Region Stockholm

Proactive Collaboration within the transport sector is needed for managing resilience and operational efficiency under NIS2 and CER Directives

Anders Jonsson

Mob: +46708655301

Anders.h.Jonsson@sl.se

- SL responsible for NIS2/CSL readiness (consultant)
- Member AHWG EUCS & WG for AI (ENISA)
- Previously has a long internationally career in IT, Tech and software development.

EU – CYBERSECURITY STRATEGY

STRATEGY

2008 **2013** **2016** **2019** **2022** **2026..**

CER Directive
- Energy/Transport

GDPR
NIS1

CSA
Cyber Security Act

NIS2
CER*

CSA (EUCC/EUCS/5G)
Cyber Resilience Act
AI Act
Chips Act
Etc..

***CER:DIRECTIVE (EU) 2022/2557**
Public transport — Public transport undertaking as defined in Article 2(d) of Regulation (EC) No 1370/2007 of the European Parliament and of the Council.

Definition: EC 1770/2007 (Art 2d):
Public transport undertaking: a public or private undertaking, or a public or private group of undertakings, which operates public transport, or a public body which provides public transport services.

If you are included in the annex of CER directive you are also identified as an essential entity under NIS2.

The goal with the EU's Cybersecurity strategy is:

1. Strengthen Europe's resilience to cyber threats

- Protect networks, information systems, and critical infrastructure (energy, transport, health, finance, etc.).
- Ensure all Member States reach a common high level of cybersecurity through NIS2 & CER Directives.

2. Build collective defence and response capabilities

- Improve cooperation and information-sharing among EU countries, the private sector, and EU institutions.

3. Secure digital technologies and supply chains

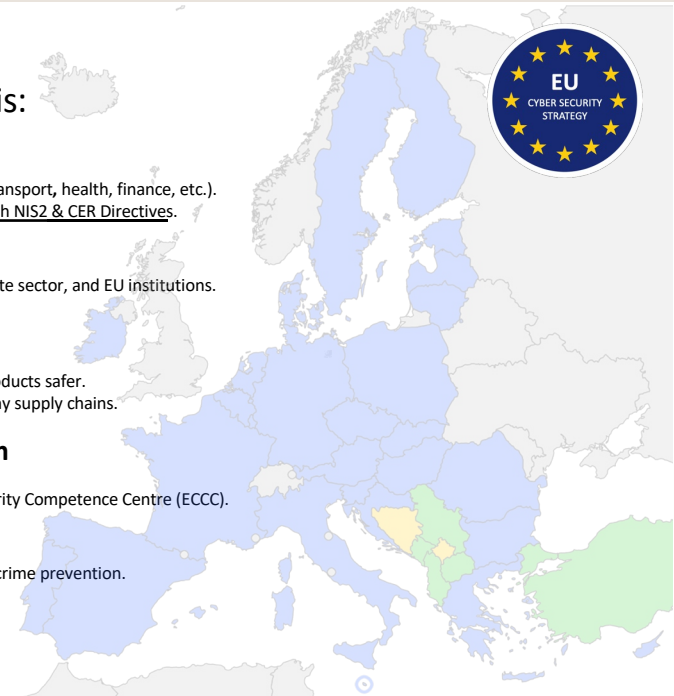
- Promote "security by design" in digital products and services.
- Introduce the Cyber Resilience Act (CRA) to make hardware and software products safer.
- Reduce Europe's dependence on non-EU technologies and ensure trustworthy supply chains.

4. Develop skills, awareness, and a strong cyber ecosystem

- Invest in education, training, and workforce development in cybersecurity.
- Support innovation, startups, and research through the European Cybersecurity Competence Centre (ECCC).

5. Promote a global, open, and secure internet

- Strengthen international cooperation on cyber norms, diplomacy, and cybercrime prevention.

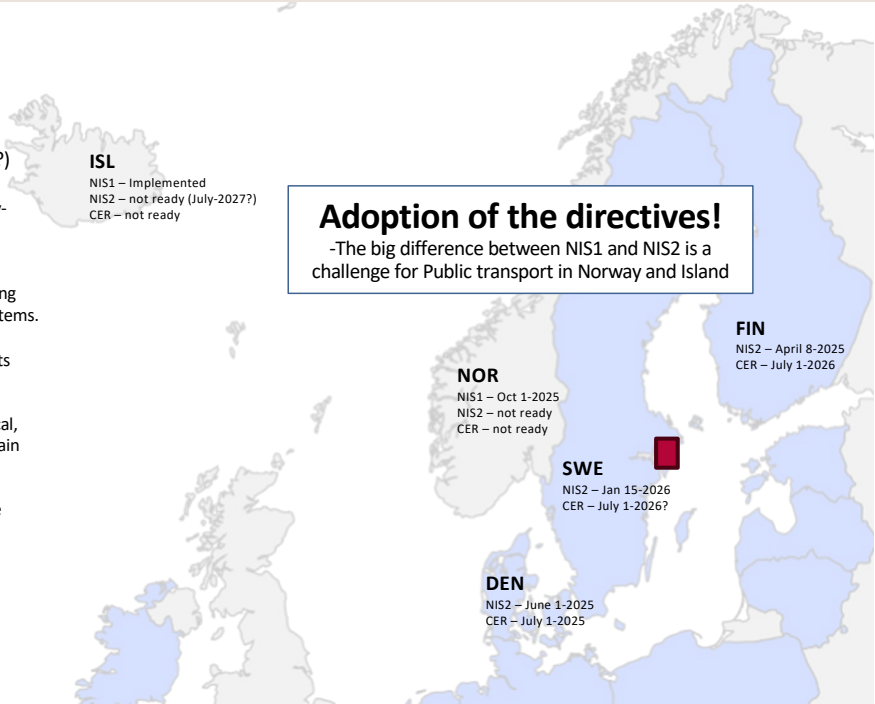


Key Requirements & Preparations

(Will NIS2 and CER be adopted to Norway/Island under EEA?)

Even before formal legal adoption, should organizations in Norway-Island begin preparations for compliance based on what NIS2 will require?...Including:

- **RISK MANAGEMENT**: Carrying out risk assessments, mapping threats and vulnerabilities of all network & information systems.
- **INCIDENT REPORTING**: Obligations to report major incidents quickly to competent authorities / CSIRTs, within 24h.
- **ORGANIZATIONAL SECURITY MEASURES:** Including technical, operational and organizational security, covering supply chain risk, backup, resilience.
- **GOVERNANCE RESPONSIBILITY**: Management / board have clearer/responsible duties under NIS2.
- **SUPERVISION & PENALTIES**: Expect stronger regulatory oversight & significant fines for non-compliance.



The pillars of the NIS2 directive

National responsibility:

Each member state shall designate a responsible authority against EU/ENISA. Develop a National Crisis/Contingency strategy and set up a National Cybersecurity Center including identify supervisory authorities per sector.

MSB (SWE)

NCSC

Supervisory authorities per sector

Entity's responsibility

Each identified entity is required to comply with the CER/NIS2 according to instructions developed by the sector specific authority. Include following:

Accountability at the top management

Organizations need to implement security measures, including the supply chain

Reporting of significant incidents is mandatory, including the supply chain

Risk & Vulnerability Analysis based on “all-risk”

Continuity planning

Background checks

Every entity's responsibility

Collaboration

To achieve increased resilience, collaboration is required across the entire transport sector. To be able to resist/get help in the event of attacks, we need collaboration within both Sweden and at the EU level.

Sector specific collaboration NIS2 & CER

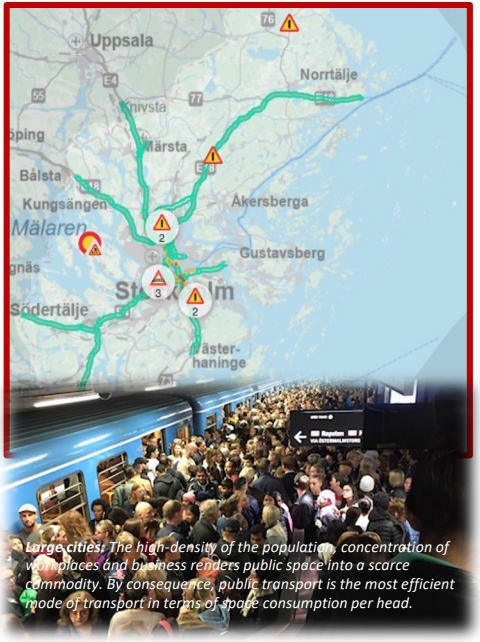
Vulnerability handling/register

National collaboration
CSIRT network

Proactive Collaboration within the rail-bound public transport sector has been a success for mange resilience and operational efficiency in Sweden.

*”When we began working with **NIS2 directives**, we quickly recognized that rail-bound public transport, **particularly in large cities**, plays an even more critical role for functioning of other essential sectors than traditional railway services”*

TRANSPORT STYRELSEN
TRAFIKVERKET
SJ
SL
MSB
Tågföretagen
MTR
CONNECTING STOCKHOLM
Göteborgs Stad
green cargo



Large cities: The high-density of the population, concentration of workplaces and business renders public space into a scarce commodity. By consequence, public transport is the most efficient mode of transport in terms of space consumption per head.

Public transport in Metropolitan area of Stockholm

2.5 Miljon boarding passengers per working day - 2025

- Metro: 439 metro cars (39%)
- Bus: 2,396 vehicles (38%)
- Commuter train: 129 cars (15%)
- Tram/Local train: 120 cars (8%)
- Boat: 25 vessels + 50 chartered (<1%)

* (1.5 M Saturdays - 1.2 M Sundays)

Public transport plan Stockholm 2050*
Work trips: Increase from 56% in 2015 – to 64% in 2050
Business trips: Increase from 43% in 2015 – to 57% in 2050
(School trips: 93% in 2015 to at least 93% in 2050)

*Public Transport Plan 2050 is the Stockholm Region's long-term plan for the development of public transport from 2030 to 2050.

Areas in scope of sector specific collaboration:

- **Collaboration on cybersecurity training** (IT/OT) and participation in various European programs/groups
- **Develop and share a common method for NIS2.** How to identifying and assessing critical functions-IT & OT services
- **Analyze incident and report hierarchy.** When is the incident critical enough to report? and who does what?
- **Data-driven dynamic maintenance reduces costs.** But it can also increase resilience!
- **What can we learn from each other about AI**, share experience within our sector.
- **NIS2 versus National security legislation - c**ollaboration and consensus are needed.

Starting point for assessing critical functions, critical systems and incident reporting

Incident notification within 24h
Iincident report within 72h
Full report within 30 days

Significant incident (NIS2):

An incident shall be considered to be significant if:

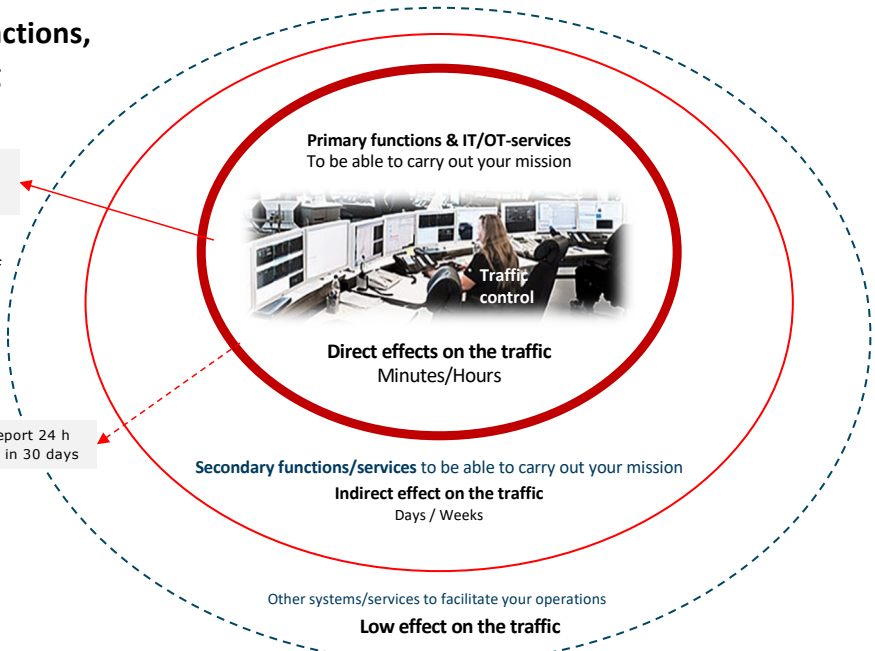
- it has caused or can cause severe operational disruption of the services (public transport) or financial loss for the entity concerned;
- it has affected or can affect other natural or legal persons by causing considerable material or non-material damage

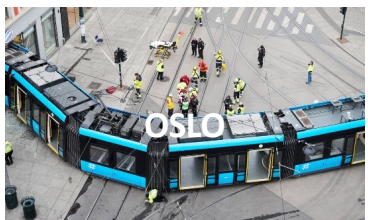
Incident report 24 h
Full report in 30 days

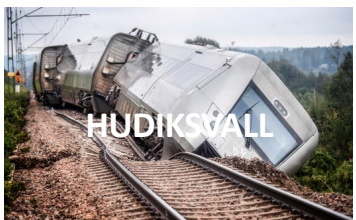
Significant incident/disruptive effect (CER):

For significant incident, the following should be considered:

- the number of users relying on the essential service
- **the extent to which other critical sectors depend on the essential service in question**
- the duration of the disruption, and
- the geographical area affected by the disruption, considering whether the area is geographically isolated.







When is the incident “**critical enough”** to report, according to the new Directives?

A notification within 24h!

Proactive Collaboration within the Nordic transport sector can make it easier to manage resilience in the community!

THANK'S

Anders Jonsson
Mob: +46708655301
Anders.h.Jonsson@sl.se

- SL responsible for NIS2/CSL readiness (consultant)
- Member AHWG EUCS & WG for AI (ENISA)
- Previously has a long internationally career in IT, Tech and software development.