Cyber Resilience in the Nordics: Lessons from the Public and Private Sectors

Peter Sund
CEO
Finnish Information Security Cluster - Kyberala ry
2025

Finnish Information Security Cluster

PECB REGIONAL WEBINARS



Contents:

1. Situation
2. Systems and Actors
3. Policy Recommendations
4. Q&A

Peter Sund

- CEO, Finnish Information Security Cluster (FISC)
- Branch Director, Cybersecurity, Technology Industries of Finland
- Education: LL.D. Cand., MBA, MEng, CVT, DPS, ESDC alumni

Prior work-life exposure on security in EU, UN, OSCE and corporate roles. Research activities focused on regulation and policy issues of cyber security governance systems.

Finnish Information Security Cluster (FISC), a branch of the Technology Industries of Finland is a trade and advocacy organization for the cybersecurity industry. Our purpose is to promote the viability of the sector, as well as information and digital security in Finland and in Europe, in cooperation with public administration, businesses, and the civil society.

Finnish Information Security Cluster Kyberala



Finnish Information Security Cluster

SITUATION: SECURITY DRIVERS

Drivers

- Change in the security environment
- NATO memberships
- EU's growth as a security actor
- Experiences gained from domestic crises
- Lessons learned from Russia's war of aggression against Ukraine
- Administrative changes
- Other security projects

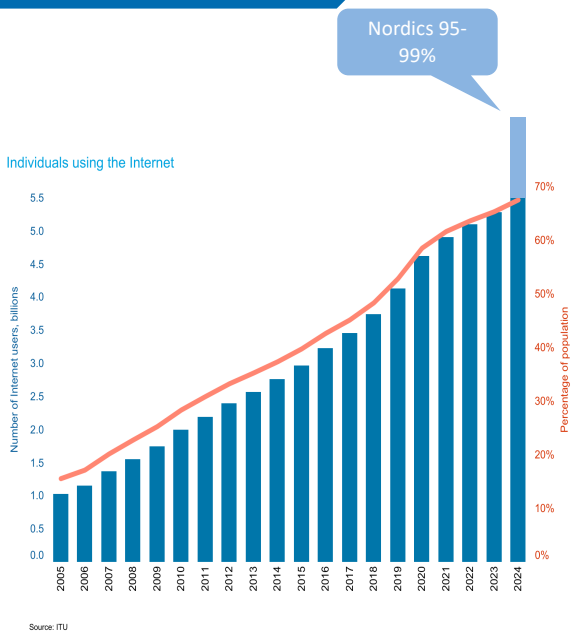
Needs:

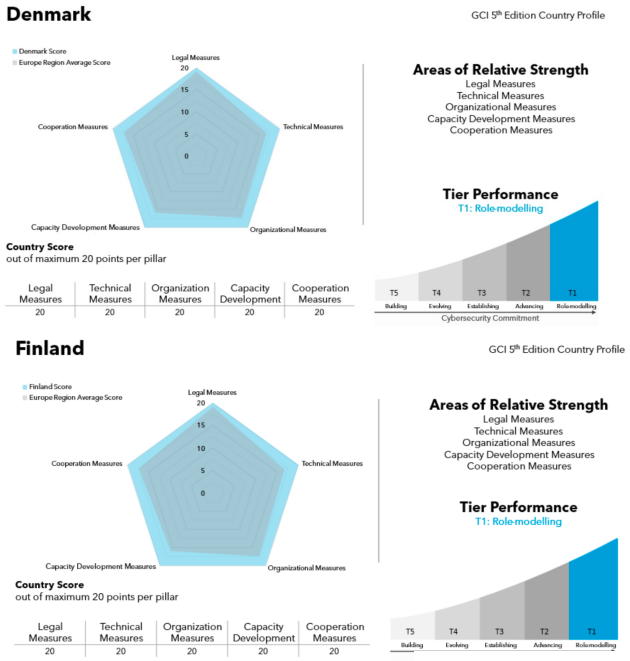
- In addition to preparedness, ability to respond to disruptions and crises
- Instead of focusing on vital functions and actors, more emphasis placed on activities themselves
- The connection to the EU's and NATO's developing resilience work to be strengthened
- The responsibility of individuals as key actors in security to be emphasized

Finnish Information Security Cluster

PECB REGIONAL WEBINARS

SITUATION: UNDERSTANDING CYBERSECURITY

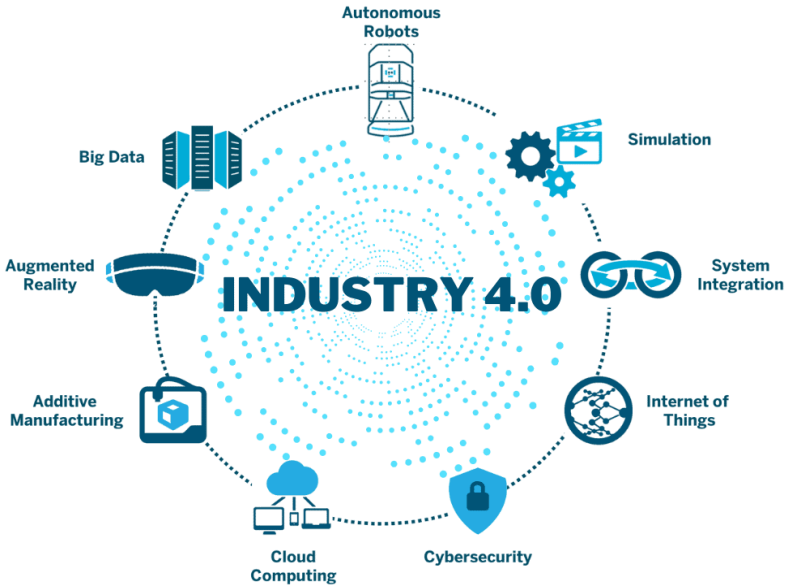


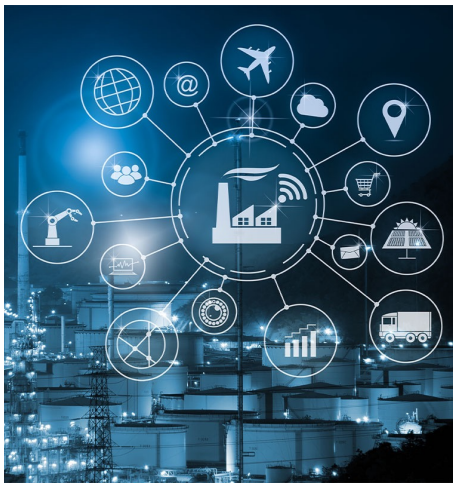


Finnish Information Security Cluster

PECB REGIONAL WEBINARS

CORE ISSUES





Finnish Information Security Cluster

PECB REGIONAL WEBINARS

SITUATION: UNDERSTANDING CYBERSECURITY

- Many systemic risks in the digital operating environment have materialized due to unconsidered technological optimism and inadequate risk management
- E.g. uncontrollable number of security breaches, fraud, theft, espionage as well as misinformation, and widespread misuse of personal data
- 2-3 malicious cybersecurity attempts / second / 365
- Total Cybercrime 8.5 - €10 T€ (2024)

Cybercrime Type	Estimated Annual Cost (2024)
Data Breaches	€3.8 - €4.5 Trillion
Ransomware Attacks	€500 - €600 Billion
Fraud & Phishing	€1.2 - €1.5 Trillion
Business Email Compromise (BEC)	€40 - €50 Billion
Identity Theft & Dark Web Sales	€200 - €300 Billion
Cryptocurrency Scams & Theft	€400 - €500 Billion
IoT and AI-related Cybercrime	€100 - €200 Billion

* Sources: Cybersecurity Ventures, IBM Cost of a Data Breach Report, World Economic Forum, Europol

Finnish Information Security Cluster

PECB REGIONAL WEBINARS

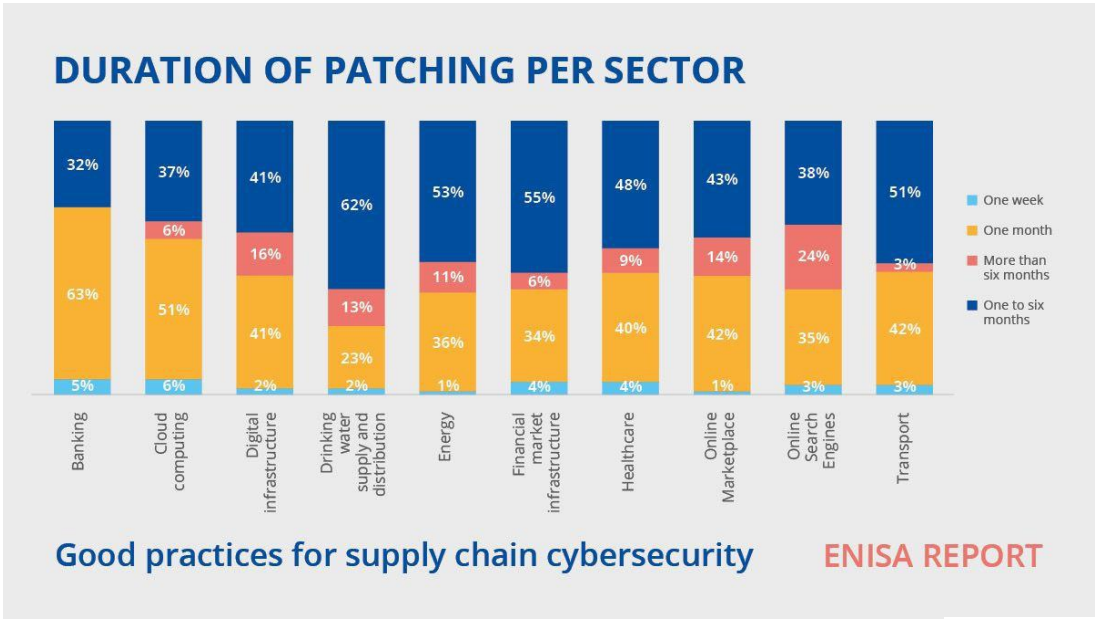
SITATION: ACTORS AND REPRESENTATION



Finnish Information Security Cluster

PECB REGIONAL WEBINARS

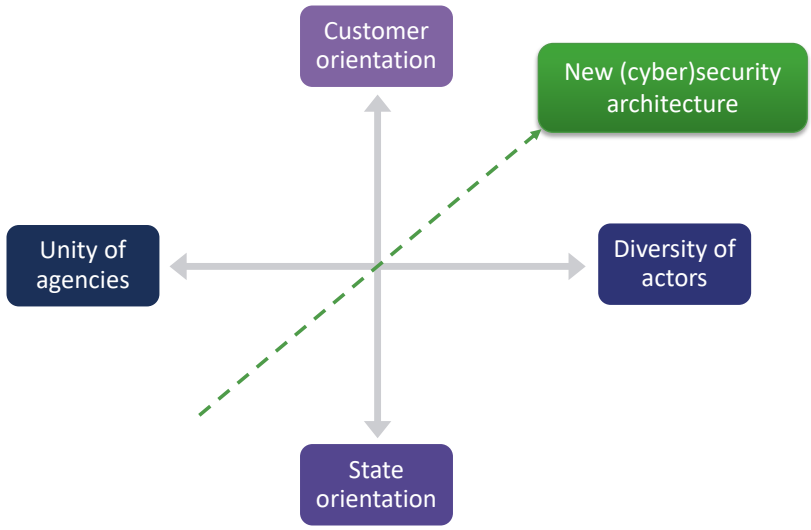
CRA HUOMIOITA



Finnish Information Security Cluster

PECB REGIONAL WEBINARS

CYBERSECURITY ARCHITECTURE



Adapted from © Huotari V. & Jukarainen P. (2024)

Finnish Information Security Cluster

PECB REGIONAL WEBINARS

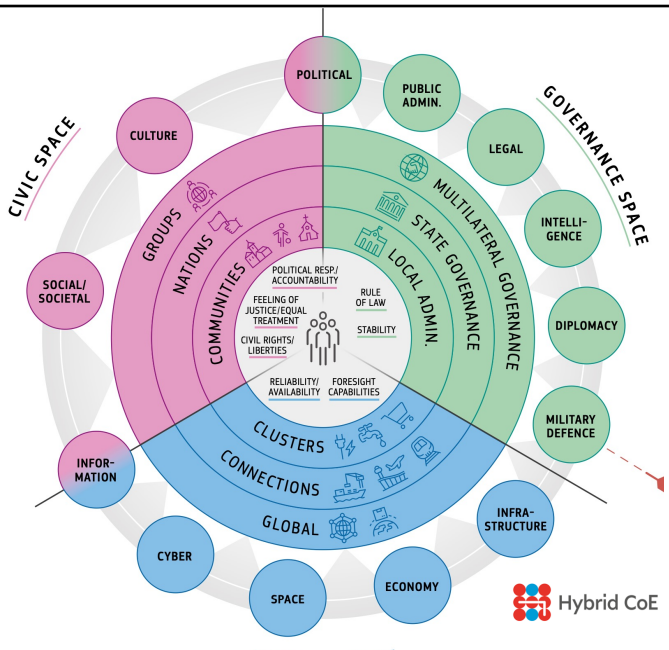
REGULATION AND POLICY: CYBER CONTEXT

- How is cybersecurity created?
- By who?
- By which objectives?
- Under who's authority?



REGULATION AND POLICY: END GAME

Not just enduring and surviving challenges (resilience), but shaping actions in a **sustainable**, **just** and **democratic** way



National security of supply

Shared responsibility of the company and NESA

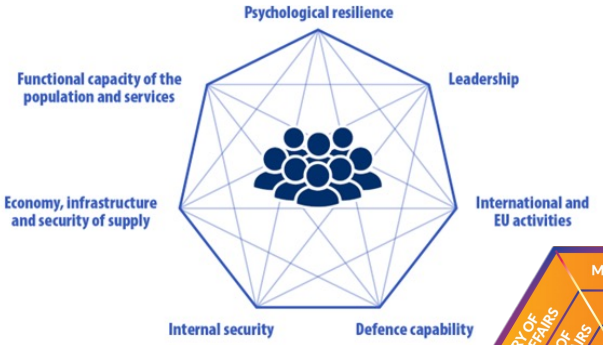
Under companies' own responsibility

SOCIETAL NEEDS: Needs-based dual- and multi-faceted risk management

LEGAL REQUIREMENTS: Risk management based on regulation and other external obligations

BUSINESS REQUIREMENTS: Company's own risk management (reputation, competitiveness and quality, customer obligations)

REGULATION AND POLICY: CYBER CONTEXT

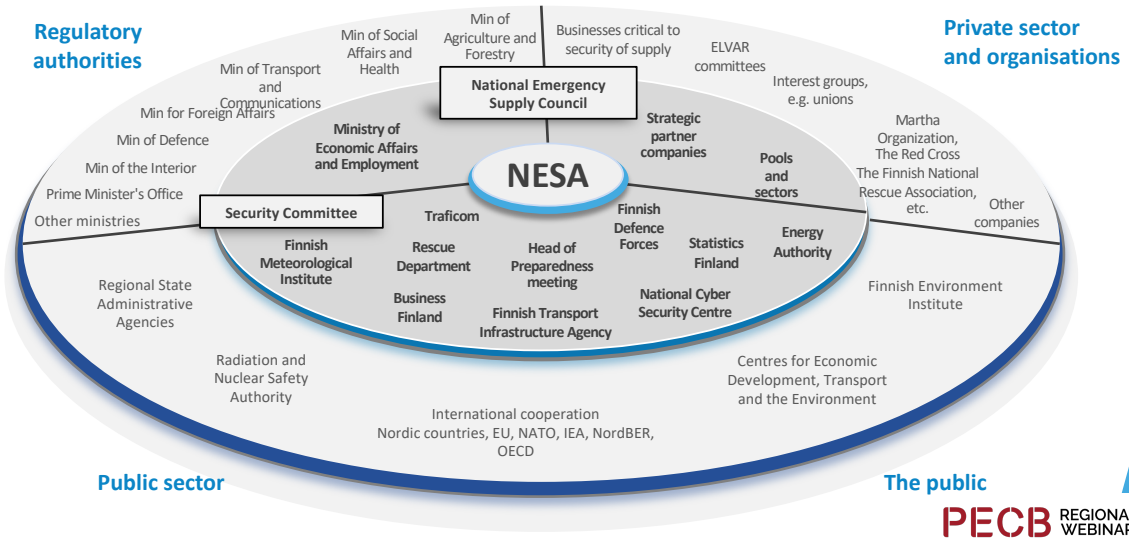






National Emergency Supply Organisation

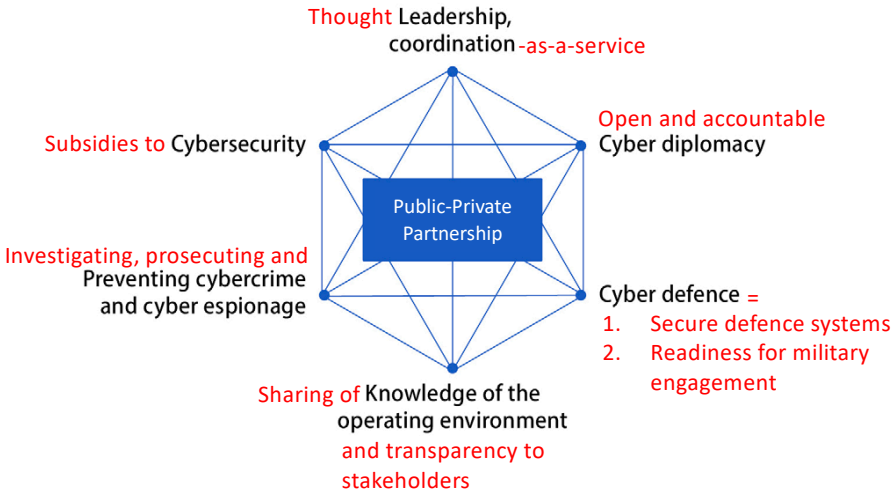
NETWORKED OPERATING ENVIRONMENT



PECB REGIONAL WEBINARS

REGULATION AND POLICY: MEANS AND RATIONALITY CHECK

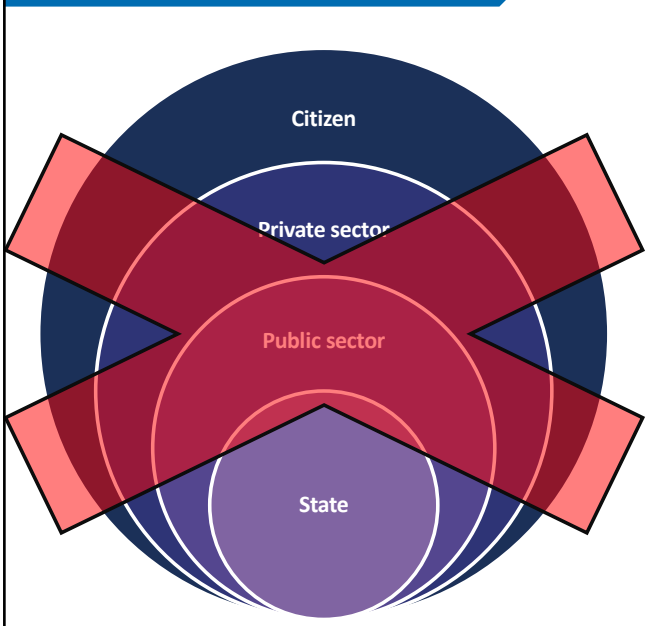
Under the scope of international law, emphasizing rule of law and fostering economic prosperity

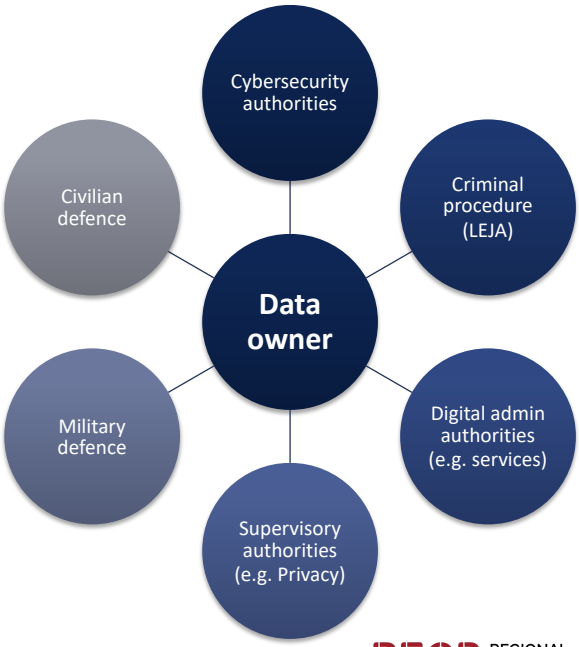


Finnish Information Security Cluster

PECB REGIONAL WEBINARS

ROLES AND RESPONSIBILITIES: UNDERSTANDING CYBERSECURITY

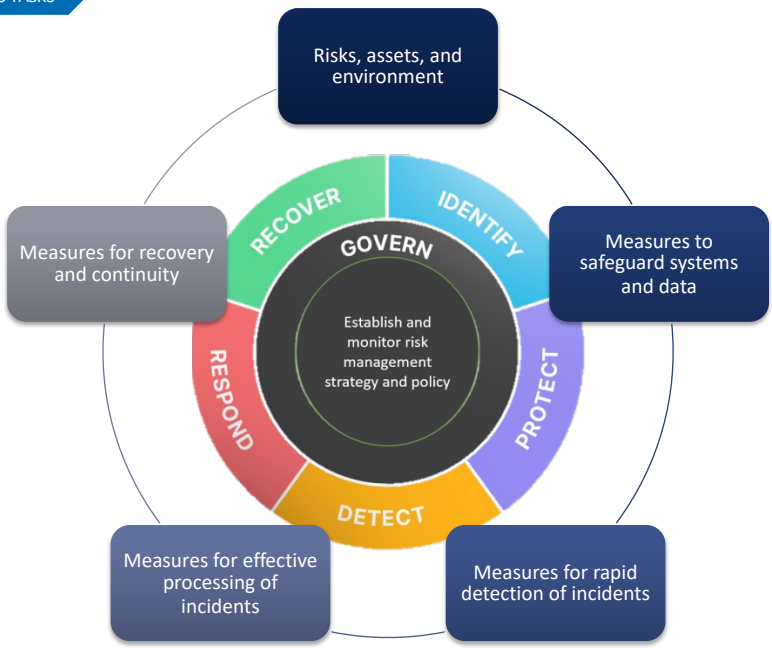




Finnish Information Security Cluster

PECB REGIONAL WEBINARS

MANAGEMENT: DATA OWNERS TASKS



Finnish Information Security Cluster

PECB REGIONAL WEBINARS

Strategic approach

- Fortress, Free market or Folkhemmet?
  - Digital dictatorship (data as control mechanism)
  - Unrestricted capitalism (winner takes it all)
  - Welfare state (data enabling equal citizenship)
- Biggest effect of data individuals (vs. state, EU or UN)
  - The rise of data as the main factor of production
  - Data capitalism
  - EU regulations: Data ownership, sharing and exploitation
- Digital sovereignty
  - Independence of states in foreign and security policy
  - Independence of companies
  - Independence of human individuals from external forces
- Security provides only part of digital trust
  - Strong rule-based support is therefore needed
- Outcome-based regulation



Finnish Information Security Cluster

PECB REGIONAL WEBINARS

