Critical infrastructures and their resilience in the Finnish context

Tuomas Raivio
Docent, Executive in Residence, Aalto University
Critical Infrastructure Lead, Sweco Finland

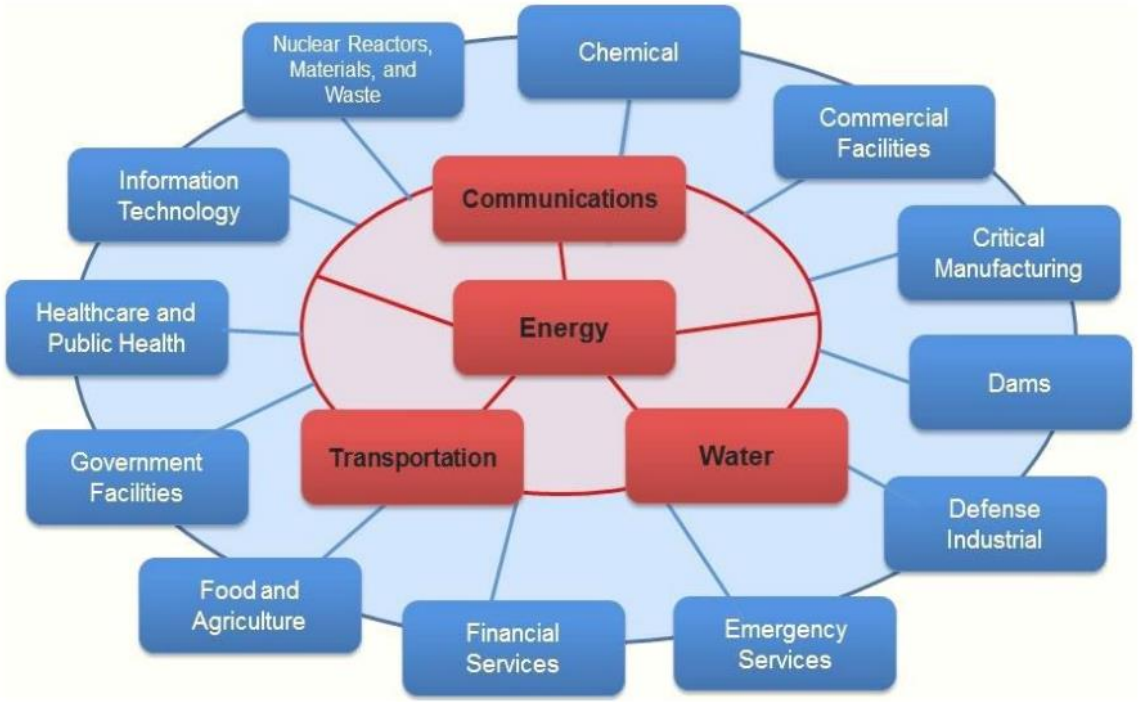
Outline

1. What is a critical infrastructure?
2. What is resilience?
3. Finnish context and safeguarding

1. What is a Critical Infrastructure?

What is a critical infrastructure?

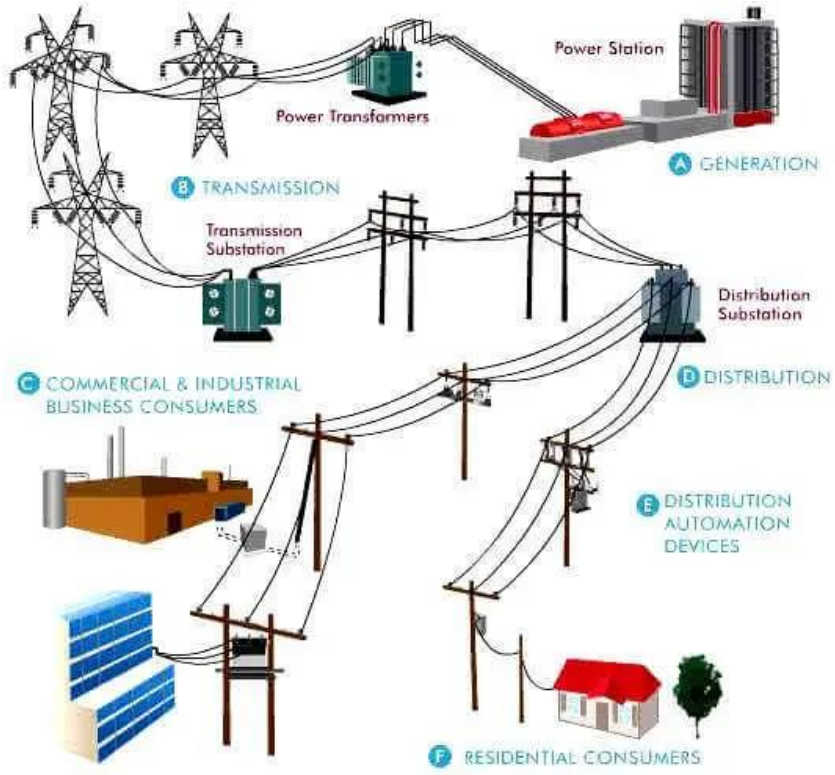
- Society relies more and more on various basic systems and services
- In Finnish conditions, certain systems are necessary for immediate survival
- Other systems are necessary for the functioning of society
- The vital functions of society rely heavily on these system
- **Critical infrastructures are the services and structures that enable survival and the functioning of society**
- Not everything that is claimed to be critical is critical for everyone.



H2020 700416, SUCCESS project, "Securing Critical Energy Infrastructures," http://www.successenergy.eu/

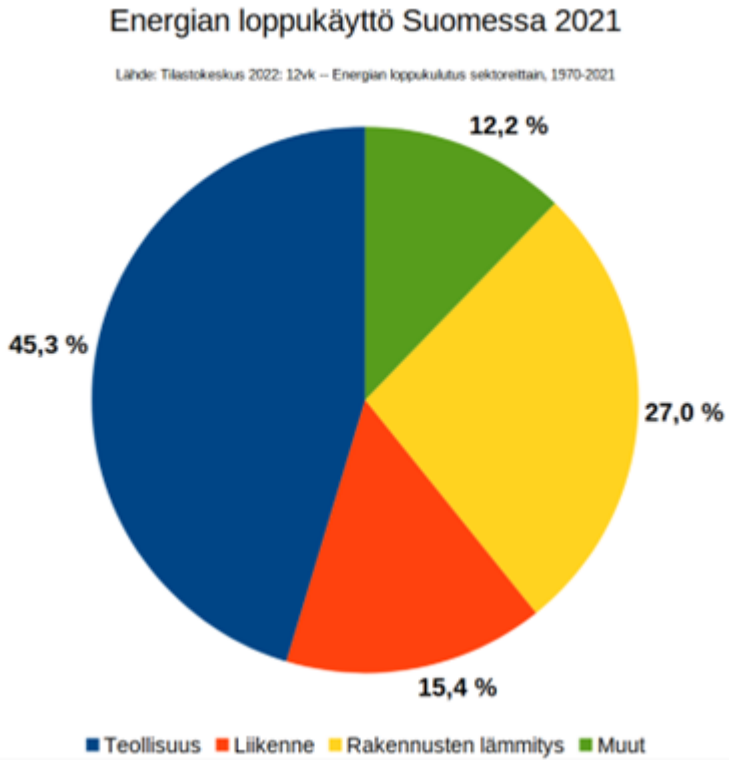
Key critical infrastructures 1

1. Power generation and distribution



Problem: No electricity

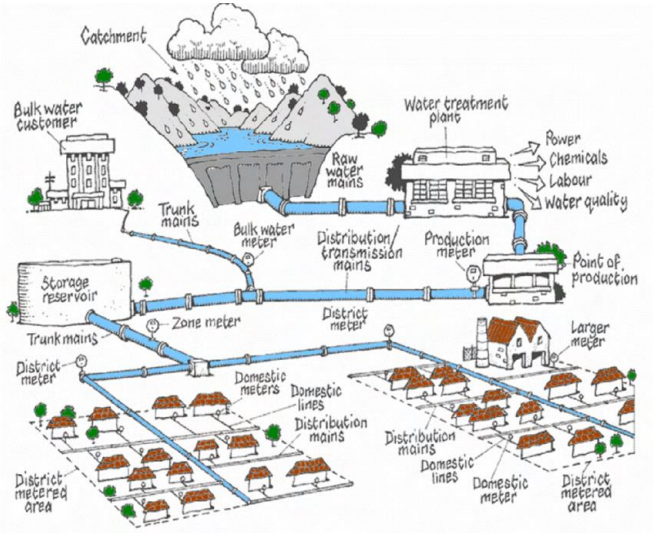
2. Other energy production and transmission



Problem: No heat

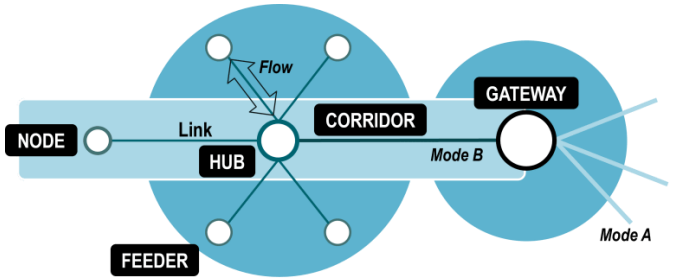
Key critical infrastructures 2

3. Water and wastewater



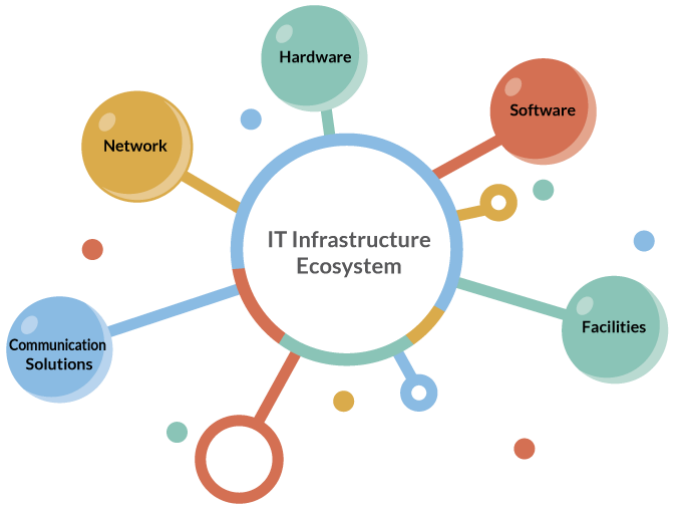
Problem: Too little, too much water, or it's dirty

4. Transportation



Problem: No transportation

5. ICT

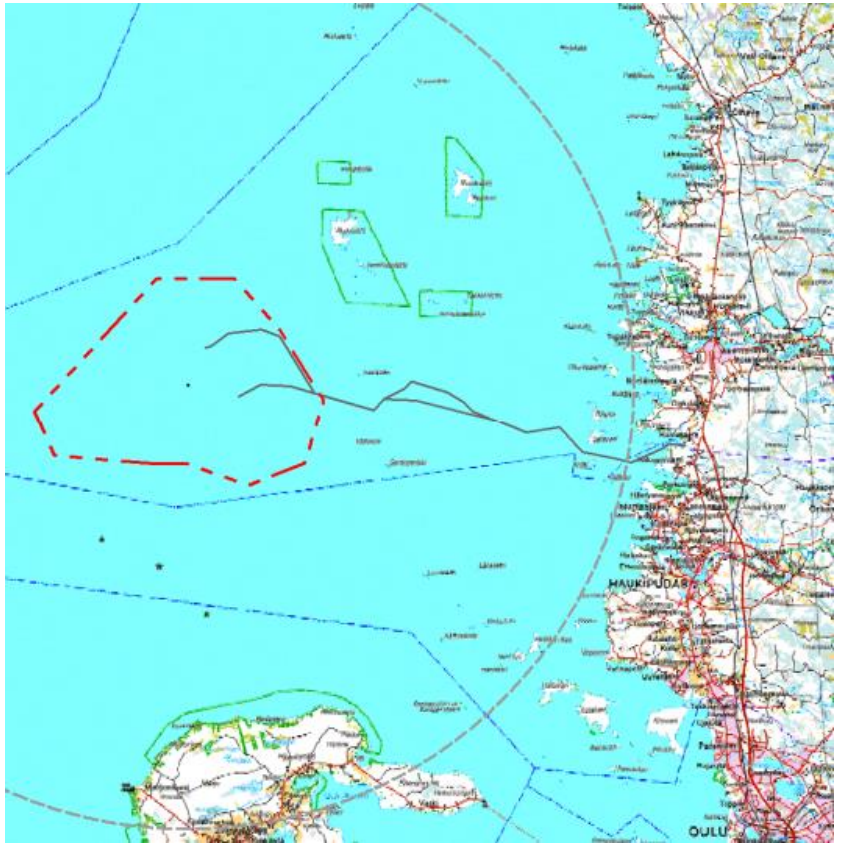


Problem: Neither I nor C

The green transition will generate new critical infrastructures

National hydrogen network

Offshore wind cabling



What threatens critical infrastructures?

1. Physical and Biological Natural Phenomena
2. Man-made physical threats
    1. Your own foolishness and the foolishness of those involved: Wrong design, wrong operation itself; naivety, lack of maintenance; misconduct of the parties involved
    2. Intentional action:
        1. On behalf of myself
        2. For the cause
        3. On behalf of the state
    3. Various megatrends and developments, e.g.
        1. Outsourcing
        2. The physical is replaced by contracts
        3. Reduced combustion makes energy storage more difficult

Hurricane knocked down a 400 kV pole in Eura, Finland (!)

Why the management is difficult?

- Massive and complex
- Several owners and decision makers
- Developed and built over decades
- Include technical infrastructure, services and production
- It is not in directly the interests of companies to prepare for society
- Completely dependent on other infrastructures and often also on maintenance and e.g. spare parts

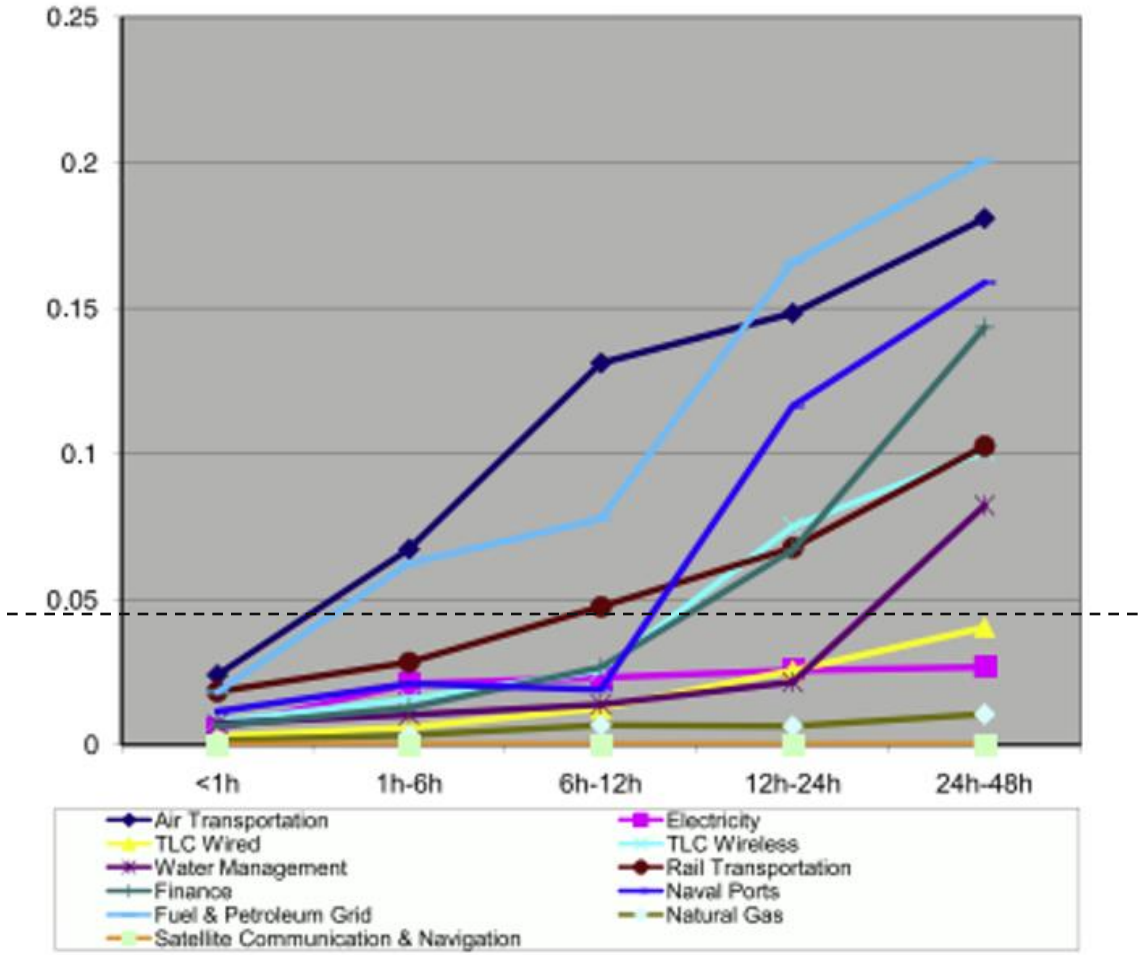


Fig. 4 – Dependency indices δ_i for various outage periods.

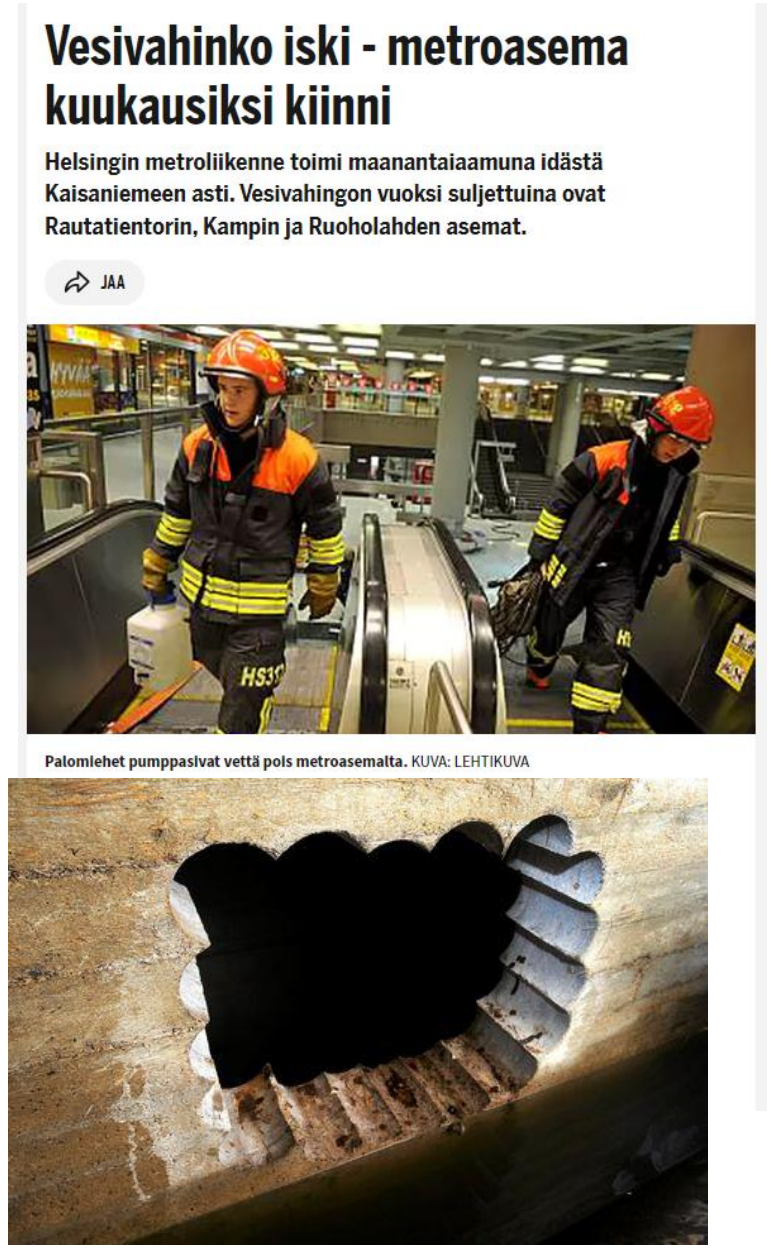
https://www.sciencedirect.com/science/article/pii/S1874548209000390

Dense urban structure causes significant location-based **dependencies**

- When infrastructures are located close to each other, one can break the other, or the same threat can break both
- E.g. 11.9. 2001:
  - Rescue operations were almost impossible due to traffic, debris and people
  - Mobile networks were overloaded
  - Damaged gas pipelines ignited countless fires
  - No extinguishing water was available because the water supply network was damaged

No eggs in one basket

- Dependencies are a key challenge for the protection of critical infrastructure
- Other dependencies:
  - **Physical dependencies**: almost all systems need electricity and society, especially in Finland, needs heat
  - **Cyber dependencies** and telecommunications infrastructure: If information is not transmitted, systems will be paralyzed
  - Dependency through **human decisions**
- Dependencies often arise insidiously, they are difficult to trace and they are only revealed when something happens



Vesivahinko iski - metroasema kuukausiksi kiinni

Helsingin metroliikenne toimi maanantaiaamuna idästä Kaisaniemeen asti. Vesivahingon vuoksi suljettuina ovat Rautatientorin, Kampin ja Ruoholahden asemat.

JAA

Palomiehet pumppasivat vettä pois metroasemalta. KUVA: LEHTIKUVA

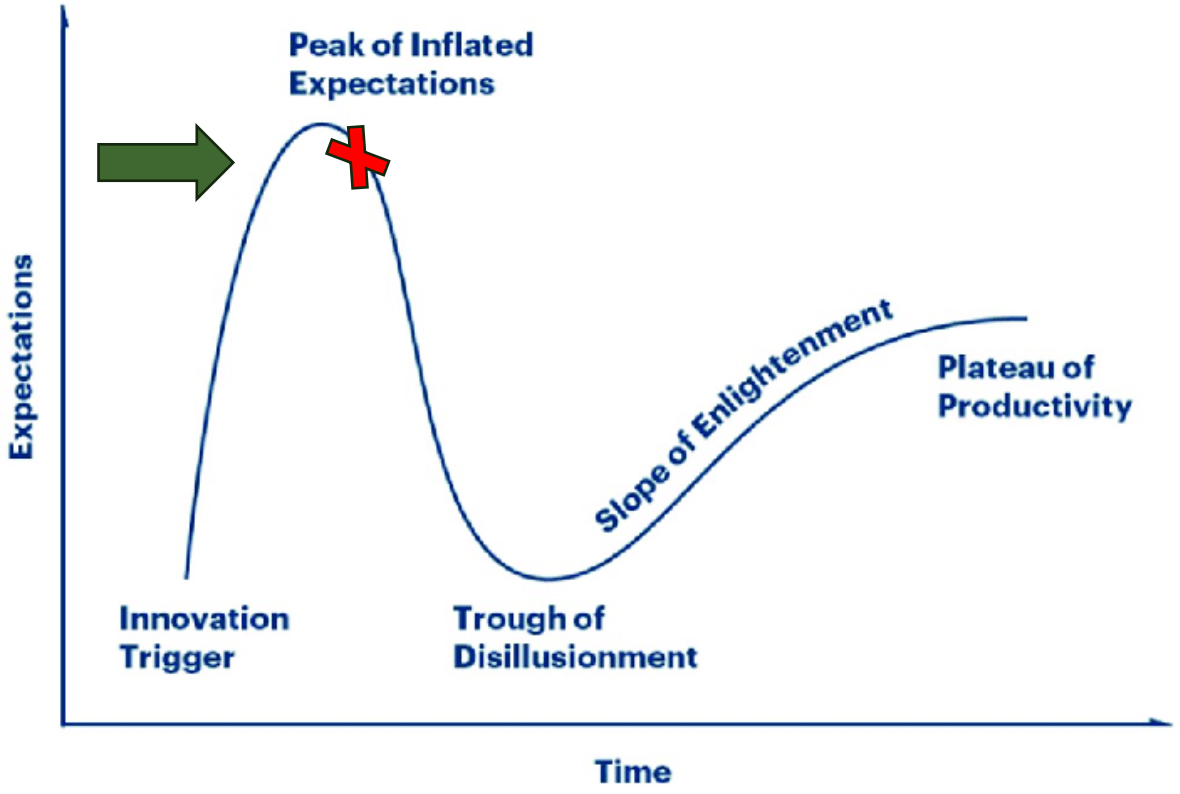
Rinaldi (2001)

SWECO

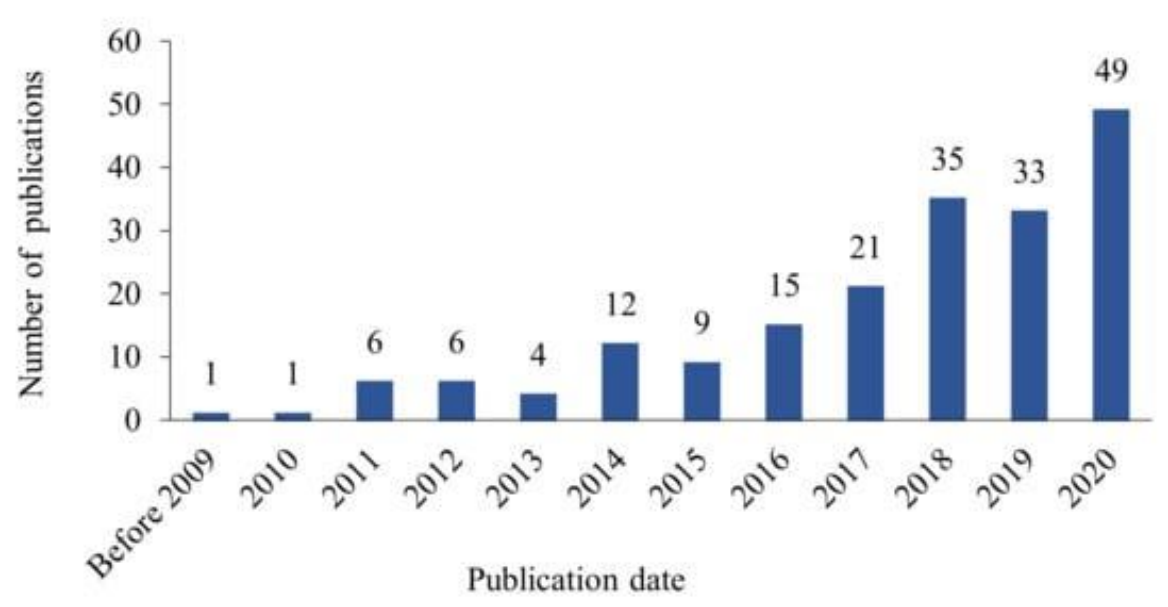
2. What about resilience?

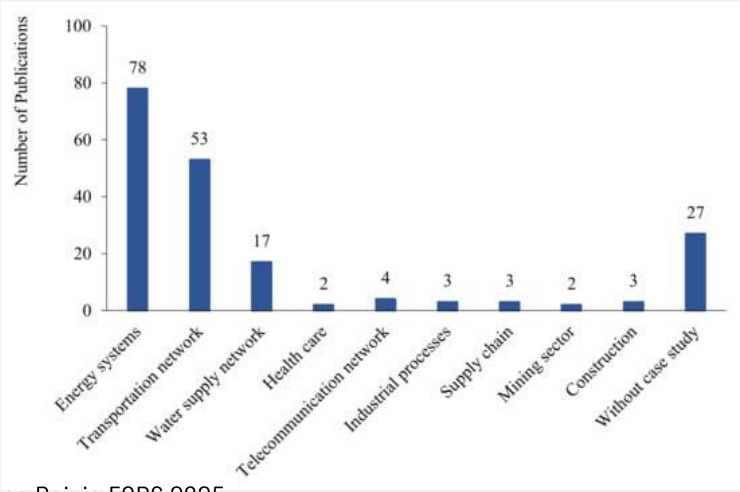
Resilience?

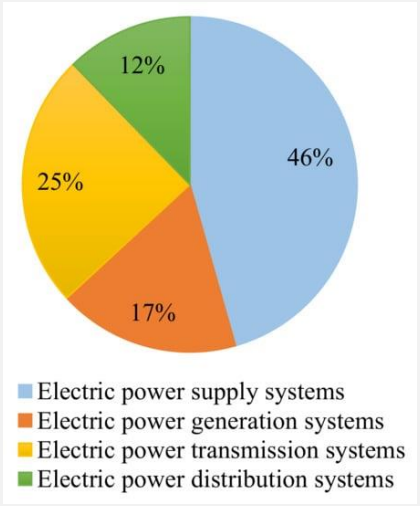
- Resilience refers to crisis resilience, crisis resilience, resilience, resilience, resilience, coping, resilience, resilience to change, mental resilience and mental resilience
- The basic idea is to focus more on the capabilities of the system and less on the threats that affect it or how to prevent them
- In order for the term to be meaningful, many things need to be addressed
- **A particularly difficult question is how to verify resilience**

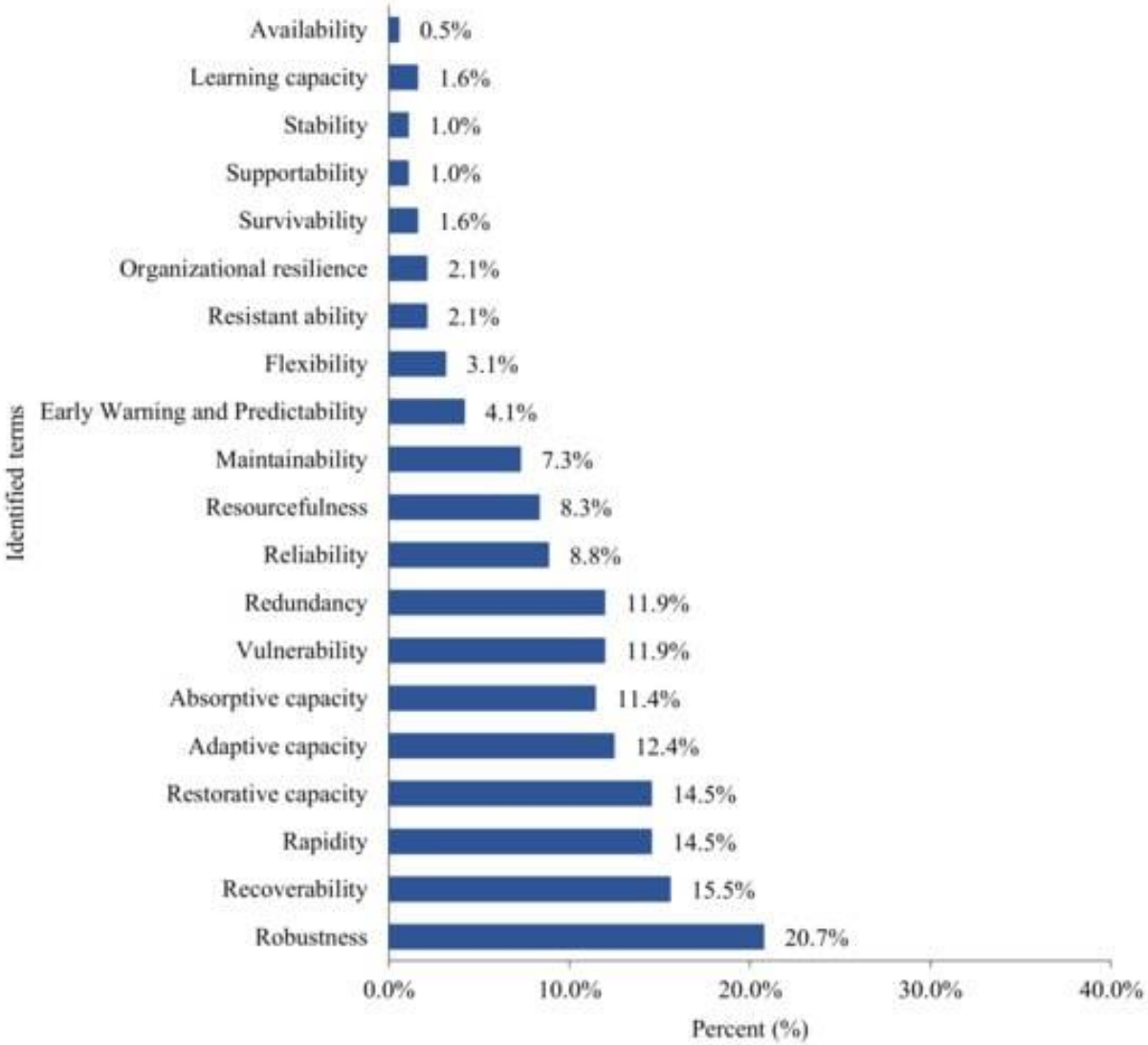


Resilience of critical infrastructures in the literature





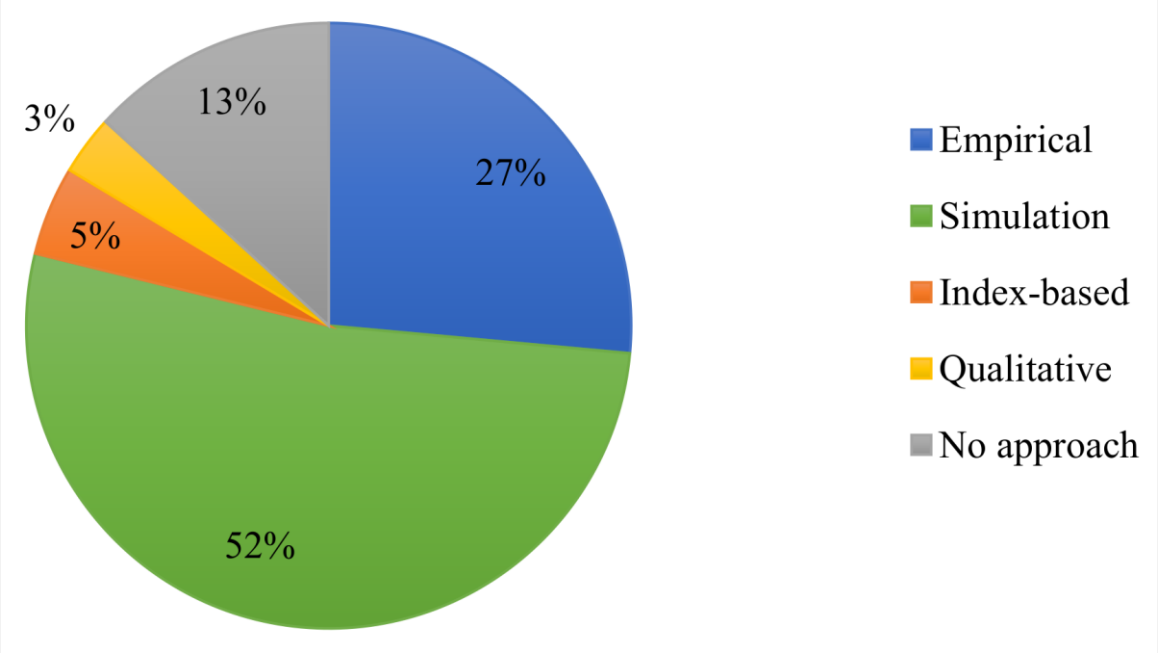




https://www.mdpi.com/1996-1073/14/6/1571

Approaches in the literature

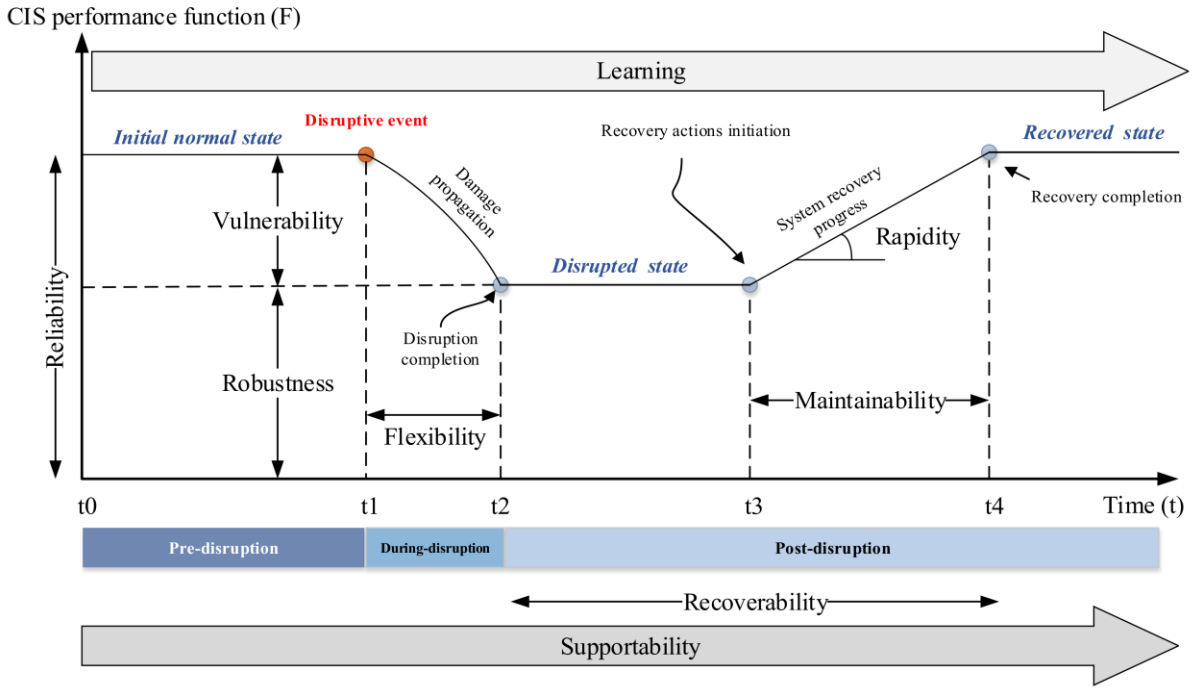
- **Simulation methods:** Simulation is used to study how the structure of CI affects its tolerance
- **Empirical approaches:** In empirical approaches, resilience is assessed using failure and recovery curves, which are usually determined by analyzing historical data
- **Index-based approaches:** Data from CI is structured into different KPIs
- **Qualitative approaches:** Attempting to assess the flexibility of CI without numerical descriptions



Resilience of critical infrastructures

Resilient critical infrastructure is characterised by the ability to

- Imagine what's coming
- Protect yourself from and resist disruption
- Dampen the effects of disruptions
- Adapt to new conditions and changes caused by disruptions
- Recover as quickly as possible



Resilience refers to the ability of a system to resist disruptions. The focus is on the features of the system. Difficult to verify.

Security usually means minimizing malicious events or threats and being prepared to deal with them as efficiently as possible. The focus is on external threats. Failure in particular is verifiable.

Resilience cheat sheet

Redundancy: Duplicate critical system components or ensure that different parts of the system are able to replace others

Diversity: Use a variety of techniques and approaches for mission-critical operations. If a particular threat compromises one technology, the others remain the same

Modularity and segmentation: Design systems in a modular way so that failures from one module do not transfer to others and repair is easier

Decentralization: Physically and logically separate functions to reduce the impact of connections

Ensure communication: Ensure that the system has several reliable communication methods

Flexibility and adaptability: Build systems that adapt to changing circumstances by changing their operations in the face of unexpected challenges (cross-train)

Regular stress testing: Test how the system works and reacts in extreme situations – fix the system according to the results

Real-time monitoring: Monitor the operating environment and performance to detect and respond to issues

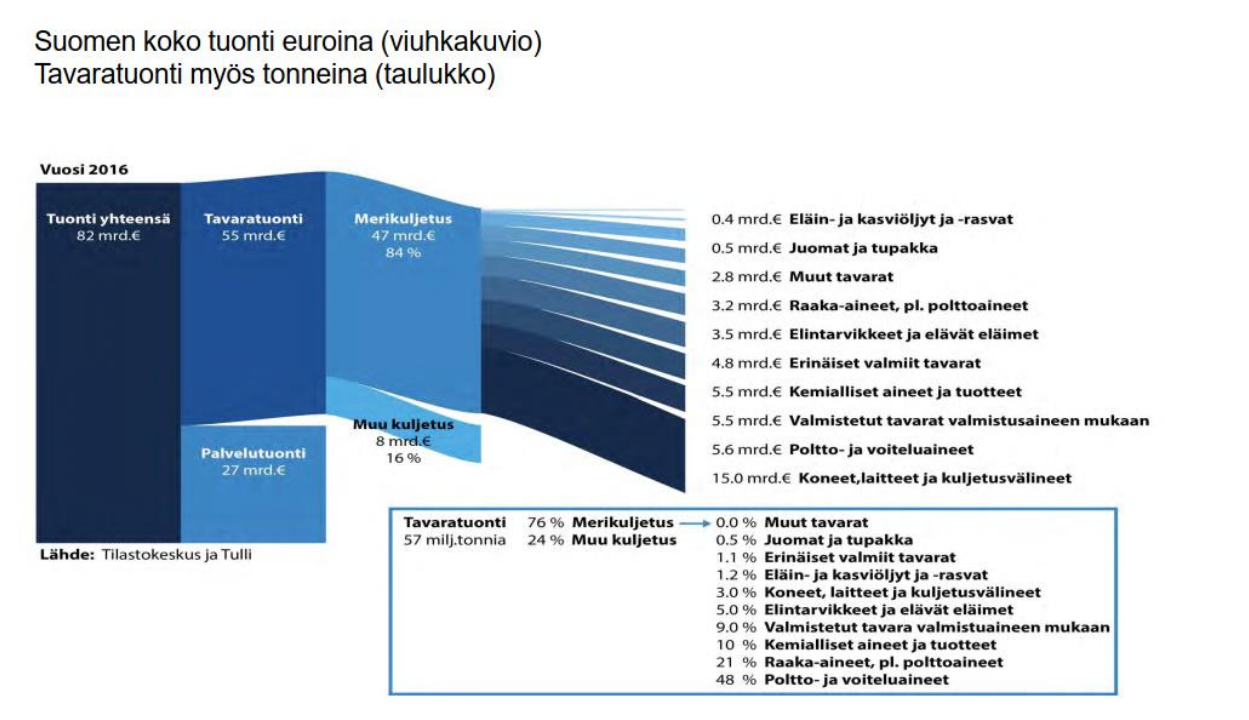
Contingency planning: Continuously develop detailed plans for various threat scenarios

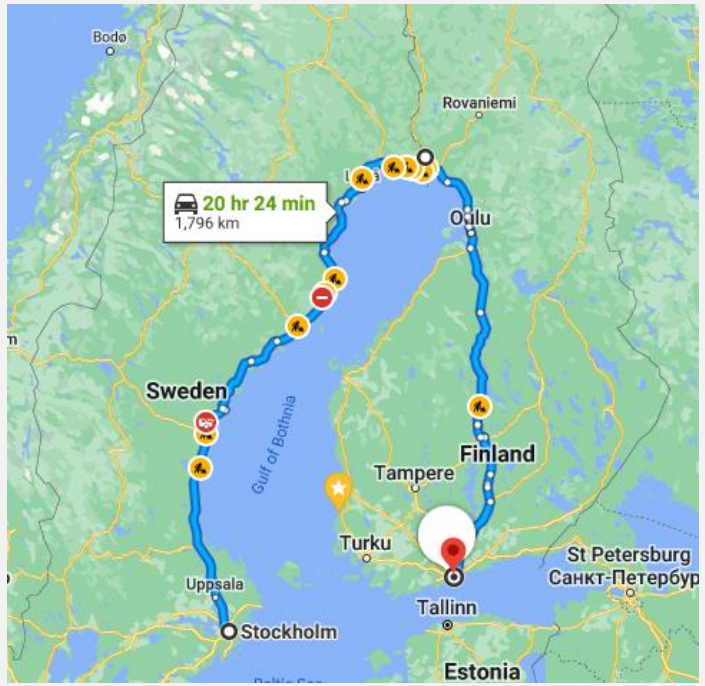
SWECO

3. Finnish Context

Geopolitical starting points 1: Finland is an island

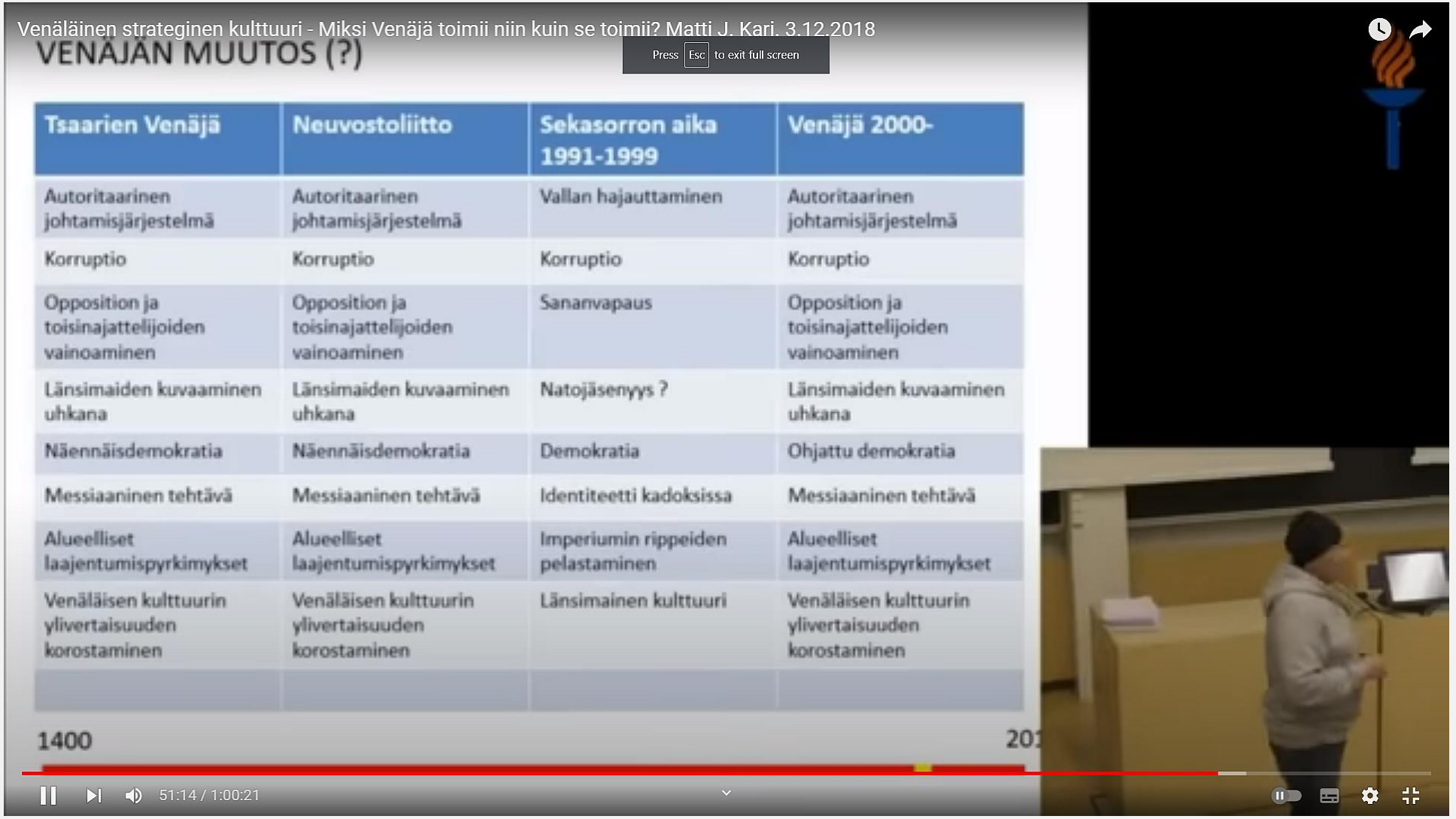
- 80% of Finland's freight traffic is transported by sea every year
- Finland is one of the few countries where all coasts freeze almost every year





Helsinki-Stockholm 400 km by water, 1796 km by land

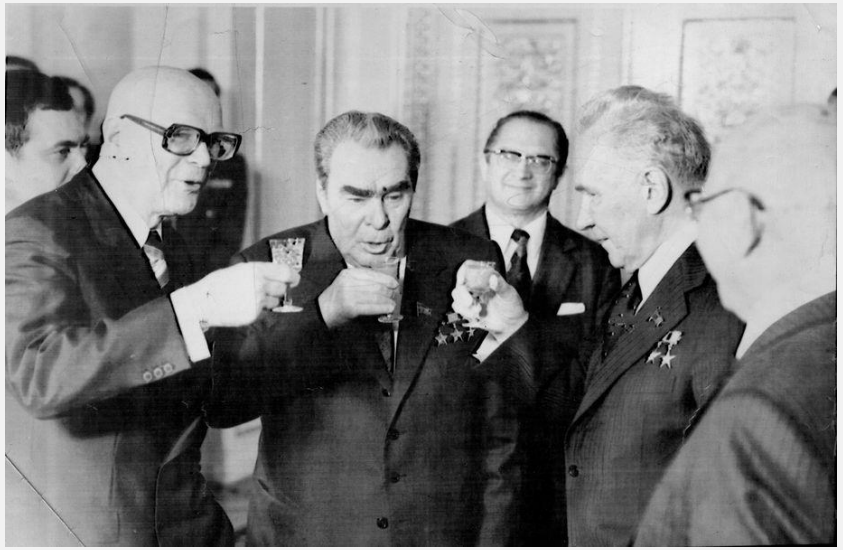
Geopolitical Starting Points 2: Russia's threat has been persistent



https://www.youtube.com/watch?v=uuFv-2KtGyI

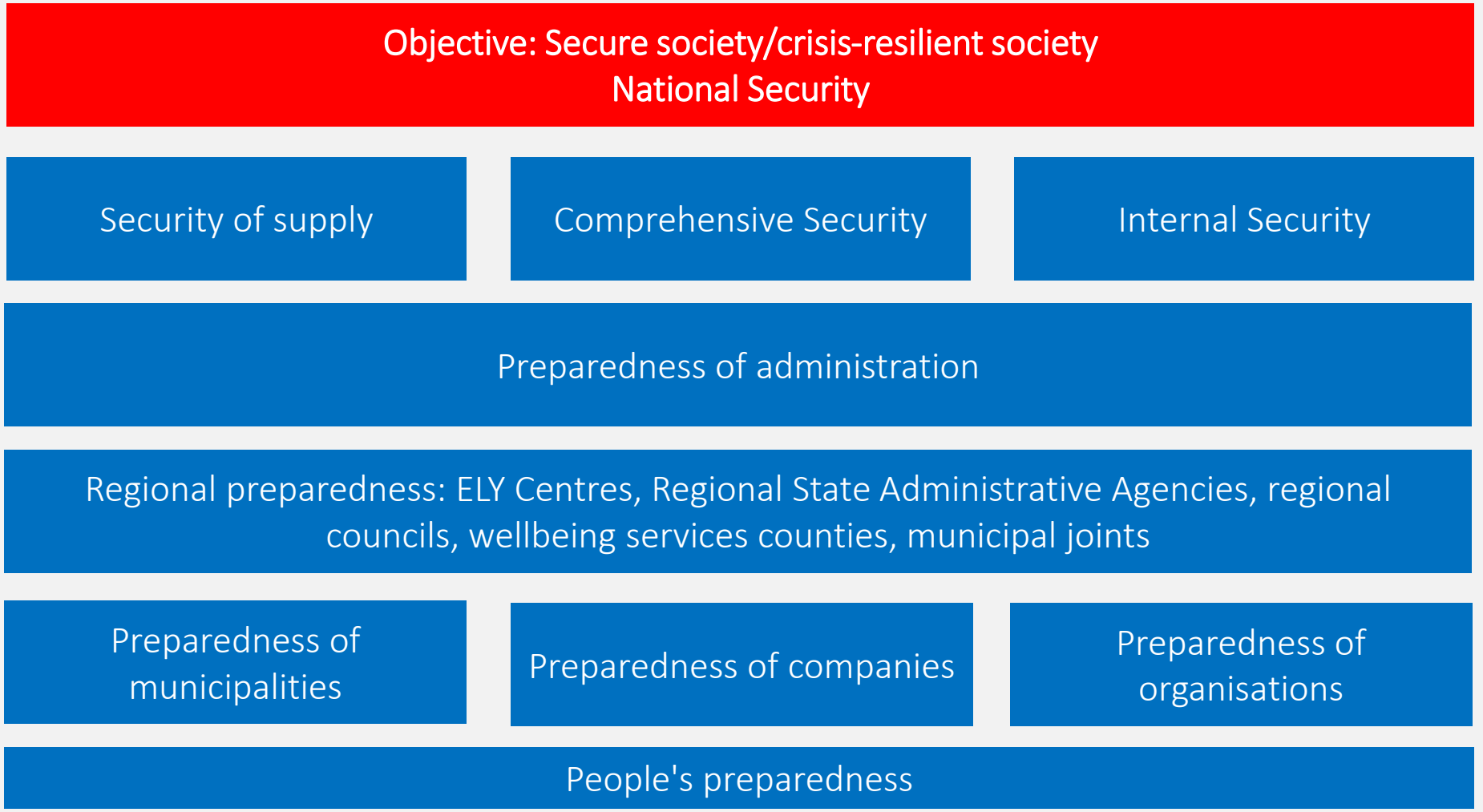
Geopolitical starting points 3: Finland has tried to be neutral

- No help in the Winter War, only compassion
- In the Continuation War, help was received that might not have been needed
- Because of the Soviet Union and Russia, Finland has had to balance between East and West for a long time
- Everyone can judge for themselves how they succeeded
- The recent history of preparedness in Finland stems from these rather desperate starting points
- It has been clear that Finland has had to prepare for difficult threats in a self-sufficient manner for a long time – this has naturally coloured where we are
- Now we are in EU and NATO



”Thou shall not trust unfamiliar help ”

CIP is widely visible in Finnish preparedness – yet not pronounced



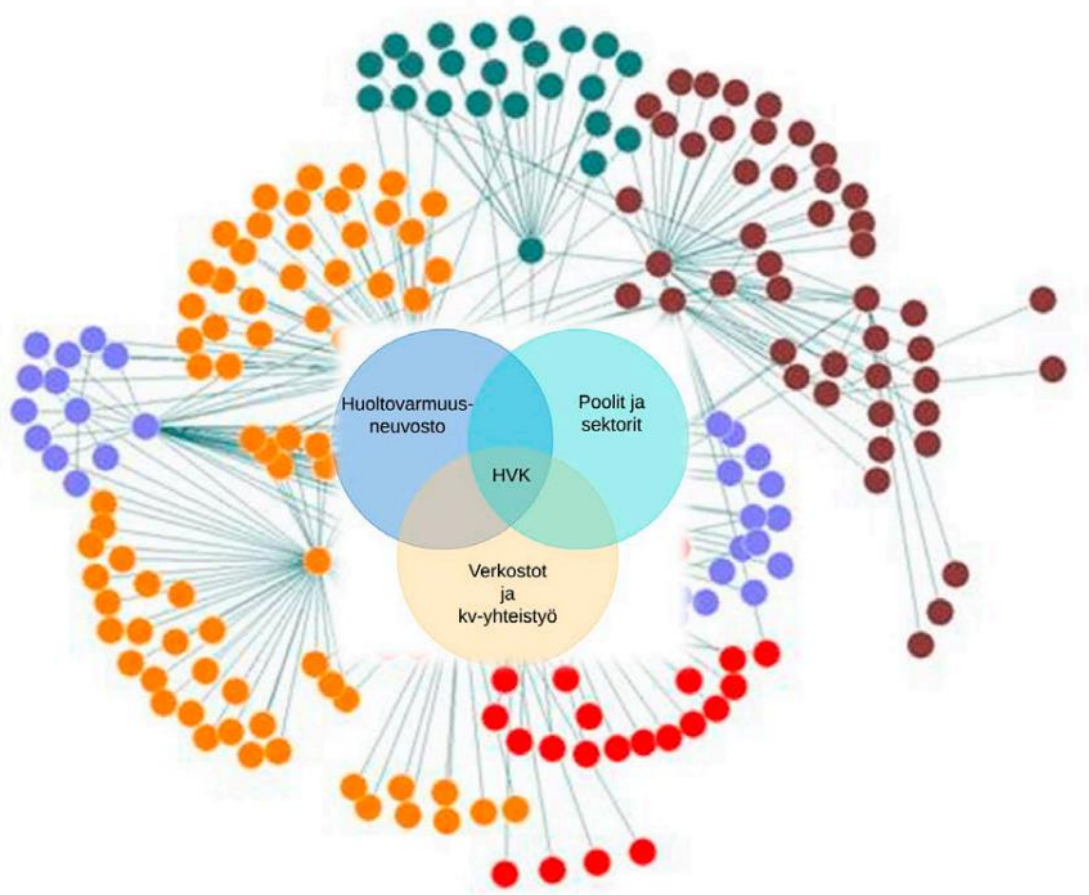
EU

NATO

SWECO

Security of Supply Organisation

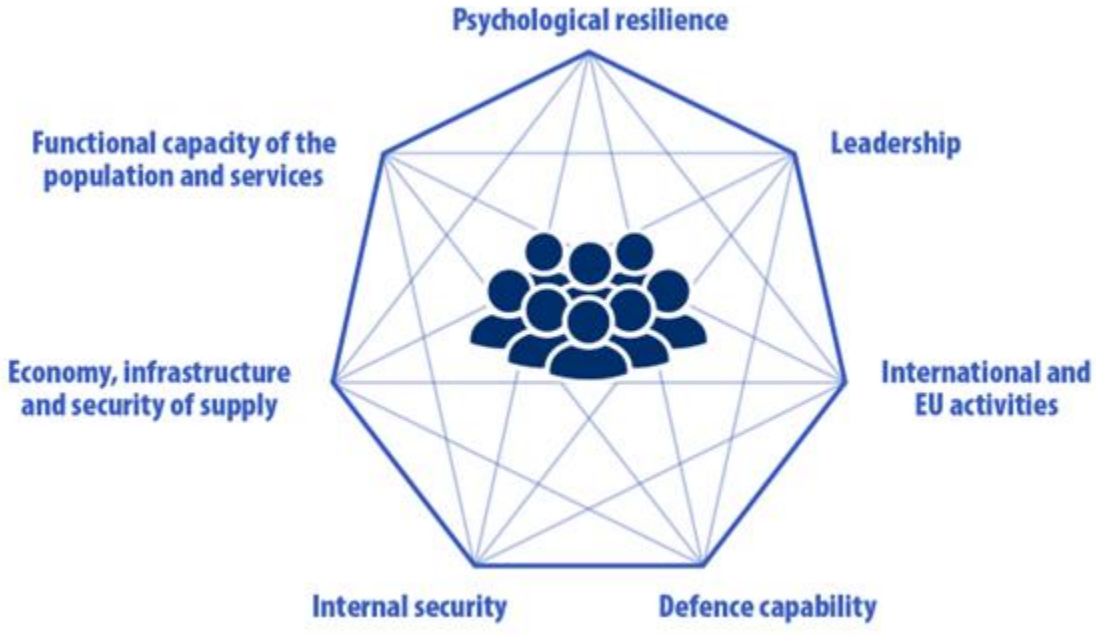
- The National Emergency Supply Organisation is a network that works together to promote Finland's operational capacity and the security of supply required by it.
- 1) The National Emergency Supply Council: A high-level expert group
- 2) Pools and sectors
  - Pools are bodies based on pool agreements between the National Emergency Supply Agency and business organisations or companies. Preparedness is based on regulations and voluntarily concluded pool agreements
  - The sectors are cooperation organisations formed by authorities, industry organisations and the most significant actors.
- 3) National Emergency Supply Agency



https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163181/TEM_2021_32.pdf?sequence=1&isAllowed=y

Comprehensive security: Security Strategy for Society

- The Security Strategy for Society describes the concept of comprehensive security
- The **vital functions of society** are taken care of in collaboration between the authorities, business community, organisations and citizens.
- Comprehensive security forms the foundation of resilience in Finnish society.
- The objective of the strategy is to provide all actors with a common framework for implementing comprehensive security from their perspectives



Internal Security

- The Ministry of the Interior's area of responsibility is internal security
- Rescue services, police, emergency response centre operations, border control, maritime search and rescue, immigration
- Regional administration's preparedness for disruptions and emergencies
- The Ministry of the Interior has been particularly interested in improving the resilience of society and how internal security actors carry out their duties in various critical infrastructure disruptions (preparedness in their own sector)
-

What about Critical Infrastructures?

- National critical infrastructures have not been defined unambiguously, and there is no specific CI authority
- CI has been successfully interlaced with the three pillars above
- However, the EU *Critical Entities Resilience directive CER* is now being implemented
- There will be a national point of contact for CIP, most likely NESA

Resilience starts with planning

1. Taking resilience into account in design

- New threats
- New standards
- Innovative solutions
- Cost effectiveness

2. Ensuring resilience in implementation

- What is caused to other infras
- Shortcuts and ad hoc solutions that jeopardise resilience
- Continuous monitoring

3. In-service asset, risk and resilience management

- Asset management
- Identifying, analysing and managing risks
- Real-time monitoring
- Contingency planning
- Stress testing
- Continuous improvement

The earlier resilience is taken into account, the better the end result