

Supply Chain Risk Management

Logistics for Europe

Andreas Wilhelm

Chairman CLECAT Security Institute,

Brussels

13. November 2025



Organisational resilience is an organization's **ability to absorb and adapt to a changing environment
(ISO 22316:2017)**

Main risks affecting international supply chains



Natural disasters and environmental risks

Disrupt or impair access to

- Personnel
- Energy & power supply
- IT infrastructure & means of communication
- Critical infrastructure (roads, ports, airports, rail systems, warehouses) and suppliers



Pandemics & diseases

- Limiting movement of personnel
- Closure of borders



Man-made disruptions

- Social unrest and strikes
- Acts of warfare, asymmetric and hybrid warfare
- Acts of terrorism



Cyber attacks & organized crime

Orchestrated by

- Organised crime groups
- State actors (hybrid warfare)
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Ransomware attacks
- Phishing & Spear phishing

Regulations play an important role in defining entities and industries, which are critical to supply the population of member states with essential services:

- Healthcare manufacturer and services
- Supply of drinking water / wastewater handling
- Energy supply
- Food supply
- Digital infrastructure and communication networks
- Public transport
- Air- & seaports and rail infrastructure
- Banking industry
- Public administration



Regulatory frameworks should :

- **Achieve harmonisation to enable global implementation**
- **Be outcome oriented**
- **Prevent duplication of effort by acknowledging existing risk mitigation measures (ISO standards)**
- **Define reasonable and appropriate thresholds and criteria at for entities falling in scope of regulations**
- **Consider the size and (financial) capabilities of regulated entities**
- **Grant privileges and facilitation to entities certified under regulatory certification schemes to increase attractiveness thereof to industry and grant a reasonable ROI (costs for implementation and maintenance)**



Deficiencies in today's regulatory frameworks

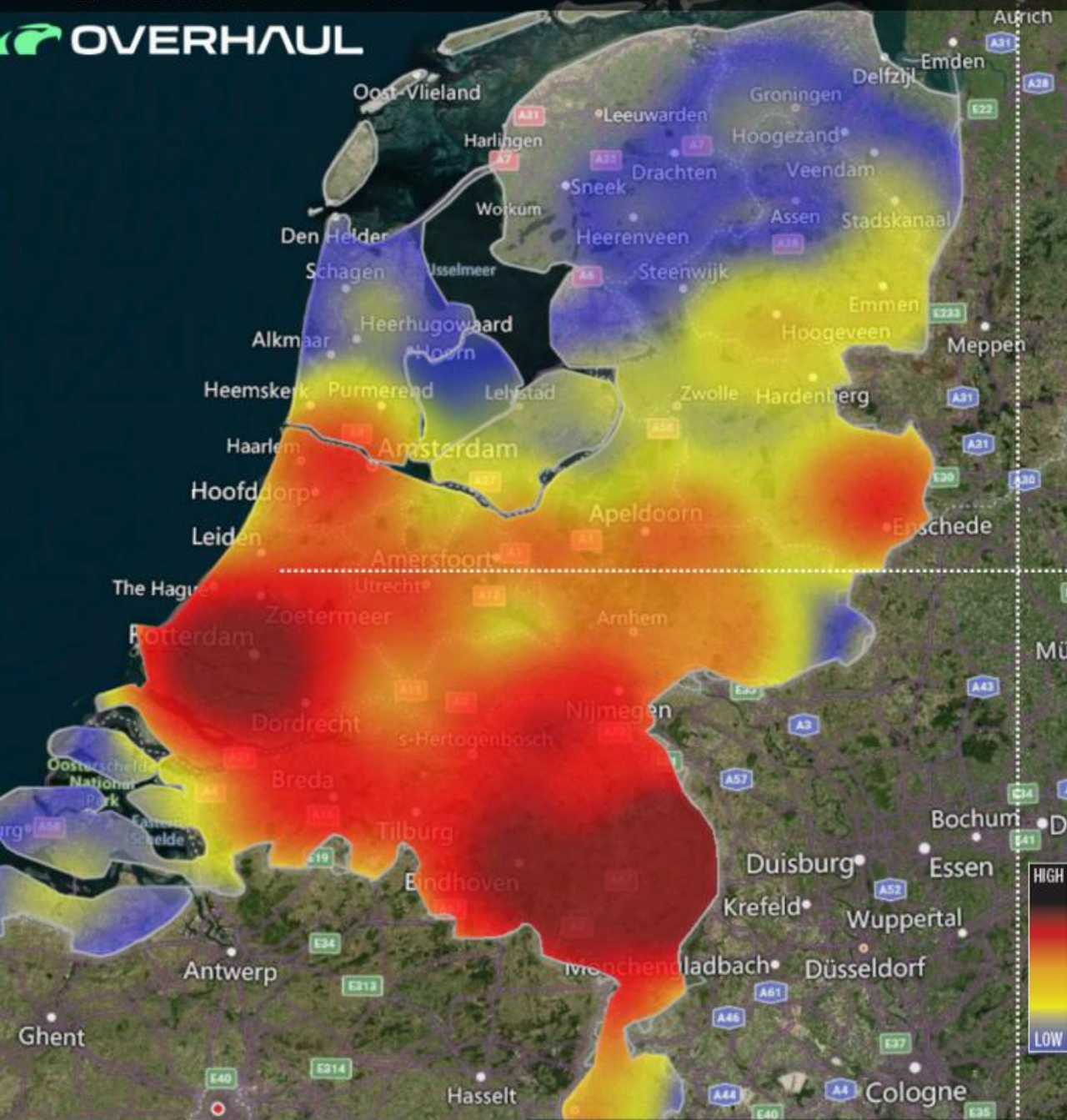
- Framework laying down collaboration between member states
- Prevention of inappropriate and disruptive unilateral measures by member states (e.g. border closures during COVID 19 pandemic)
- Consultation of subject matter experts of industry in decision process
- Lacking harmonisation in regulatory frameworks and risk mitigation measures



QUADRANT 1 - 5%

QUADRANT 2 - 18%

OVERHAUL



QUADRANT 3 - 32%

QUADRANT 4 - 45%

Location and route risk assessments

Understanding geographical areas of elevated risks & tactics of adversaries

- Usage of intelligence information to perform location and route risk assessments
- Assessment of areas with elevated criminal activities
- Assessment of tactics and modus operandi used
- Continuous monitoring of threat level changes and emerging crime trends/ shift of tactics & m.o.s
- Implementation of counter-measures based on risk and tactics used
- Circumnavigation / prohibition of stops in high-risk areas and enforcement by means of geofencing

Modus operandi used by organized crime



Opportunistic thefts

Tactics by cargo thieves

- Slash & grab thefts during overnight rests on (un)secure parking places
- Forced entry into box trailers, swap bodies & containers
- Forced entry into inadequately secured warehouses
- Theft of loads from vehicles while driving at night (so-called Romanian rollover m.o.)



Targeted strategic thefts

Cargo thieves impersonate legitimate carriers

- Cargo thieves target full truck-and container loads of highly valuable goods (e.g. highly valuable electronics)
- Exploit vulnerabilities in internet freight exchange platforms, multi-tier sub-contracting arrangements, multiple changes of custody and lacking entitlement verification



Sophisticated tactics

Usage of advanced technology & firearms

- Usage of power tools to cut holes into vehicle bodies, containers and warehouse doors to bypass alarm systems
- Ram-raid attacks (warehouses)
- Armed hijacking using jamming technology to disrupt GPS tracking and means of communication
- Usage of advanced reconnaissance and commando-style attacks on warehouses in Northern Italy & Netherlands
- Acts of terrorism and hybrid warfare (e.g introduction of IIDs into air supply chain)



Picture: Luxemburger Wort

Trafficking

Organised crime groups infiltrate supply chain actors or corrupt / intimidate personnel for collaboration

- Sea containers and perishable goods preferably targeted
- Introduction into legitimate supply chain and onforwarding into criminal supply chain by insiders
- Risk of detrimental effects on supply chain actors (loss of AEO certification etc)

Risk-based mitigation strategies



Personnel

- Personnel background screening
- Security & cyber security training (office & warehouse personnel)
- Management to foster a security culture (if you see something, say something)
- Driver security training

Physical

- Design of physical deterrents
- Intrusion detection systems & IPS
- Access control policy & systems (MFA)
- Internal system scanning & patching cycle
- Firewall & encryption technologies
- Heavy duty locking devices
- Usage of safe & secure parkings (EU SSTPA / RPL)

Procedural

- Route risk assessments
- Application of principle of least privilege & phishing simulations
- Strict KYS programmes
- Prohibit usage of freight exchange platforms and 2nd-tier sub-contracting and brokerage
- Entitlement & integrity verification (9-point inspection)
- Reporting of incidents & deviations

Enhanced measures

- Active monitoring of high value transports
- Reinforced doors and intrusion detection systems on vehicles moving theft endangered loads
- Unarmed / armed escorts based on risk and in alignment with customer
- Threat detection by AI-supported CCTV systems
- KN developed anti-jamming system
- Red teaming tests

Inspire. Empower. Deliver.

