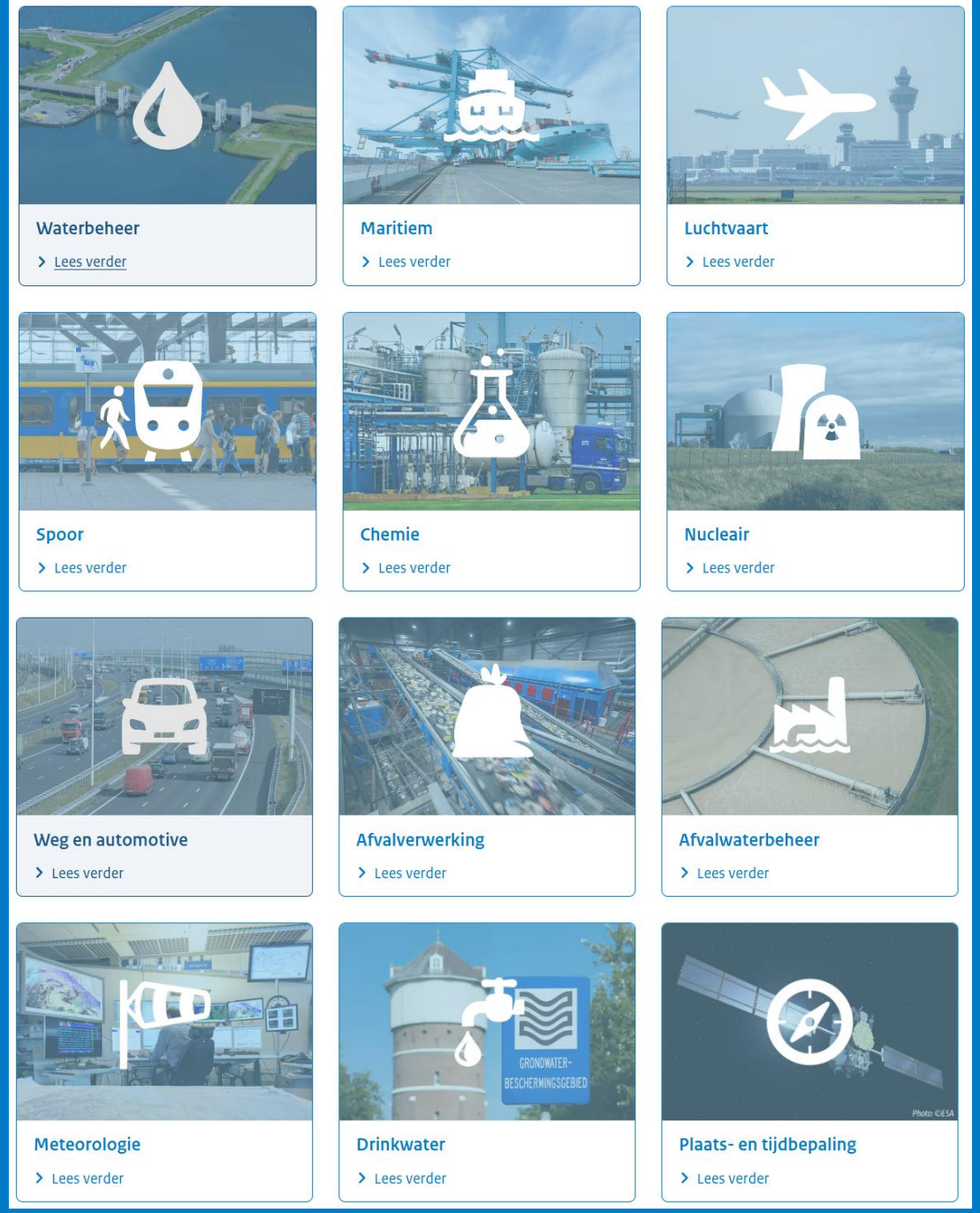


Ministerie van Infrastructuur
en Waterstaat

Cyber Resilience Programme of the Ministry of Infrastructure and Watermanagement Netherlands

Introduction

Daniëlle Ramsanjhal-Lala

**Senior policymaker –
Programme manager Cyber Resilience**

When you think of collaboration, you think of Daniëlle

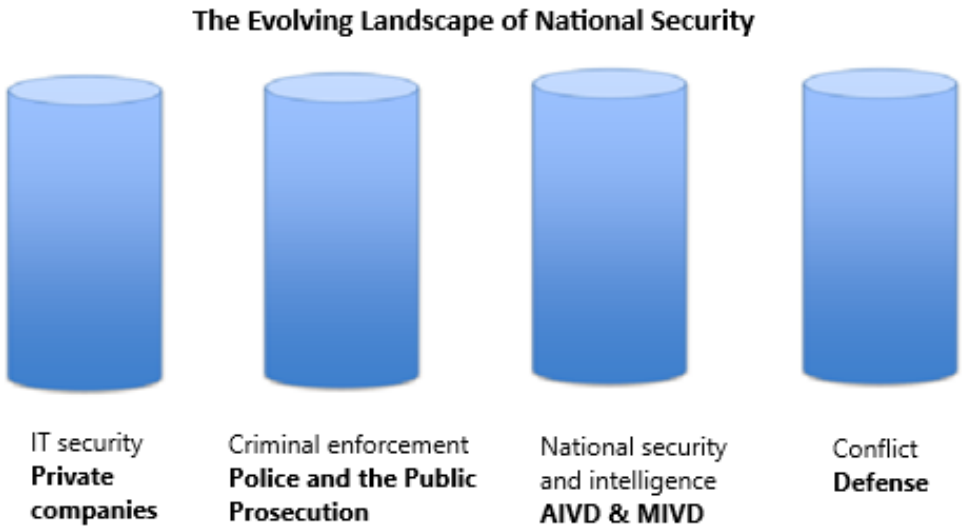
Introduction

Cyril Springveld

Senior policymaker –
Programme manager Cyber Resilience

Items for today

- The Evolving Landscape of National Security
- Dutch Cybersecurity Strategy (NLCS)
- Cyber Resilience Programme of the Ministry of Infrastructure and Water Management
- Common thread and specific focus: Operational Technology
- Highlights/best practices
- Q&A’s

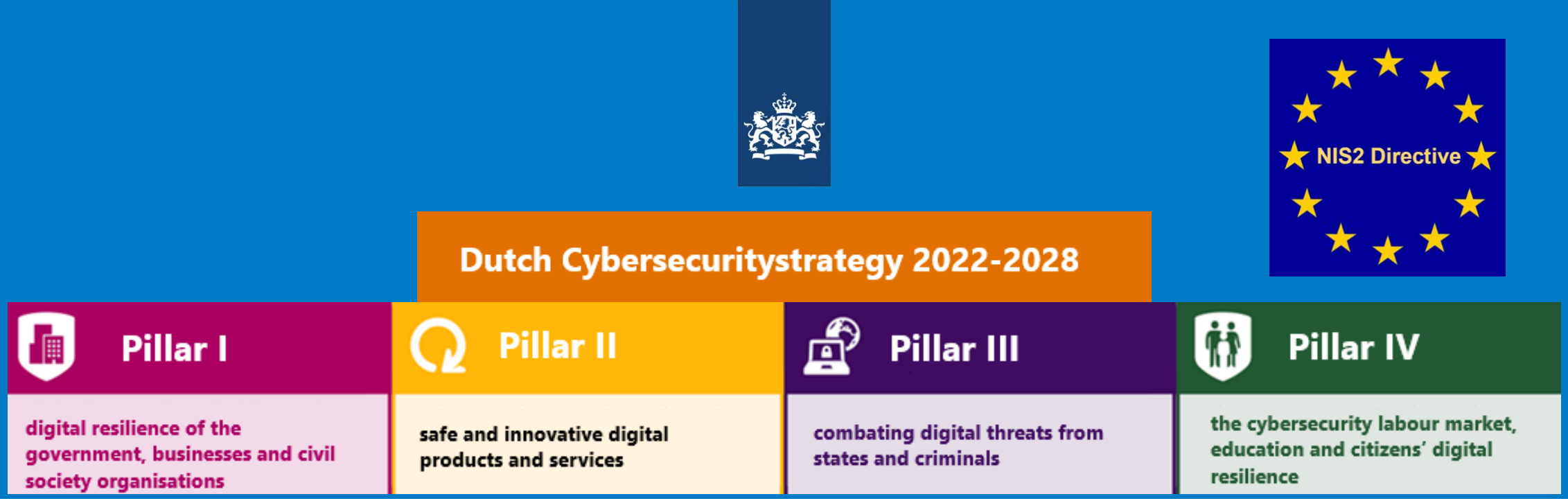


- *Evolving landscap*
- *Shared responsibility*
- *More than just compliance*
- *Spotting opportunities*
- *Respond, recover & adapt*

Shared responsibility

Cybersecurity ≠ Cyberresilience

- *Evolving landscap*
- *Shared responsibility*
- *More than just compliance*
- *Spotting opportunities*
- *Respond, recover & adapt*



Objective 2 in pillar 1: Organisations are well protected against digital risks, taking into account their importance to the sector and other organisations in the supply chain.

Sub-objective: I.2.5: Digital resilience of the infrastructure and water management sectors

Cyber Resilience Programme Ministry of Infrastructure and Watermanagement

Cyber Resilience Programmes: aim to help NIS2 entities to strengthen their cyber resilience

Bottum up approach; public-private collaboration(s), including NIS2 entities, CSIRT, applied science and technology organisation (TNO)

Based on five themes:

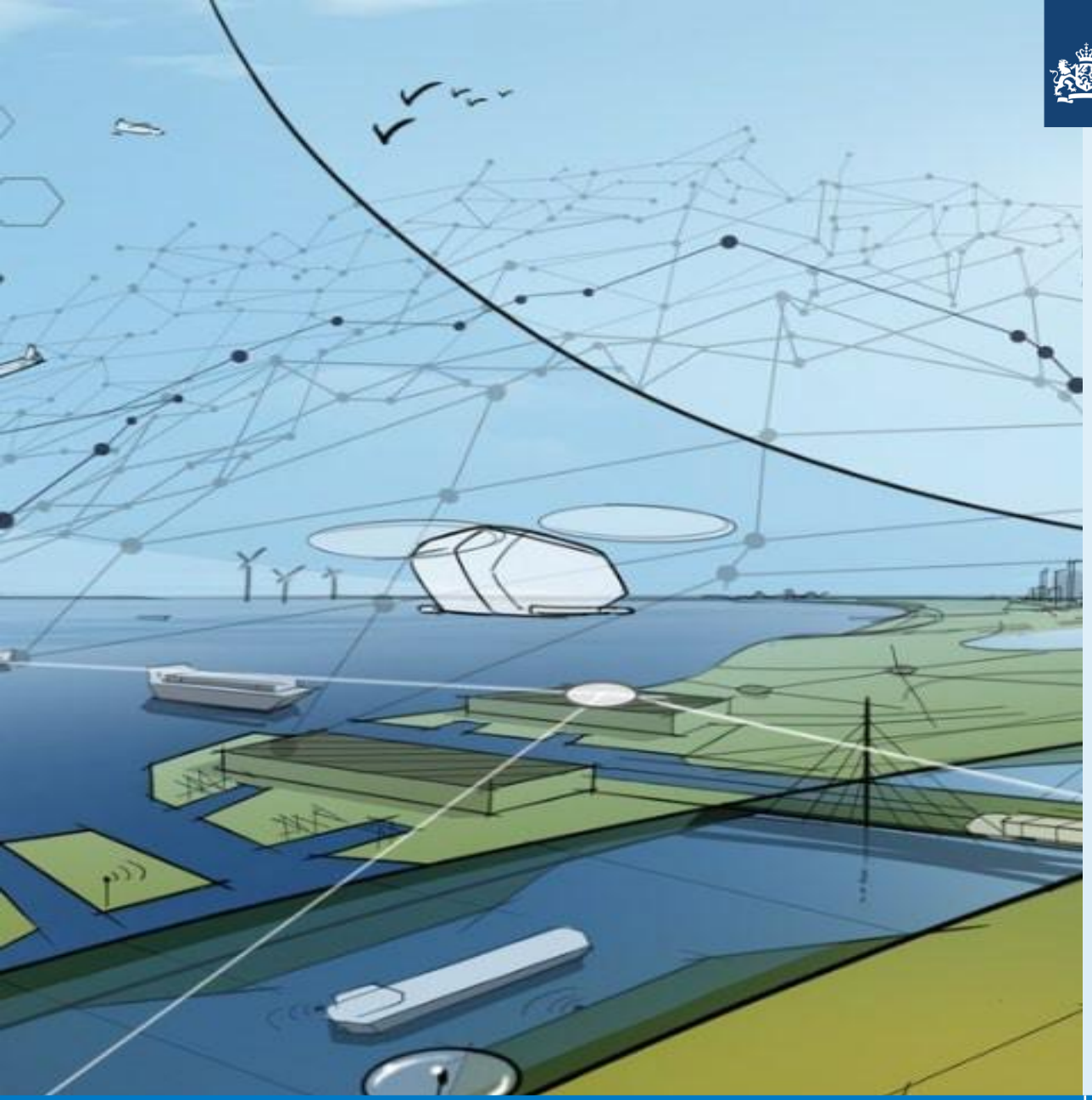
- **Risk management and (supply) chains**
- **Collaboration and expertise**
- **Measures and implementation**
- **Monitoring and detection**
- **Training, testing and drills**

Training, testing and drills	Risk management and (supply) chains	Measures and implementation	Monitoring and detection	Collaboration and expertise
Awarenesssessies bestuur	Handreiking risicobeheer OT omgeving	Implementatie NIS2: ontwikkeling van richtlijnen en standaarden	Borgen bereikbaarheid lauwe en warme fase/IenW expertgroep cyberincidenten	IenW Cyberweerbaarheids-conferentie (jaarlijks)
Training leveranciersmanagement	Handreiking cyberweerbare leveringsketen	Doorontwikkeling CSIR baseline	Workshop best practices monitoring en detectie	Bijdrage ONE conference/ OT track
Red team / blue team training	Podcast 'Keten in zicht' (samenwerking NCSC)	cybersecurity awarenesscampagne voor sectororganisaties		**Communicatie:** website
OT fundamentals/OT professionals training	Inzicht dreiging luchtvaart en maritieme sector/MASKER methodiek NCSC	Verkenning cybervereisten onbemande luchtvaart en onbemande zeevaart		**Communicatie:** podcastseries
Adviesdag Ransomware Preparedness (RAP)	Ontwikkelen methode ketenanalyse/cf. CYRA standaard	Link cyber en Artificial Intelligence (in samenwerking met CISO office)		**Communicatie:** nieuwsbrieven
OT suitcase (samen met TNO en NCSC)				Bijdrage/vertegenwoordiging Cyberweerbaarheidsnetwerk (CWN)/IACS coalitie
				Verkenning OT expertise centrum

Instrument niveau 1: basis

Instrument niveau 2: gevorderd

Instrument niveau 3: volwassen



Main challenges

Operational technology:
Products include: further development of CSIR (OT standard), OT suitcases, guidance on risk management in OT, exploration of national OT center.

Chain collaboration/supply chain management:
Products include: guide 'Grip on the supply chain' (NCSC), podcast 'Chain in view'.

Innovations/technological developments:
Products include: exploration of cyber risks in unmanned mobility, developments in AI and quantum technology.

Human capital:
Connecting talent development with focus on NIS2 entities.

Communication:-
How to reach both directors/boards and SME NIS2 entities

Common thread Operational technology (OT)

- Cyber risks in operational technology (OT) are a growing concern for organizations that manage their infrastructure with operational technologies.
- The integration of OT with IT and the connection to the internet have led to an increased risk of cyberattacks.
- This includes risks such as ransomware attacks, vulnerabilities in factory networks, and the impact of IT failures on production processes.
- The NIS2 directive has fundamentally shifted how organizations should approach risks, taking into account not only digital risks but also physical risks in digital environments.
- This means that organizations need to focus on the all hazards approach, combining IT, OT, IoT, and physical risks in digital environments.

Ministerie van Infrastructuur en Waterstaat

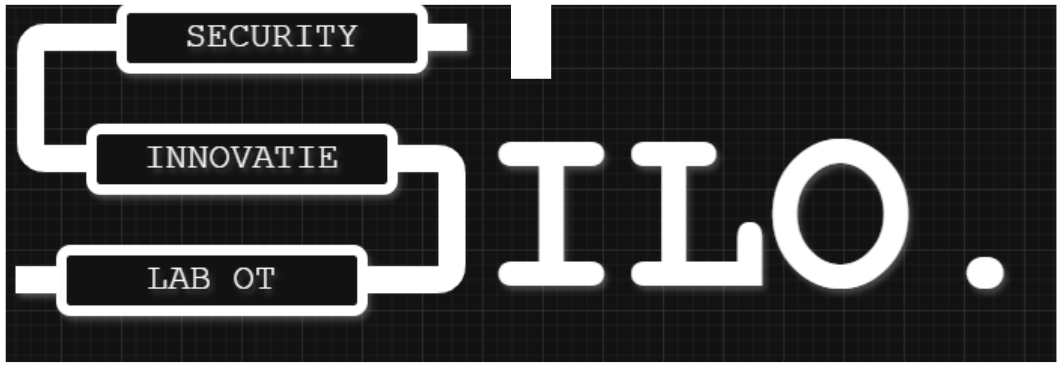
Handreiking risicobeheer in OT

Versie: Final – Handreiking 2.0 | 05.11.2025

OT risk management guide

- Identify: Map OT systems, assets, vulnerabilities, threats, and the so-called 'crown jewels' of the organization. This includes both physical devices and logical networks, as well as intellectual property.
- Analyze: Quantify risks by conducting impact analyses (Business Impact Analysis) and developing a risk matrix. This assesses the potential impact on business operations and security.
- Manage: Implement measures to mitigate risks, including fundamental basic measures, organizational conditions such as management involvement, available resources, and clear role allocation.
- Monitor: Continuously oversee risks and measures, including evaluation and adjustment of the risk management process to improve digital resilience.

Project SILO – TNO – NCSC - IenW



- Legacy software
- Proprietary Hardware
- Decision making between assetmanagers & cybersecurityspecialists

› State-of-the-art mobile OT cyber lab for testing, simulations, and experiments.

› A powerful ecosystem in which knowledge, resources, and threat intelligence are shared

› Governance model that strengthens collaboration between asset managers and cybersecurity specialists

› Short-cycle collaborative innovation with proven higher adoption rate

Question for the public:
Possible cross border (Benelux) initiatives?

www.versterkenweerbaarheid.nl

Contact

Cyril Springveld
(cyril.springveld@minienw.nl)

Daniëlle Ramsanjhal-Lala
(danielle.ramsanjhal@minienw.nl)