog, PhD

Department of Industrial Economics and Technology Management

Faculty of Economics and Management

Norwegian University of Science and Technology

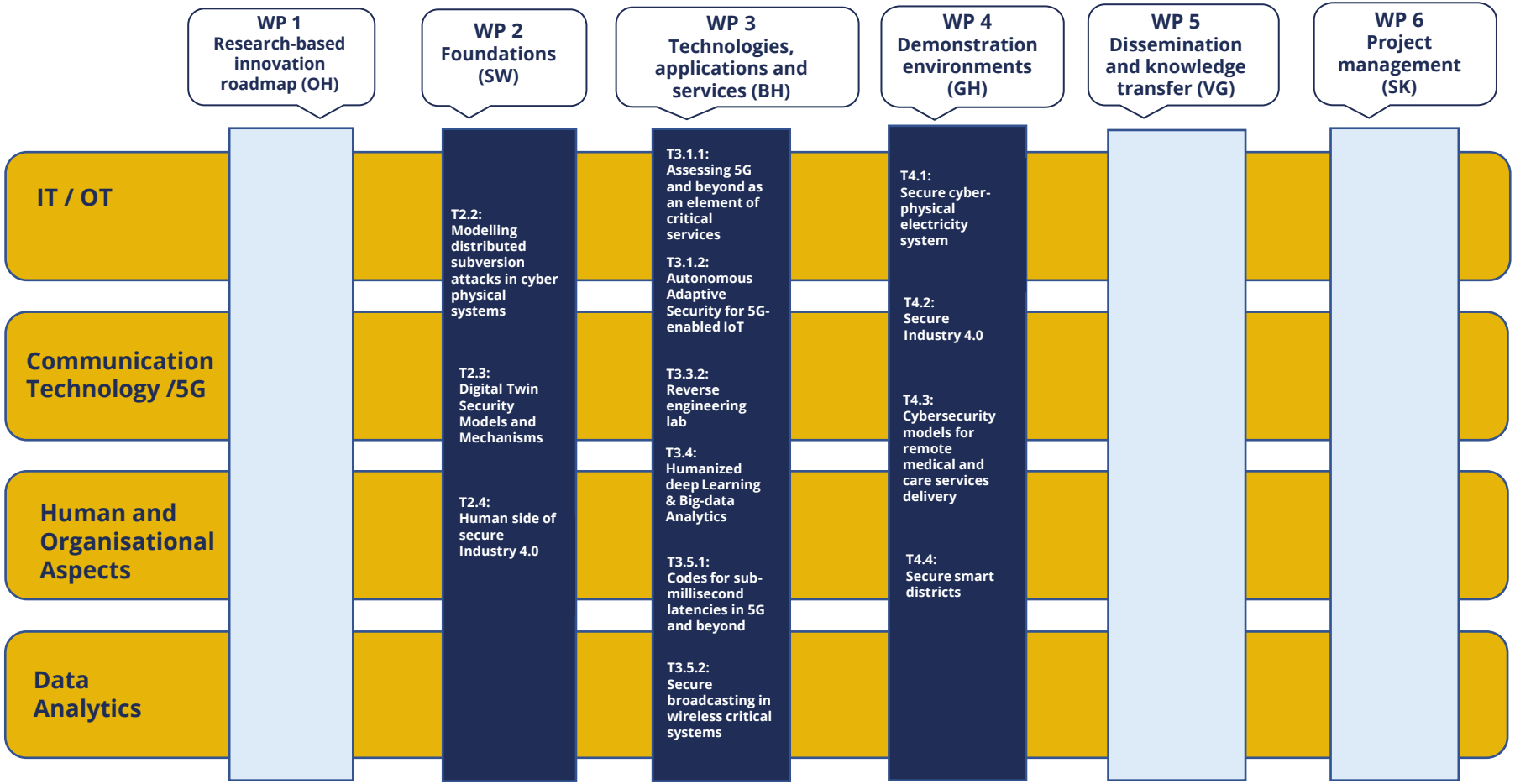
Knowledge for a better world

NORCICS – Vision and Objective

- Norway is among the most digitalized countries in the world. NORCICS's vision is to make Norway the most securely digitalized country in the world by improving the cybersecurity and resilience of its Critical Sectors, through research-based innovation.

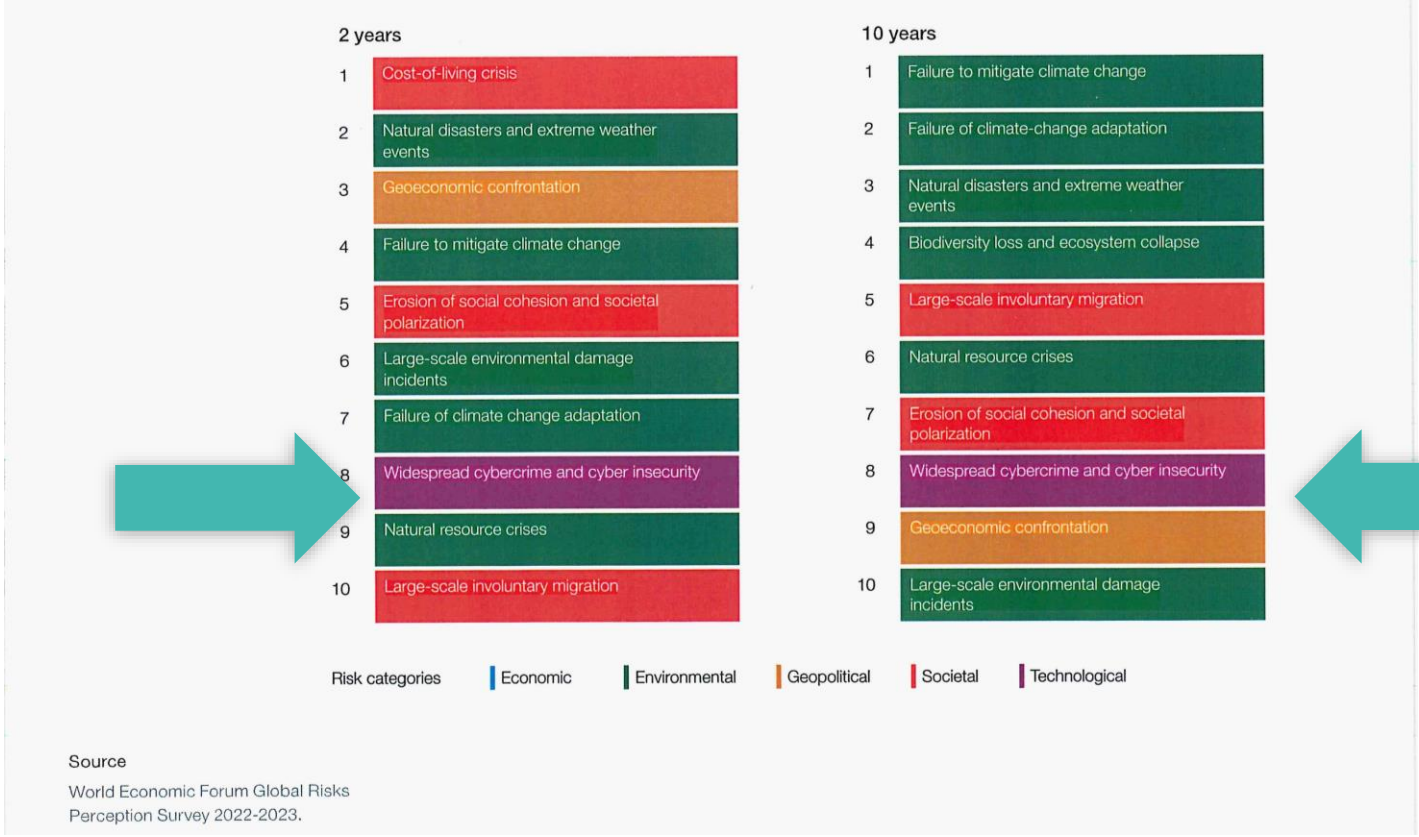
- NORCICS's primary objective is to enhance the capability of private and public sector stakeholders to respond to the current and future cybersecurity risks by developing, validating, and operationalizing innovative technologies within a cyber-physical security ecosystem that includes highly trained research personnel.

NORCICS Cross-thematic Areas - the helicopter view on NORCICS activities



NORCICS Partnership

Top 10 risks over the next 2 – 10 years



Source

World Economic Forum Global Risks Perception Survey 2022-2023.

Digital dependence and cyber vulnerabilities

Highlights:

- 435% increase in ransome in 2020
- 3 million – gap in cyber professionals needed worldwide
- 800 billion – estimated growth in value of digital commerce by 2024
- 95% cybersecurity issues traced to human error

Log4j-vulnerability

Global Cybersecurity Outlook 2022

The Gardian (UK, 30. March 2023)

- ‘Vulkan files’ leak reveals Putin’s global and domestic cyberwarfare

- Systems for offensive purposes
  - NTC Vulkan / Sandworm
    - NotPetya/Scan-V
    - Amezit
    - Crystal-2V
- Internet control, surveillance and disinformation

CNN BUSINESS

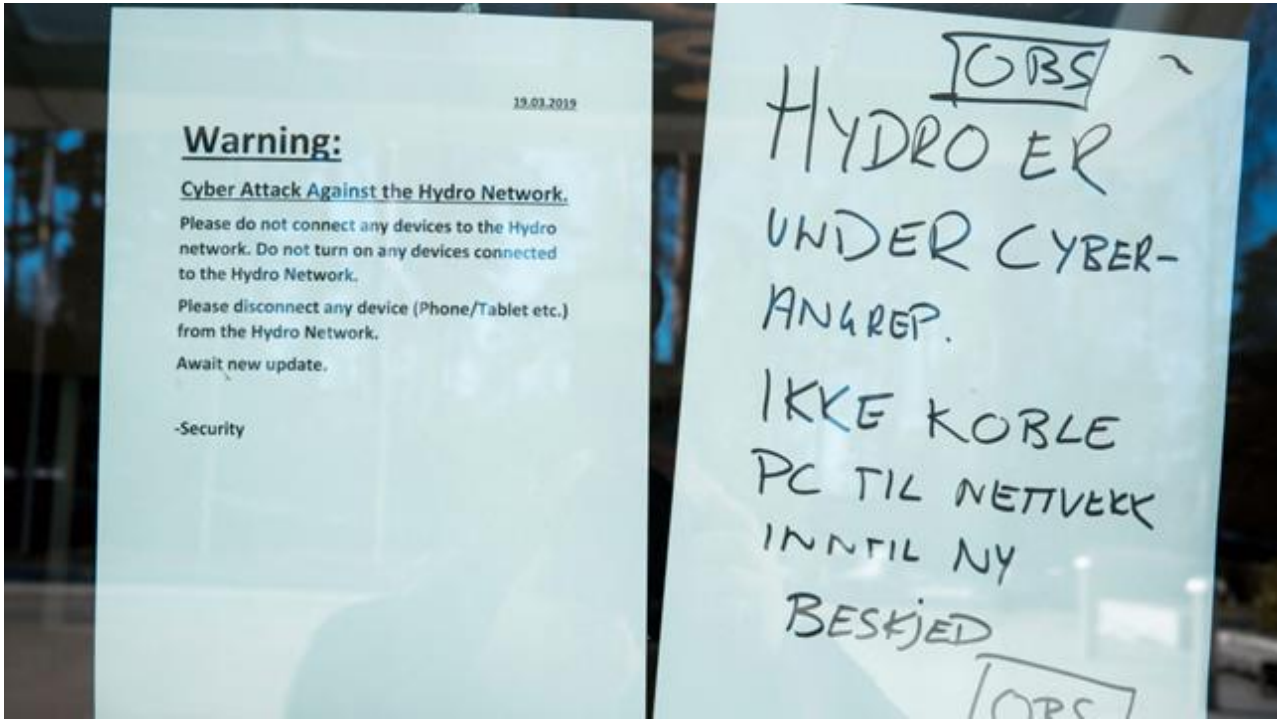
Cyberattack on Toyota's supply chain shuts its 14 factories in Japan for 24 hours

Changing the mindset

- *From: preventing it from ever happening here*

- *To: what do we do when it happens.*

The Hydro - case



Cybersecurity and Workplace Innovation

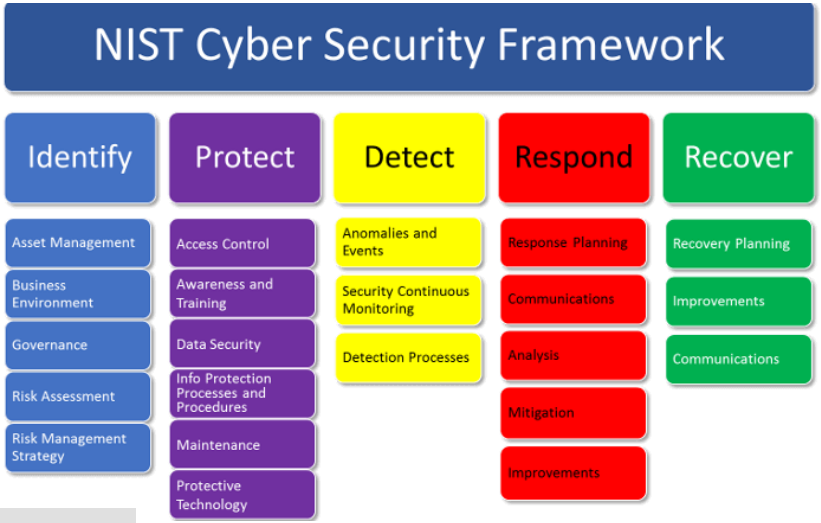
Track 1 work on Hydro attach

Investigating an organization that has experienced a serious cyber-attack

- How do people react during a cyber-attack?
- How do people react after a cyber-attack?
- What is the effect on innovation?
- What can we learn from employees' reactions during and after a cyber-attack?

Track 2

Cybersecurity knowledge is higher when the company follows dedicated security standards



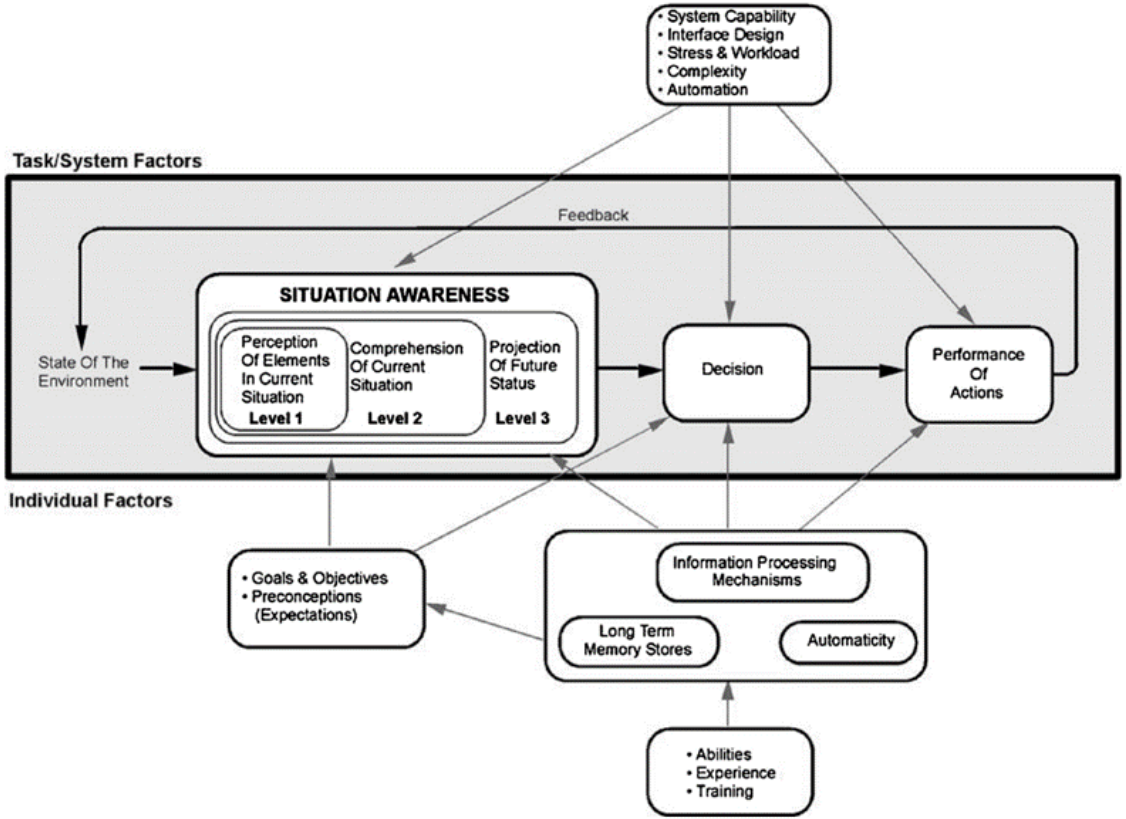
For SME's backup is the security

Endsley's Situational Awareness model (Endsley, 1995)

- Situational Awareness (SA) is a critical cognitive process that enables individuals to perceive, understand, and project the future status of elements within their environment, forming the basis for effective decision-making (Endsley, 1995)

- Insufficient SA is a key factor in incidents across aviation, healthcare, and large-scale technological systems, often due to lapses in judgment and concentration (Hunter et al., 2022).

- Endsley's model, while effective for individual scenarios, often overlooks organizational or hierarchy of individual systemic levels (Siemieniuch and Sinclair, 2008).



Track 3 – Security Operation Center

- Arguing for Cyber Situational Awareness as a subset of Situational Awareness.
- Looking into the Situational Awareness within the Security Operations Center environment.
  - Limited research found
  - Important when a breach happens
  - Language – virus / worms / etc.

Connecting SA to cyber security

Cyber security awareness

- Cyber security awareness refers to how much end-users know about the cyber security threats their networks face, the risks they introduce and mitigating security best practices/training to guide their behavior (Kim, 2017)
- Cyber awareness in the literature is about: awareness training, cyber security knowledge, awareness campaigns etc.

Cyber SA

- Cyber SA (CSA) refers to a subset of SA, where SA requirements for the human operator are aimed at cyber security (Jajodia et al., 2009; Ofte and Katsikas, 2022)
- Distributed Situation Awareness (DSA): A conceptual framework to address situational awareness in complex, socio-technical systems.

Situational awareness (Track 4)

- One must enter the world of the operator to **understand the mechanisms impacting awareness (context)**
- Navigating the complexities of digital change requires a deep understanding of SA to manage emerging challenges effectively and **maintain safety during technological transitions** (European Commission, 2021)
- Awareness is not merely the sum of individual team members' knowledge but is embedded within the interactions, processes, and tools that make up the entire operational environment. This level of analysis aims to understand how situational awareness emerges from the interplay between these various elements

Track 4 – Cyber Situational Awareness and workplace innovation

Final remarks

- The question is not how to innovate, but rather what prevent organizations from innovation.

- Innovation is treated as something extra ordinary, but what is truly extra ordinary is how we prevent it from happening.

NORCICS

SFI Norwegian Centre for Cybersecurity in Critical Sectors

Thank you for your attention!

Track 1 – Julie Leirmo, phd candidate (julie.l.leirmo@ntnu.no)

Track 2 – Kristian Kannelønningen, phd candidate (kristian.kannelonningen@ntnu.no

Track 3 – Håvard Ofte, phd candidate (havard.ofte@ntnu.no)

Track 4 – Christina Micheltree, researcher (christina.micheltree@sintef.no)