VALTIONEUVOSTO
STATSRÅDET

Cybersecurity strategy of Finland and railways

1.12.2025 ERA-ENISA cybersecurity conference, Tallinn / Estonia

Janne Hauta / Ministry of Transport and Communications Finland

Structure of Presentation

1. Finland´s ex-president Sauli Niinistö´s report on Preparedness and Readiness of the EU
2. Cooperation in the field of cybersecurity between different public authorities and private businesses in Finland
3. Cybersecurity on Railway sector in Finland / Digirail, standard´s and stakeholders

Report on Preparedness and Readiness of the EU

Special adviser Sauli Niinistö to the president of the European Commission (von der Leyen)

- All relevant military and civilian crisis response actors need to be fully ready and capable to respond effectively and seamlessly
- A higher level of preparedness is needed across the board

Preparedness is an attitude

- Preparedness may be misunderstood as a separate policy area.
- Preparing for the risk is not escalatory.
- Preparedness requires **a high level of trust**. Not only internally, but with external partners.

Report on Preparedness and Readiness of the EU

Preparing for the worst-case scenarios: Pandemic, war of aggression, climate change. Hybrid, cybersecurity, sabotage.

Shifting to comprehensive preparedness: **All-hazard, whole-of-government, whole-of-society approach**. => Under all circumstances.

Putting citizens at the core of preparedness. Empower citizens in different roles and capacities. Private sector as operators of critical infrastructure and services.

Safer together: **Threats don’t stop at the borders.**

Cooperation as the bedrock of success

National cybersecurity coperation and preparedness is coordinated by the **Office of the National Cyber Security Director**.

ISAC network (Information Sharing and Analysis Centre) Cooperation network consisting of over 300 organisations. ISAC activities and information sharing is voluntary based.

Public authorities cooperation group, cybersecurity

CRIME INTELLIGENCE

INFORMATION EXCHANGE Business community, public sector and citizens

Police
Cyber crime prevention

Government cyber coordination:
National Cyber Security Director and key ministries

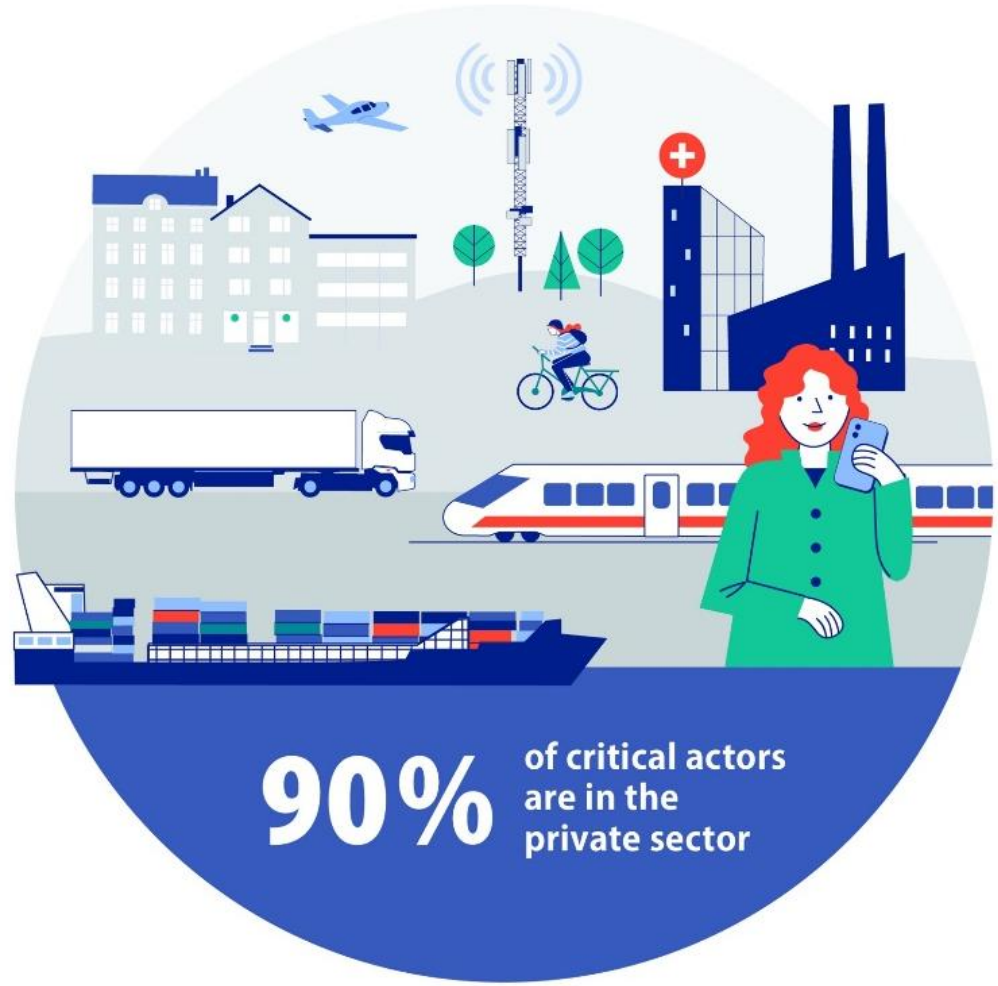
TRAFICOM
Finnish Transport and Communications Agency
National cybersecurity situational awareness and ISAC networks

SUPO
Finnish Security and Intelligence Service SUPO
Intelligence and counter intelligence

NETWORK TRAFFIC INTELLIGENCE AND THREAT AWARENESS

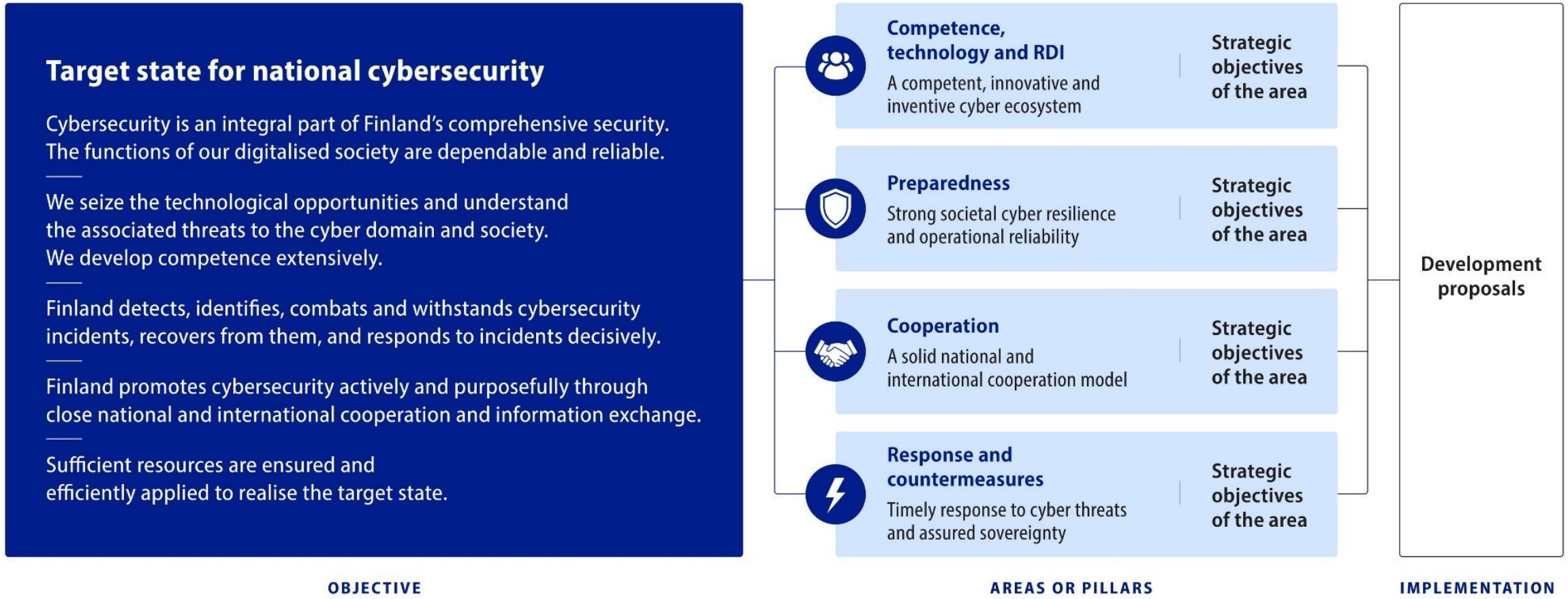
Finnish Defence Forces
Military cyber defence, defence intelligence

Critical national infrastructure, networks and services



90% of critical actors are in the private sector

The main goals for national cybersecurity and the structure of the new strategy

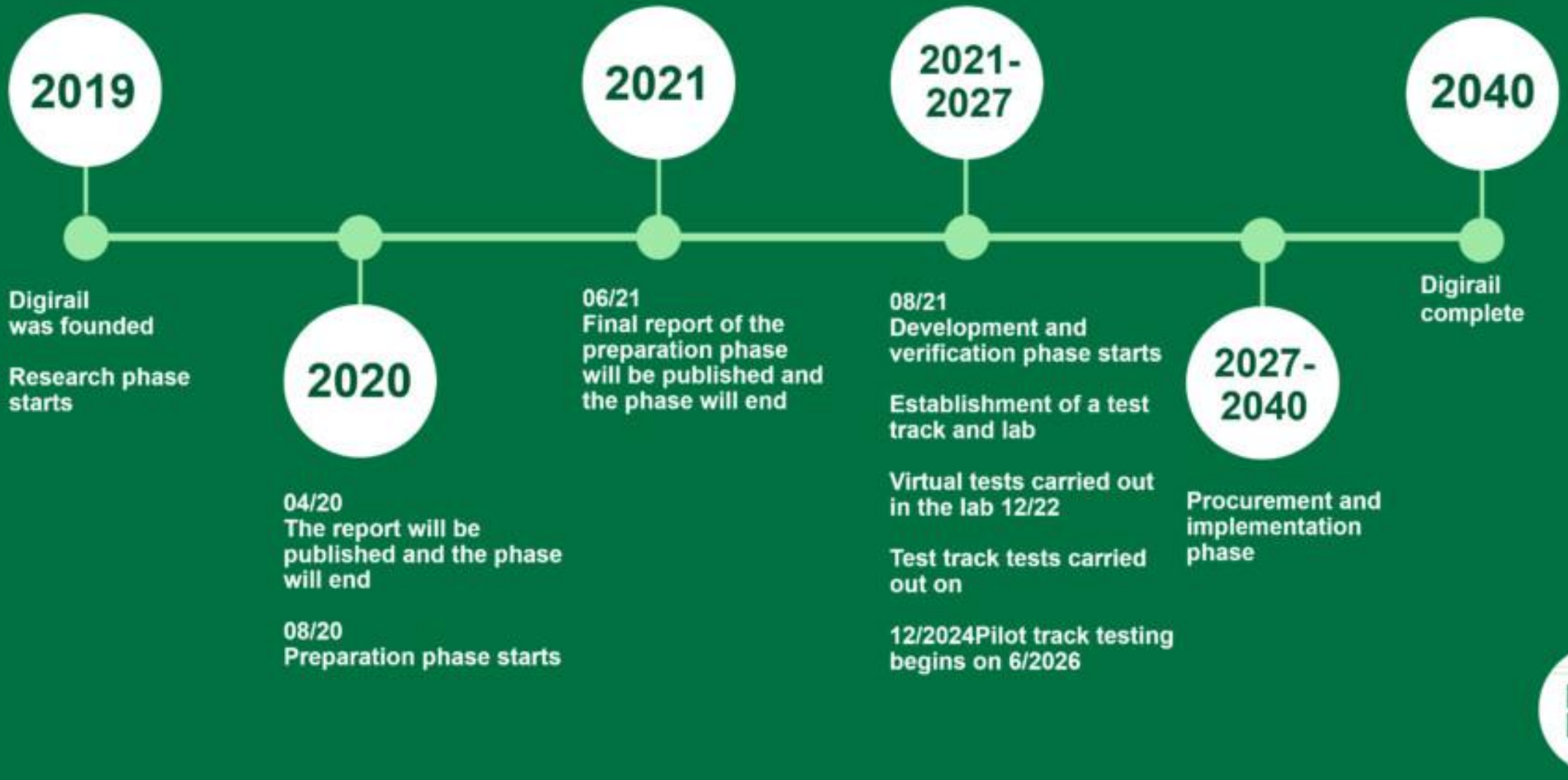


Finish national ERTMS-program- Digirail 1/2

- Ministry of Transport and Communication Finland owns this project, but
  - *It has been organised alliance-construction between Infra Manager Finland Transport Infrastructure Agency (FTIA) and traffic control operator Fintraffic Rail Ltd.*
- All main stakeholders involved from the day one.
- “Cybersecurity by Desing”
  - Railway cybersecurity standardization as a framework (TS 50701 / draft IEC 63453)
  - Active contribution to the EUG cyber and standardisation working groups
- Close co-operation with NSA (railway safety, cyber, and resilience)

Digirail Roadmap

Funded by the European Union
NextGenerationEU



DIGI RAIL

Finish national ERTMS-program- Digirail 2/2

- Digirail is not merely a railway signalling or interlocking project based on hardware: Impacts extend across the entire railway system:
- *Rolling stock*
- *Telecommunications (the Pre-FRMCS solution based on commercial radio networks)*
- *Traffic management (software)*
- *Harmonised operational practices.*
- **<= Digitalization means new type of cybersecurity solutions and preparedness**
  In Finland, innovative and cyber-secure solutions are being developed that can serve as a model for the broader evolution of Europe’s railways

The participating companies are jointly contributing to the creation of unique solutions for the railway market.

Military mobility and cybersecurity

EU put more emphasize to military mobility:

Target to develop the EU's resilience and defence readiness to improve its ability to respond to security threats.

Railway cybersecurity is an essential enabler of military mobility

⇒How TSI´s should react to cyber threads of digitalized railway infrastructure and ensure operational capability in all situations

⇒It´s not limited to operational systems

⇒Protecting information and mission-critical data

⇒Preparing for hybrid threats and hostile cyber activities

Summary

- Preparedness is attitude (requires **a high level of trust)**
- Cooperation as the bedrock of success
- Preparing for the worst-case scenarios
- Railways need new type mindset because digitalisation (Hardware to Software)
- Finland creates innovative and cyber-secure railway system for the broader evolution of Europe’s railways,
- **Safer together: <u>Threats don’t stop at the borders</u>**