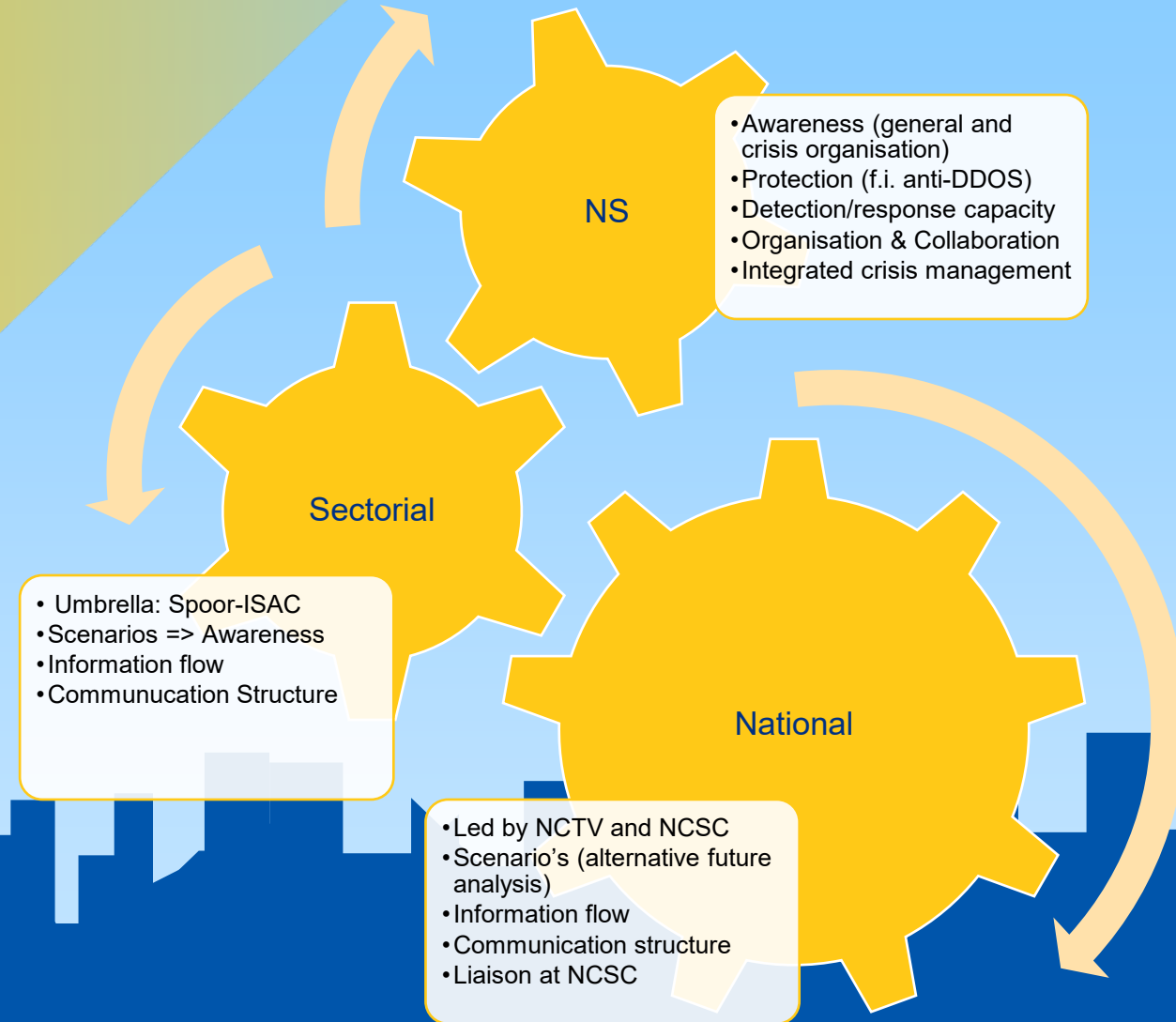# Cyber Crisis Management

Joseph Mager, manager Cyber Governance

Nederlandse Spoorwegen N.V.
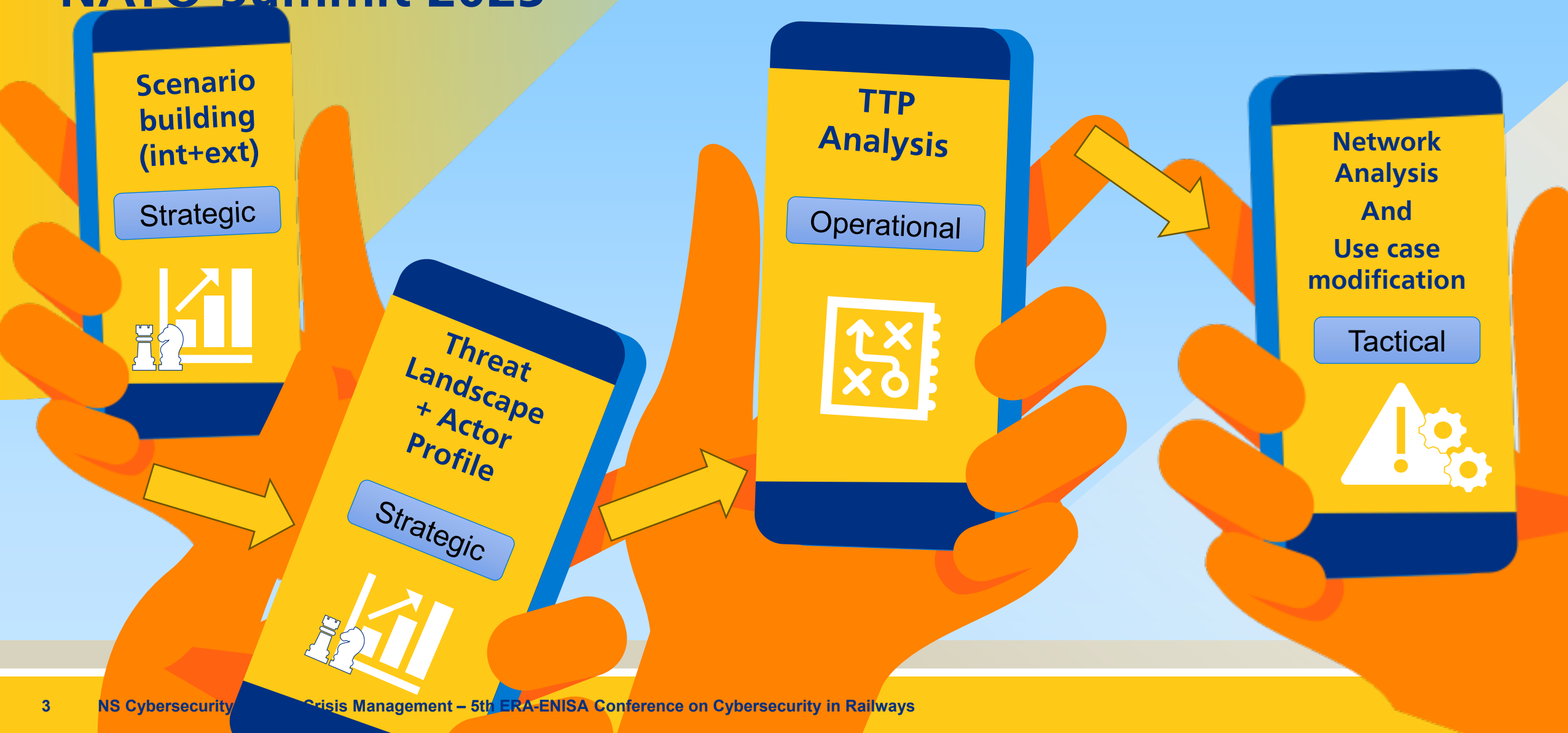
NATO Summit: Preparation
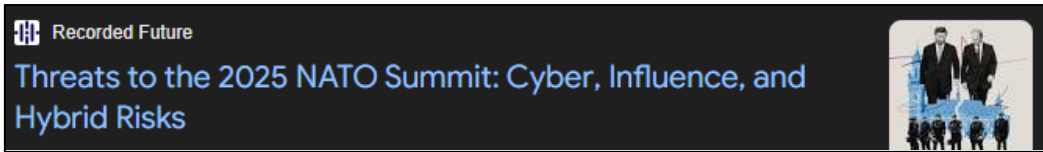
NS
- Awareness (general and crisis organisation)
- Protection (f.i. anti-DDOS)
- Detection/response capacity
- Organisation & Collaboration
- Integrated crisis management

Sectorial
- Umbrella: Spoor-ISAC
- Scenarios => Awareness
- Information flow
- Commmunucation Structure

National
- Led by NCTV and NCSC
- Scenario's (alternative future analysis)
- Information flow
- Communication structure
- Liaison at NCSC

CTI based preparation
NATO Summit 2025

Scenario building (int+ext) — Strategic

Threat Landscape + Actor Profile — Strategic

TTP Analysis — Operational

Network Analysis And Use case modification — Tactical

NATO Summit: During the Summit
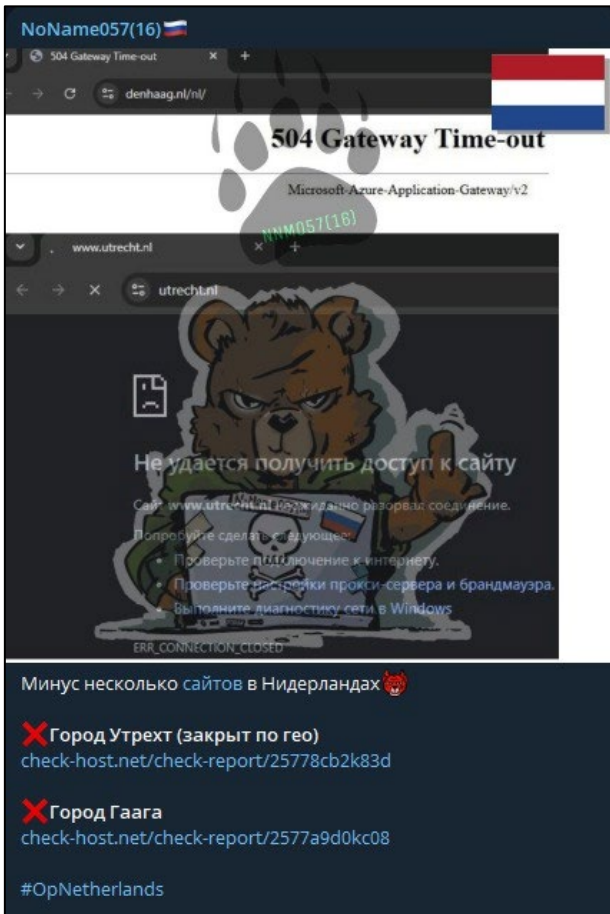
Hoe spannend werd het tijdens de NAVO-top?

De NAVO-top in Den Haag verliep op het oog misschien rustig – achter de schermen gebeurde er van alles. Wat ging goed, wat ging mis en hoe spannend werd het?

Zo is NS georganiseerd
Vanuit de NS-meldkamer houdt het Landelijk Calamiteiten Coördinatie Team (LCCT) de situatie nauwlettend in de gaten. Korte lijntjes zijn er met teams van ProRail en Politie op het OCCR. Op Den Haag Centraal staan teams van Veiligheid & Service (V&S) en de politie paraat.

NATO Summit: the aftermath

- Informing all employees on approach

- Evaluation of lessons learned
  - Positive: collaboration at all levels

- Reuse of approach for other (major) events

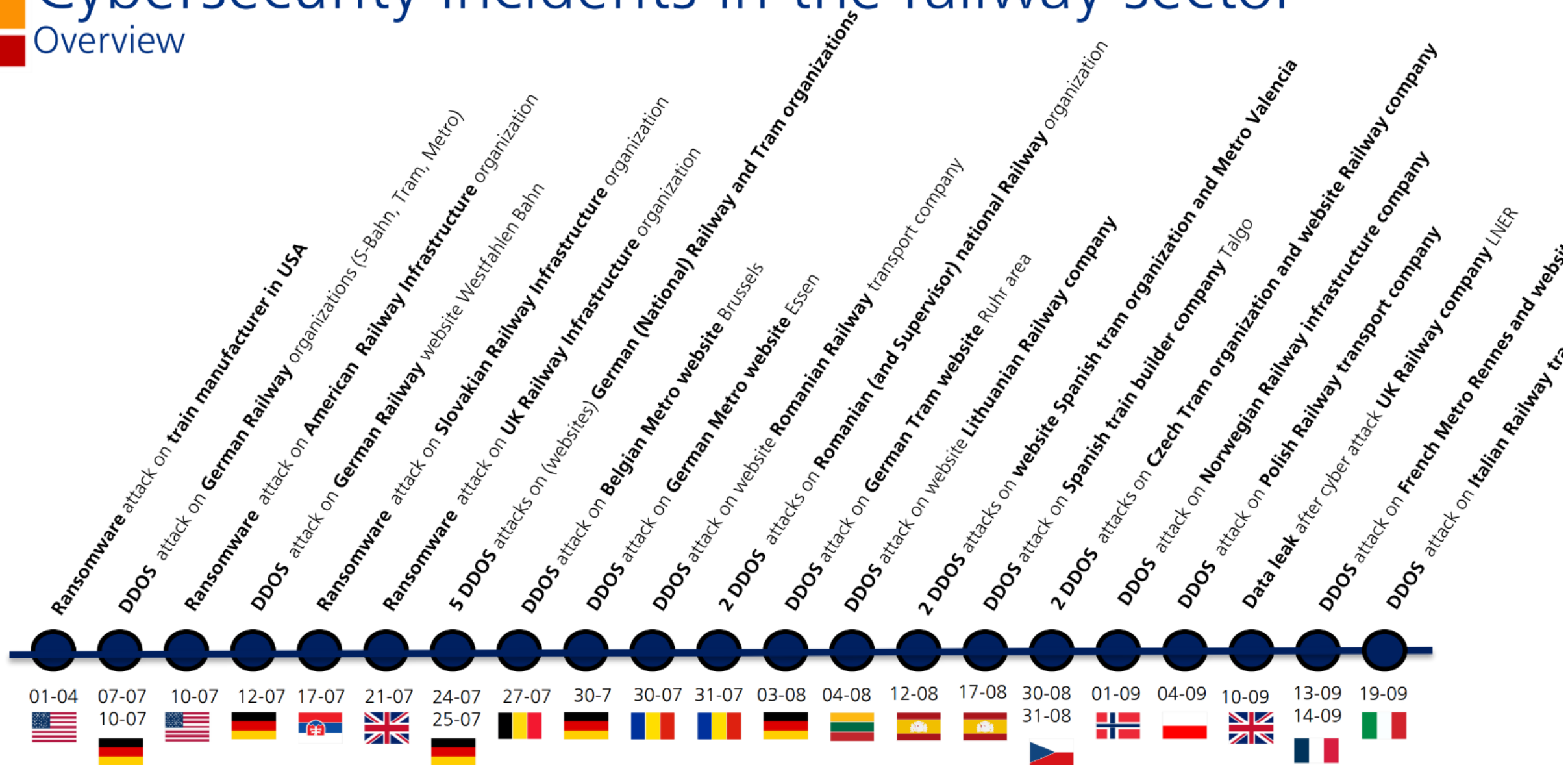# Cybersecurity incidents in the railway sector
Overview

Timeline of incidents:

- **Ransomware** attack on **train manufacturer in USA** — 01-04 🇺🇸
- **DDOS** attack on **German Railway** organizations (S-Bahn, Tram, Metro) — 07-07, 10-07 🇩🇪
- **Ransomware** attack on **American Railway Infrastructure** organization — 10-07 🇺🇸
- **DDOS** attack on **German Railway** website Westfahlen Bahn — 12-07 🇩🇪
- **Ransomware** attack on **Slovakian Railway Infrastructure** organization — 17-07 🇸🇰
- **Ransomware** attack on **UK Railway Infrastructure** organization — 21-07 🇬🇧
- **5 DDOS** attacks on (websites) **German (National) Railway and Tram organizations** — 24-07, 25-07 🇩🇪
- **DDOS** attack on **Belgian Metro website** Brussels — 27-07 🇧🇪
- **DDOS** attack on **German Metro website** Essen — 30-7 🇩🇪
- **DDOS** attack on website **Romanian Railway** transport company — 30-07 🇷🇴
- **2 DDOS** attacks on **Romanian (and Supervisor) national Railway** organization — 31-07 🇷🇴
- **DDOS** attack on **German Tram website** Ruhr area — 03-08 🇩🇪
- **DDOS** attack on website **Lithuanian Railway company** — 04-08 🇱🇹
- **2 DDOS** attacks on **website Spanish tram organization and Metro Valencia** — 12-08 🇪🇸
- **DDOS** attack on **Spanish train builder company** Talgo — 17-08 🇪🇸
- **2 DDOS** attacks on **Czech Tram organization and website Railway company** — 30-08, 31-08 🇨🇿
- **DDOS** attack on **Norwegian Railway infrastructure company** — 01-09 🇳🇴
- **DDOS** attack on **Polish Railway transport company** — 04-09 🇵🇱
- **Data leak** after cyber attack **UK Railway company** LNER — 10-09 🇬🇧
- **DDOS** attack on **French Metro Rennes and website** — 13-09, 14-09 🇫🇷
- **DDOS** attack on **Italian Railway** — 19-09 🇮🇹

Disclaimer: Most important incidents are displayed until date of delivery NSCS:CTL. For more information, see Railway Sector Cyberattacks (sharepoint.com)
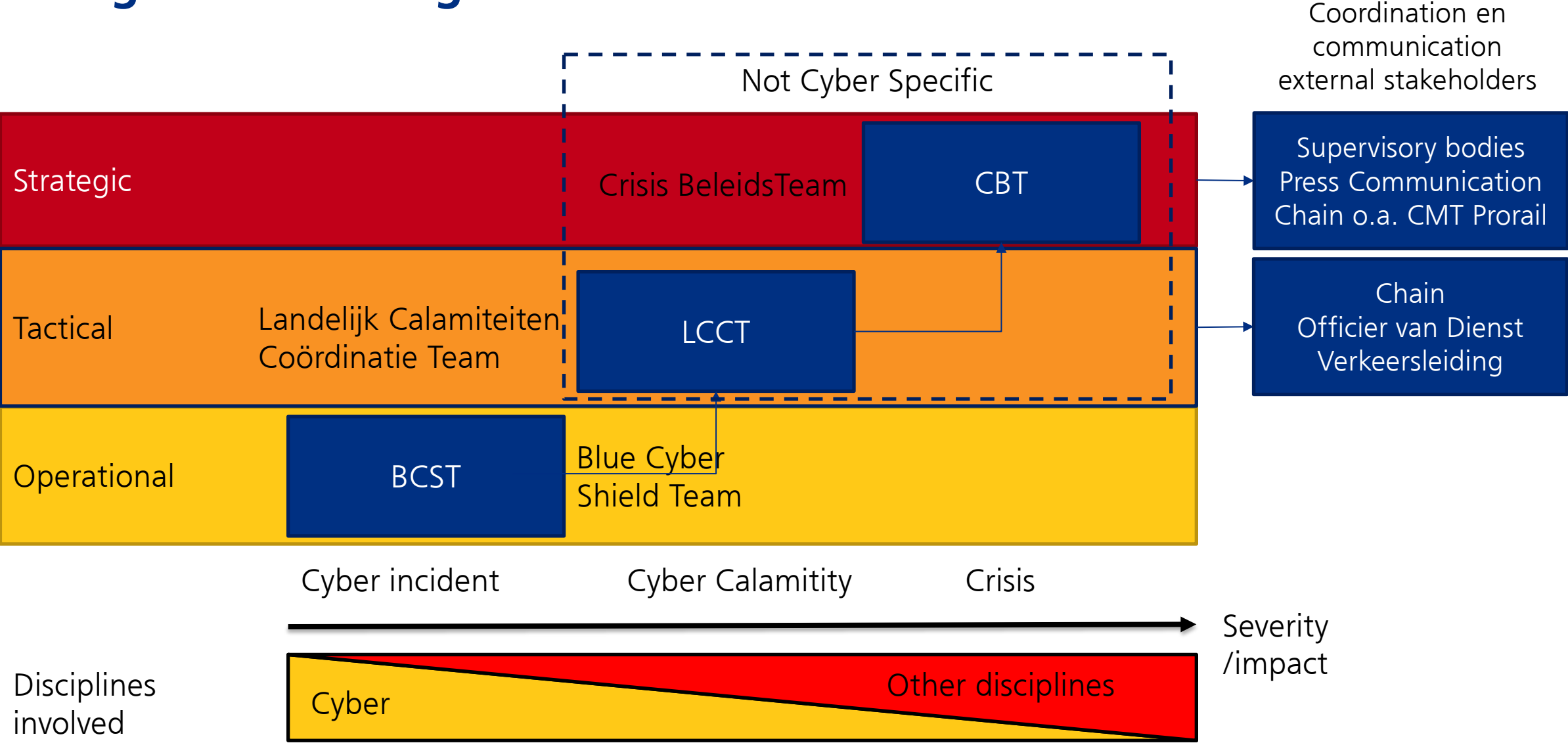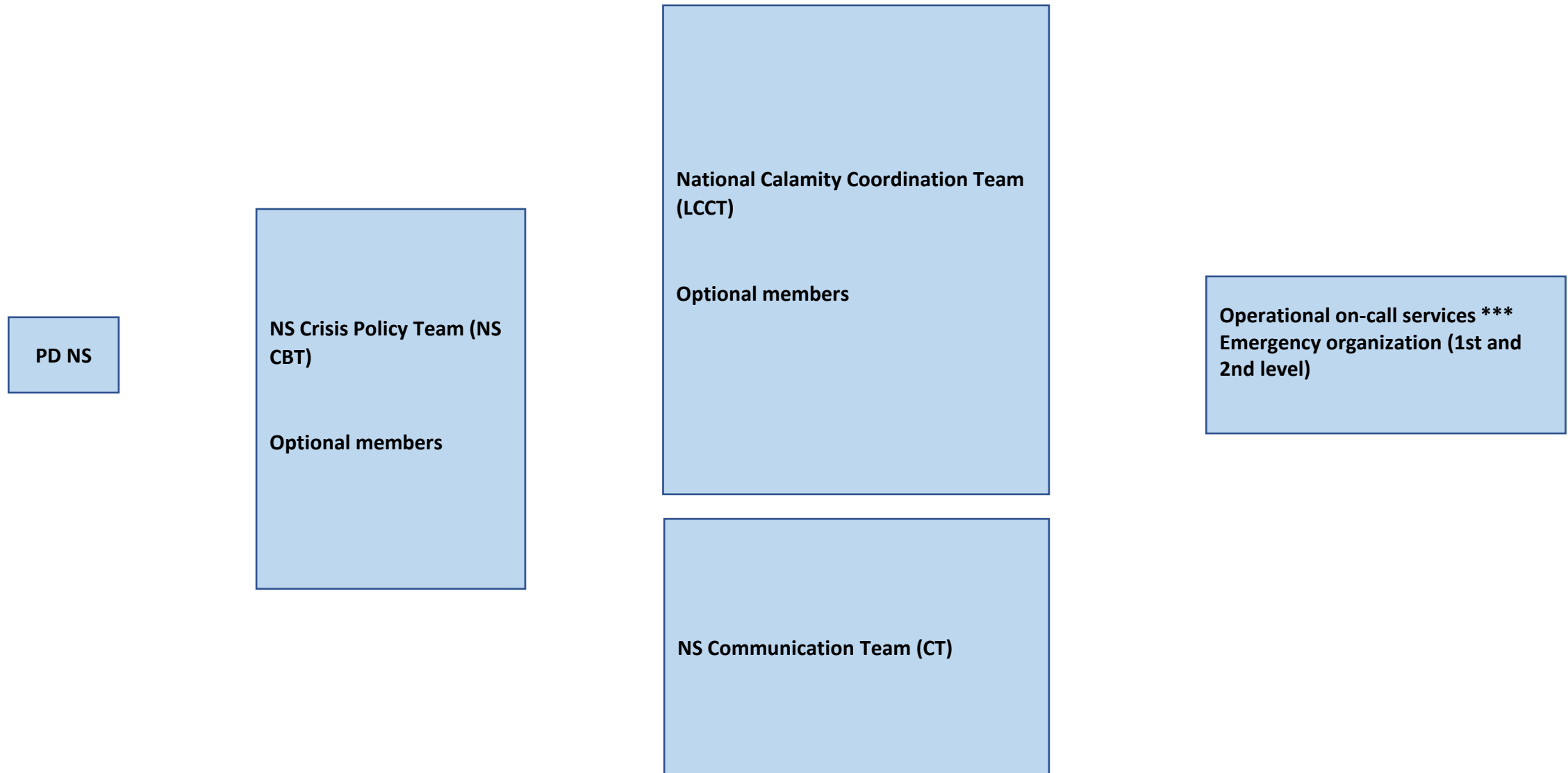
But a cyber crisis is just another crisis

- Use overarching NS crisis management organisation

- Use overarching NS crisis management processes

- NS Cyber Crisis Management Plan for specific cyber related aspects (as for other types of crises)

Using the Crisis organisation and escalation

Crisis Management Organization

PD NS

NS Crisis Policy Team (NS CBT)

Optional members

National Calamity Coordination Team (LCCT)

Optional members

NS Communication Team (CT)

Operational on-call services *** Emergency organization (1st and 2nd level)

Cyber crisis specifics

- Aspects to consider:
  - Priority of safety versus continuity of operation
  - How to deal with extortion
  - How to deal with cybercrime
  - How to deal with forensic investigation

- Critical decisions:
  - Threat of losing operational control
  - Deadline for payment
  - Data breach becoming public

Scenario approach

Type crisis	Cyber incident on NS rolling stock
Specifics crisis profile?	
Main impact areas and specifics in terms of impact?	
Specific objectives and principles?	
Possible critical moments and decisions?	
Special stakeholders/partners? (For example, because of specific authority or expertise)	
Special features in the preparation?	
Have you prepared specific facilities?	
Additional external expertise required?	
Certain plans and procedures that the team should not forget?	
Specifics in terms of signaling, alerting and/or informing?	
Derogations?	
Peculiarities in reacting and limiting negative consequences?	
Peculiarities in the first response?	
Specific interpretation of crisis organization?	
Specifics in upscaling: for example, direct CBT?	
Our role in the chain?	
Likely government scale-up? Special government partners? (For example, specific knowledge institutes, national role, etc.)	
Specifics of post-phase and recovery?	
Special aspects of recovery?	
E.g. because of complexity or long duration?	
Specific topics that require special attention?	
Specific interpretation of the post-phase organization?	

IT Impact
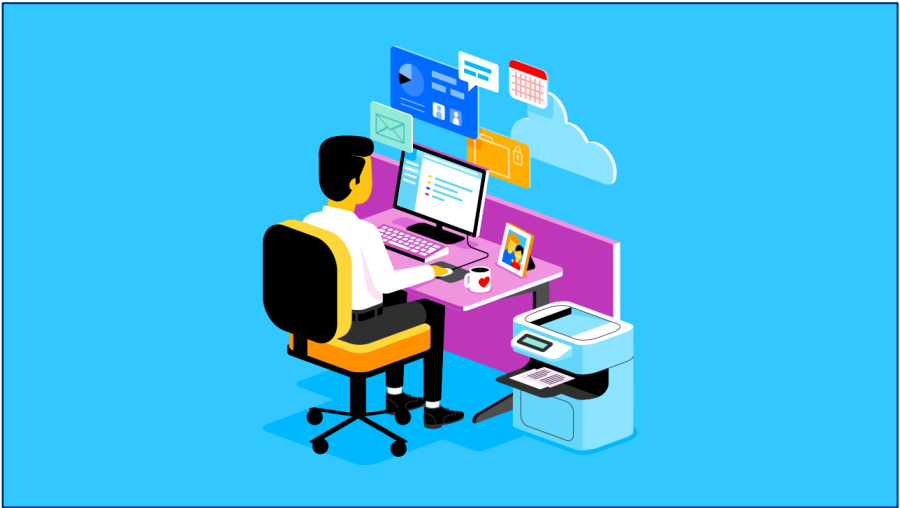
Systeem		
Naam		**Werkplek**
Belangrijkste applicaties		WPOL / Citrix / Thin Clients / Laptops / HAHP werkplek
Bedrijfsproces		O5
Eigenaar	IT	
IT		IT I&O

Beschrijving

Belang
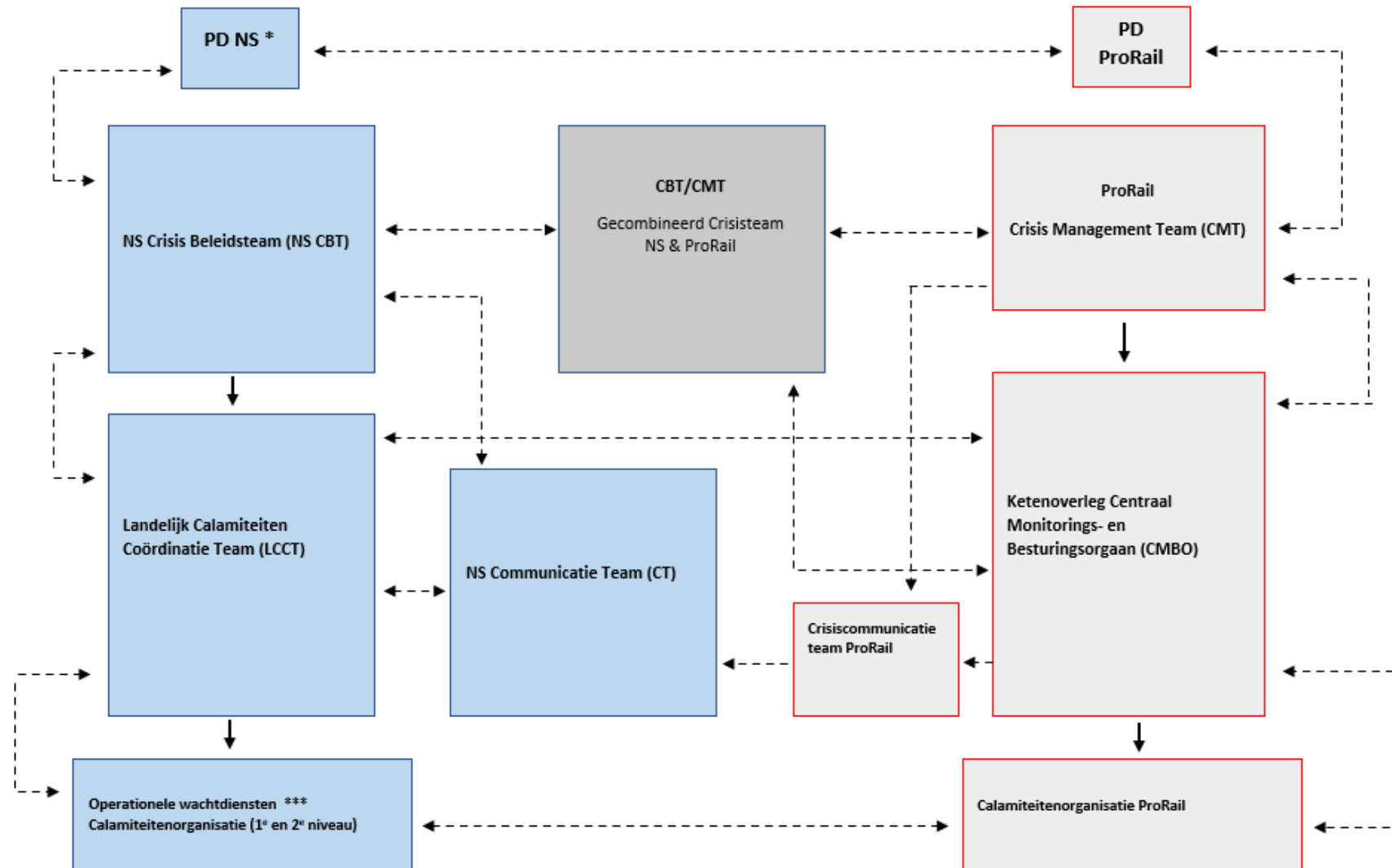
Impact op de dag

Business Continuity Maatregelen

Crisis Management in the rail sector

Combined Crisis Management Organization

Crisis Management Organization NS · Crisis Management Organization ProRail

Crisis Management - Excercises

- Included in planning per year for crisis management excersises

- Joint excersises with infrastructure manager with joint preparation

- Participation in national excersises (ISIDOOR)

- Evaluation of each excersise

  - Processes of regular crisis management

  - Cyber specific aspects
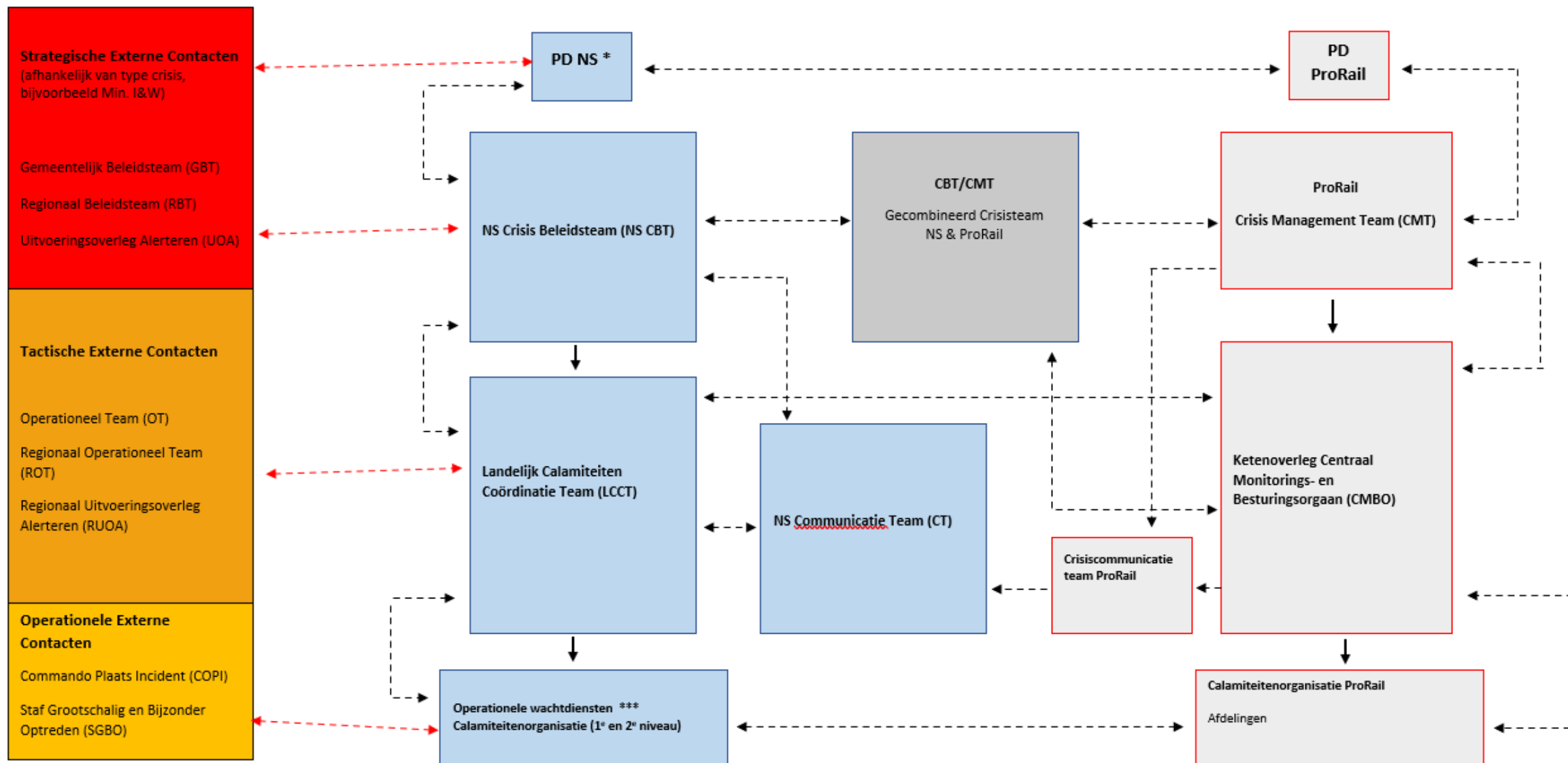
Crisis Management at a national level

National Cyber Crisis Management Organization
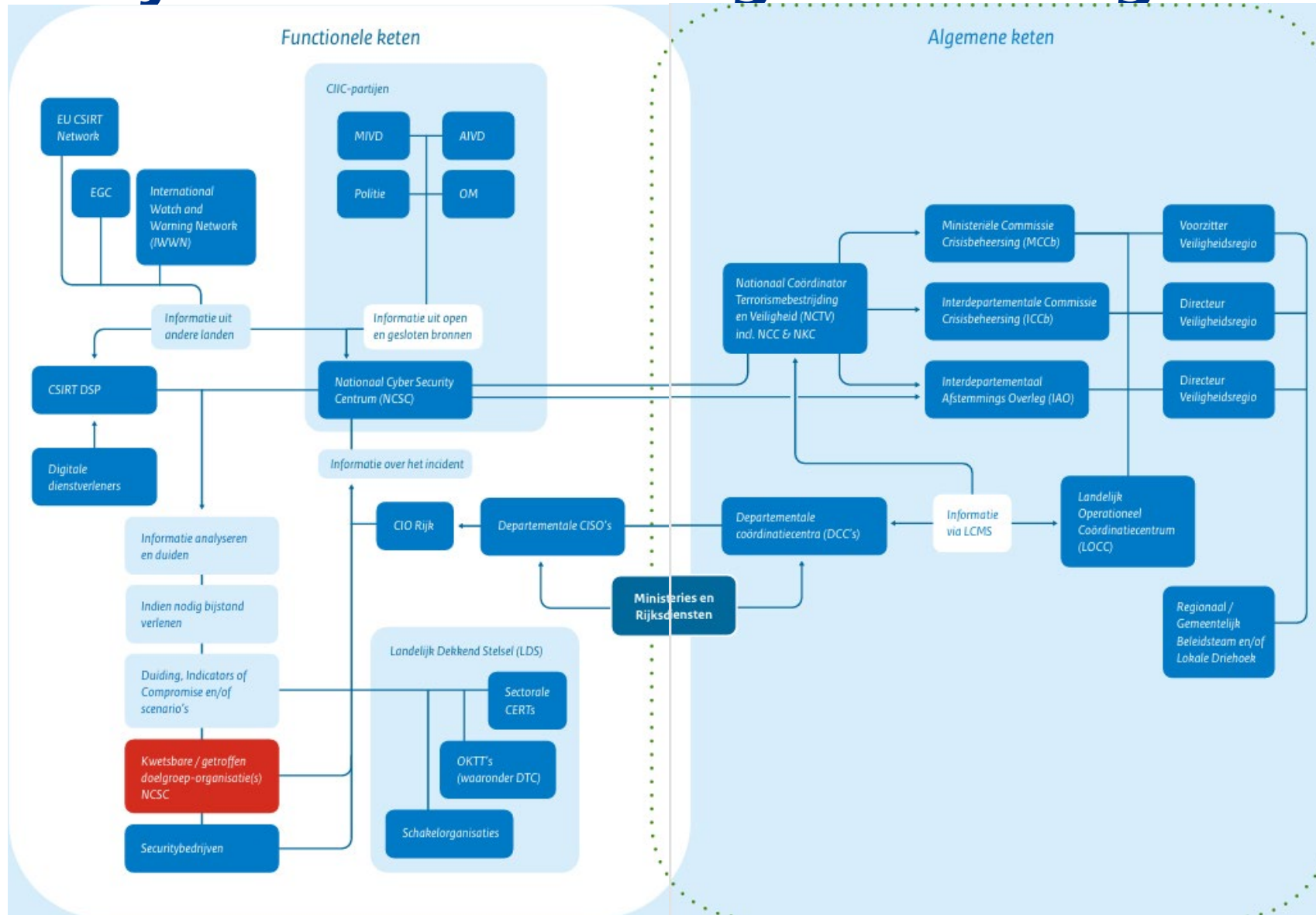
Our experience

- Cyber crisis is just a crisis but somewhat different

- Avoid fixation on going back to normal business

- Practice at all levels, with sector and with suppliers

- Use a realistic scenario, base these on incidents

- Use a "planned" crisis

- Collaborate & communicate

Questions

Check out:

Joseph Mager

joseph.mager@ns.nl

NS-Business Card

NS