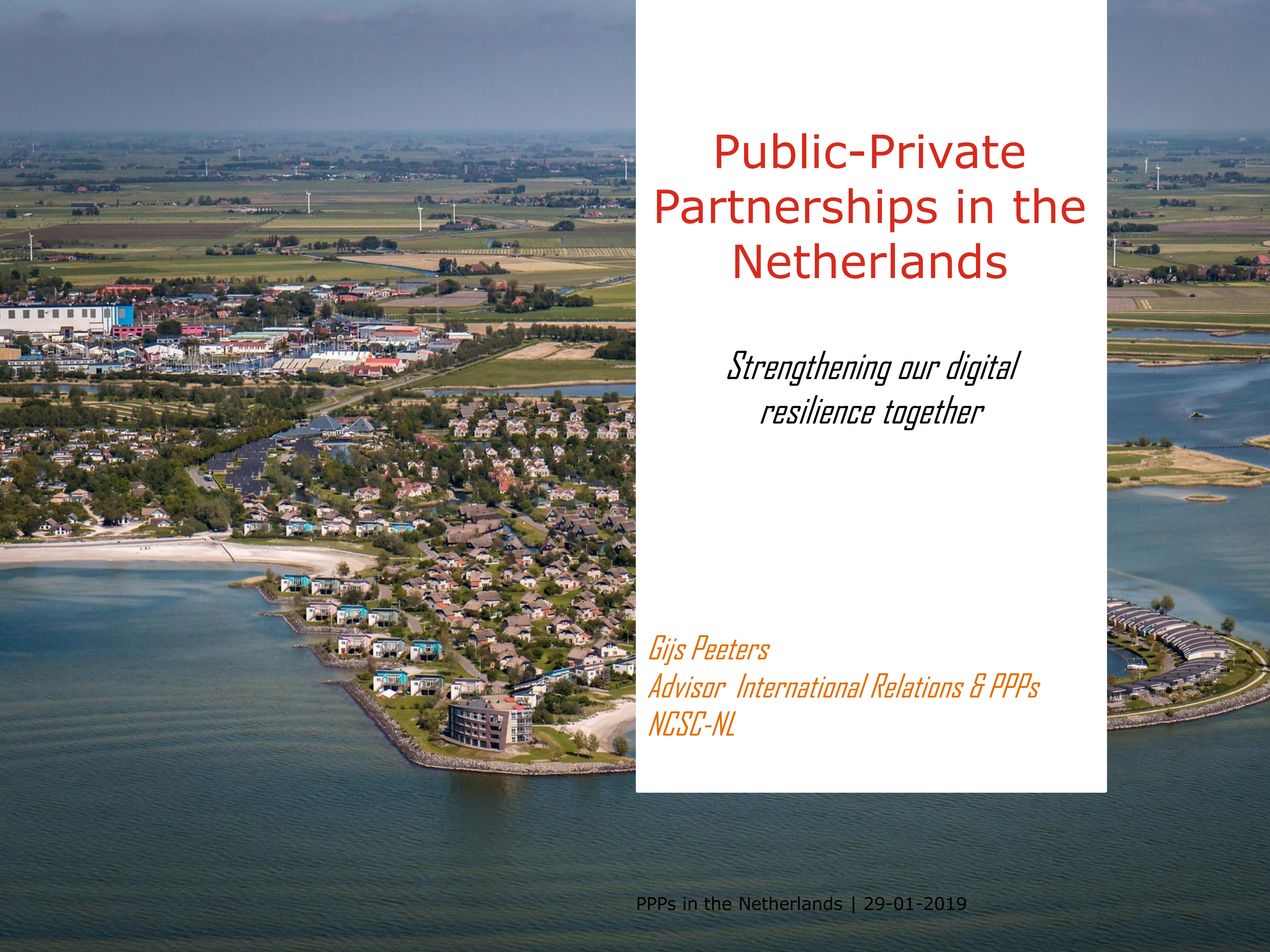
National Cyber Security Centre
Ministry of Justice and Security

Public-Private Partnerships in the Netherlands

Gijs Peeters, National Cyber Security Centre (NCSC-NL)
Advisor International Relations & PPPs

29 January 2019
ENISA NLO Meeting

NCSC



Public-Private Partnerships in the Netherlands

Strengthening our digital resilience together

Gijs Peeters
Advisor International Relations & PPPs
NCSC-NL

Content

-PPP: the Dutch way

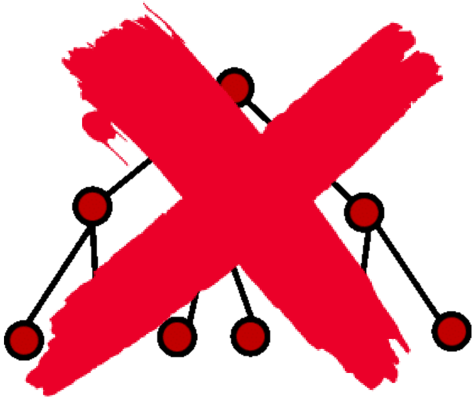
-Ambition: a nationwide network of partnerships

  - ISAC’s
  - CSIRT’s
  - Regional ecosystems

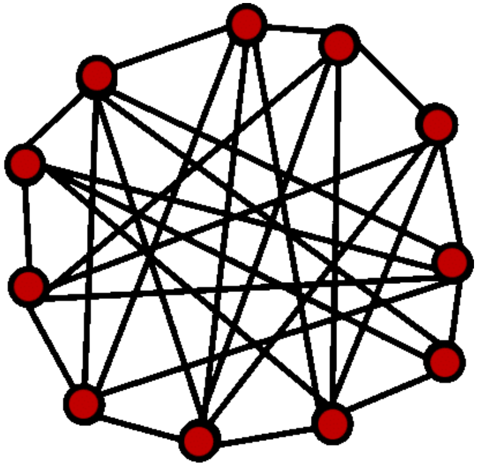
-Challenges

-Role of ENISA in stimulating PPPs

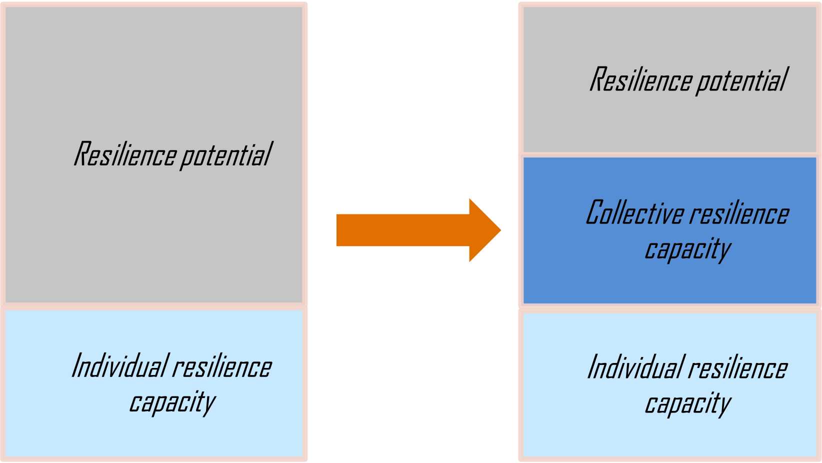
PPP – the Dutch approach



“Top-down”



“Bottom-up”



Resilience potential

Individual resilience capacity

Resilience potential

Collective resilience capacity

Individual resilience capacity

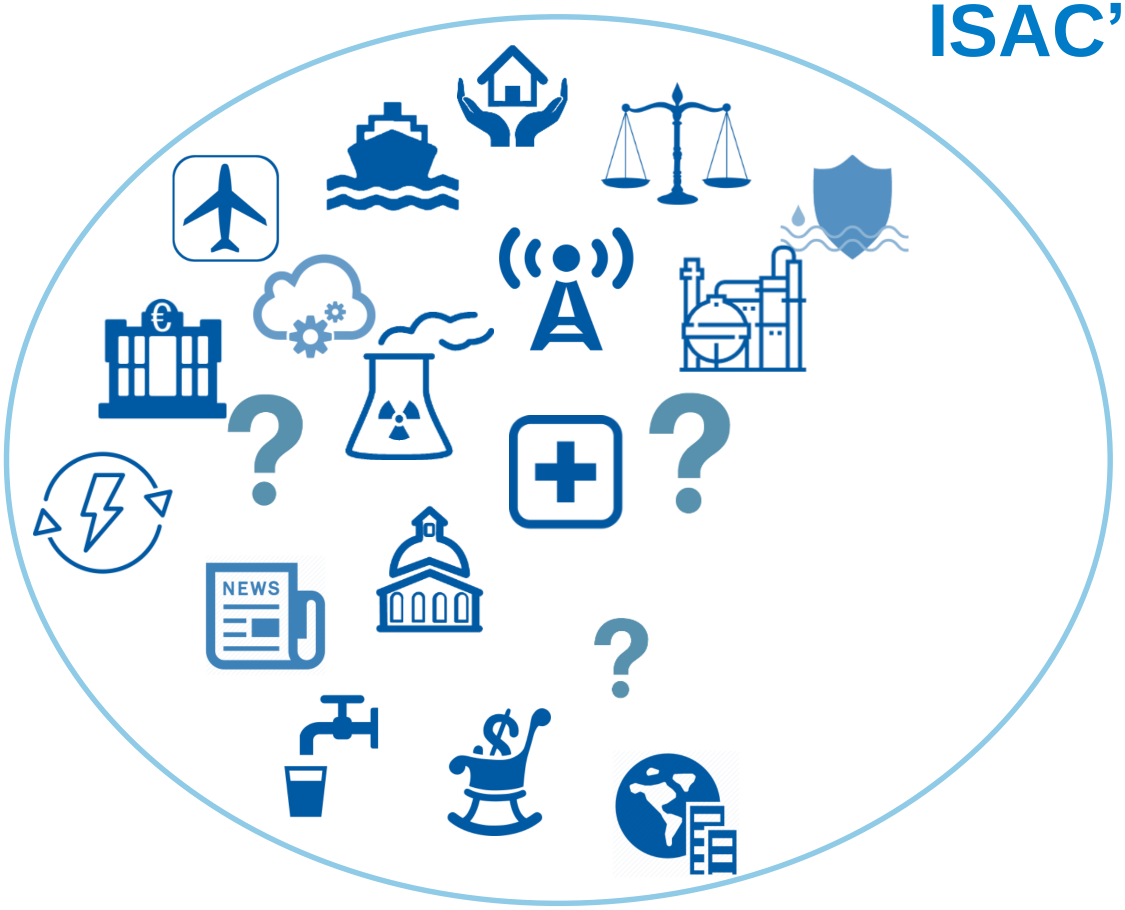
Trust = Value

National Cyber Security Agenda

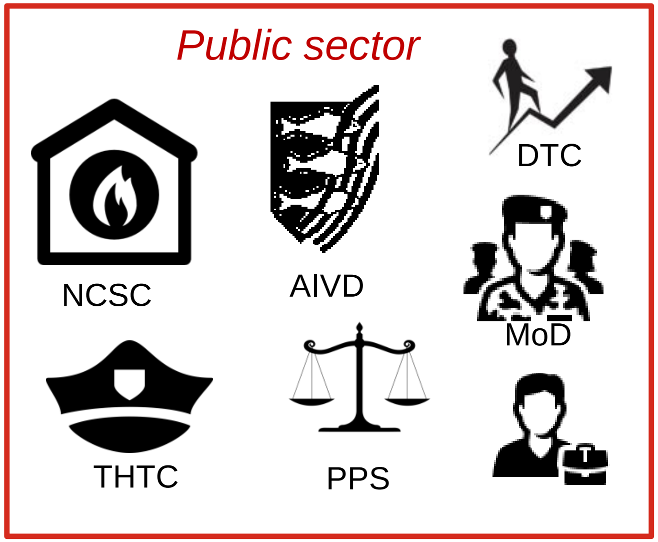
"A nationwide network of cybersecurity partnerships will be created within which information about cybersecurity can be shared between public and private parties more widely, effeciently and effectively. The aim of this network is to strengthen the capabilities of public and private parties."

A nationwide network of cybersecurity partnerships

ISAC’s



- Chair and co-chair from sector
- Sector in the lead, NCSC faciltates ISACs and brings in expertise (2 roles)



Tactical information exchange

Roadmap sectoral collaboration

Stage 1: **Explore**

Seek like-minded people and create support:

- Start out small, together with enthusiastic (chief) information security officers.
- Set up an informal working group and get to know each other better.
- Look for common goals and other similarities during the first meeting.

Stage 2: **Build**

Build a solid foundation:

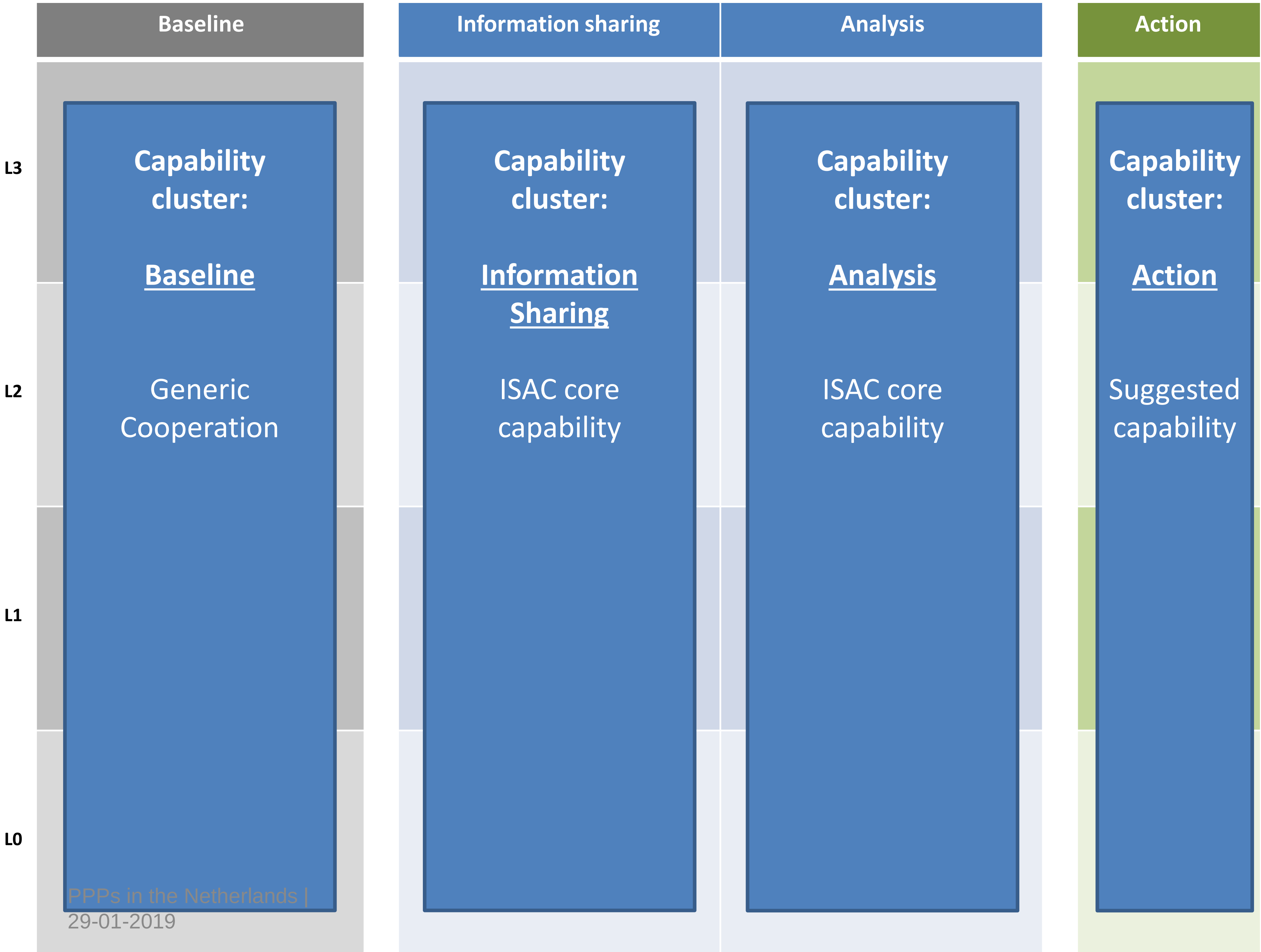
- Organise a kick-off meeting to formally start the ISAC.
- Jointly select a chair, vice-chair and secretary from those present.
- Reach agreement on how often meetings will take place and in what way you will com-mu-nicate with each other.
- Set up guidelines for a membership and information sharing.

Stage 3: **Continue**

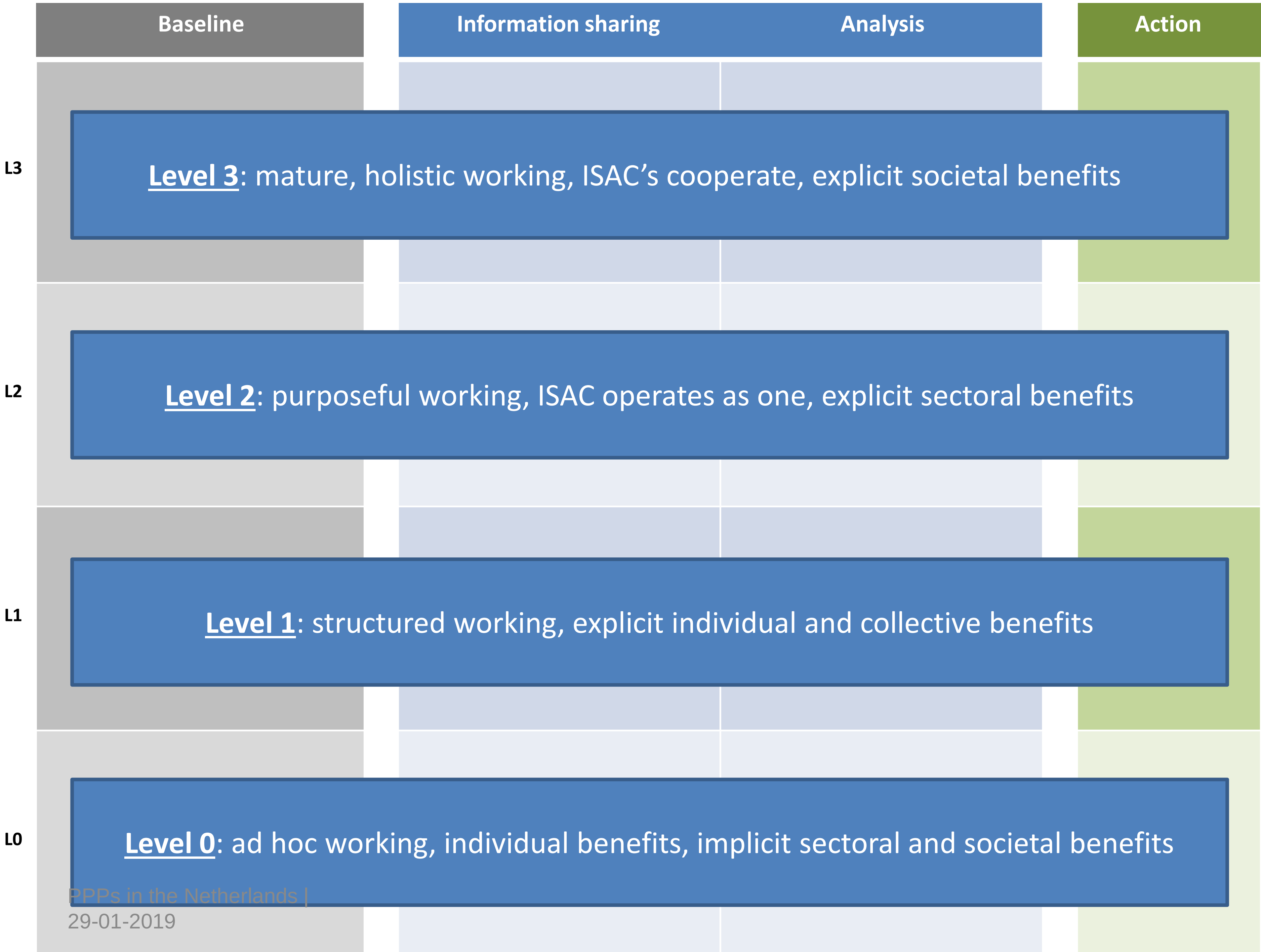
Keep working on building trust:

- Be critical of your own participation in the ISAC.
- Make room to evaluate.
- Continue to focus on the added value of information exchange.

Further growth of an ISAC?



	Baseline	Information sharing	Analysis	Action
L3	**Capability cluster:** **Baseline**	**Capability cluster:** **Information Sharing**	**Capability cluster:** **Analysis**	**Capability cluster:** **Action**
L2	Generic Cooperation	ISAC core capability	ISAC core capability	Suggested capability
L1				
L0				



Baseline

Information sharing

Analysis

Action

L3

Level 3: mature, holistic working, ISAC’s cooperate, explicit societal benefits

L2

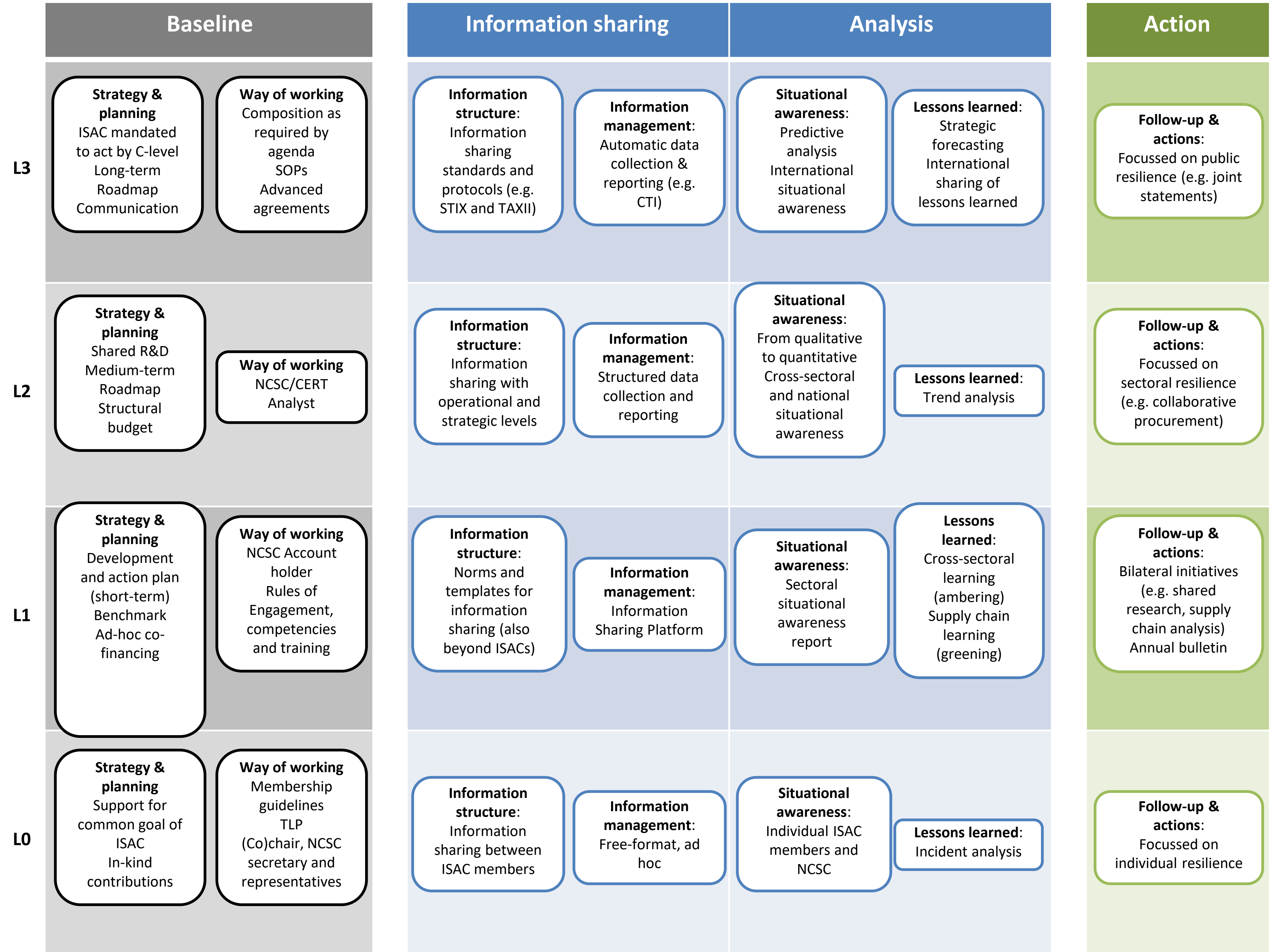
Level 2: purposeful working, ISAC operates as one, explicit sectoral benefits

L1

Level 1: structured working, explicit individual and collective benefits

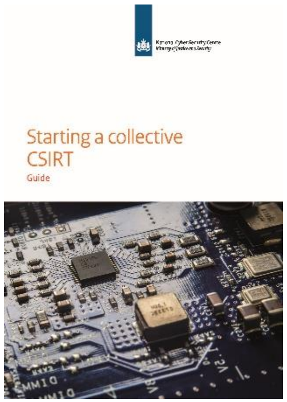
L0

Level 0: ad hoc working, individual benefits, implicit sectoral and societal benefits



	Baseline		Information sharing		Analysis		Action
L3	**Strategy & planning** ISAC mandated to act by C-level Long-term Roadmap Communication	**Way of working** Composition as required by agenda SOPs Advanced agreements	**Information structure**: Information sharing standards and protocols (e.g. STIX and TAXII)	**Information management**: Automatic data collection & reporting (e.g. CTI)	**Situational awareness**: Predictive analysis International situational awareness	**Lessons learned**: Strategic forecasting International sharing of lessons learned	**Follow-up & actions**: Focussed on public resilience (e.g. joint statements)
L2	**Strategy & planning** Shared R&D Medium-term Roadmap Structural budget	**Way of working** NCSC/CERT Analyst	**Information structure**: Information sharing with operational and strategic levels	**Information management**: Structured data collection and reporting	**Situational awareness**: From qualitative to quantitative Cross-sectoral and national situational awareness	**Lessons learned**: Trend analysis	**Follow-up & actions**: Focussed on sectoral resilience (e.g. collaborative procurement)
L1	**Strategy & planning** Development and action plan (short-term) Benchmark Ad-hoc co-financing	**Way of working** NCSC Account holder Rules of Engagement, competencies and training	**Information structure**: Norms and templates for information sharing (also beyond ISACs)	**Information management**: Information Sharing Platform	**Situational awareness**: Sectoral situational awareness report	**Lessons learned**: Cross-sectoral learning (ambering) Supply chain learning (greening)	**Follow-up & actions**: Bilateral initiatives (e.g. shared research, supply chain analysis) Annual bulletin
L0	**Strategy & planning** Support for common goal of ISAC In-kind contributions	**Way of working** Membership guidelines TLP (Co)chair, NCSC secretary and representatives	**Information structure**: Information sharing between ISAC members	**Information management**: Free-format, ad hoc	**Situational awareness**: Individual ISAC members and NCSC	**Lessons learned**: Incident analysis	**Follow-up & actions**: Focussed on individual resilience

Network of CERTs

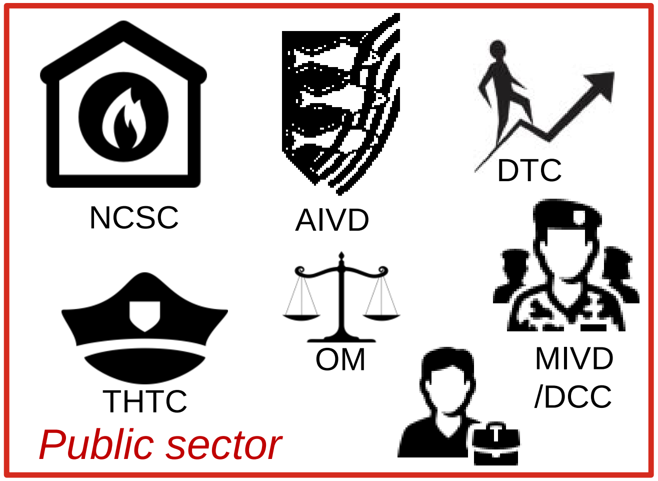


Starting a collective CSIRT

Guide

Network of CERT's

Operational information exchange



NCSC

AIVD

DTC

THTC

OM

MIVD /DCC

Public sector

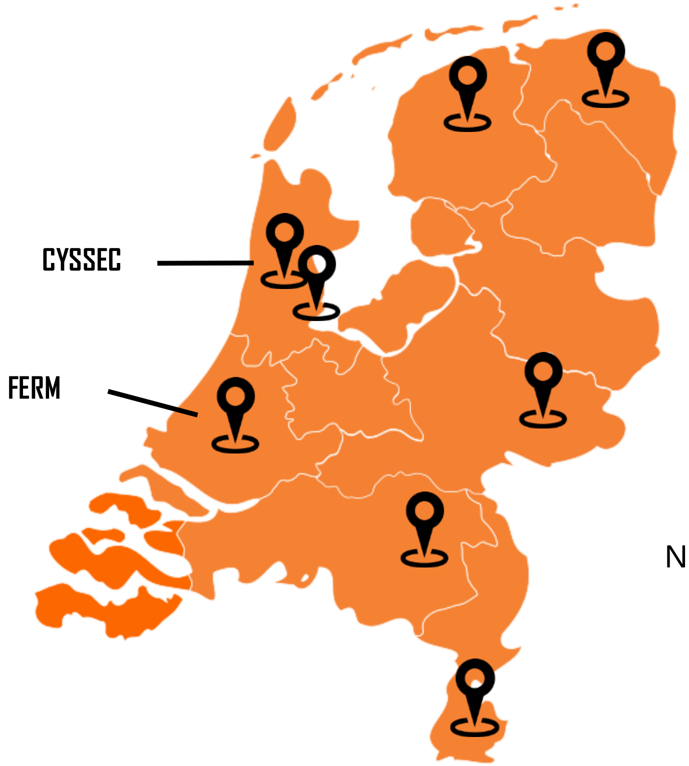
Regional ecosystems

Starting a regional collaboration

Guide

Starting a supply chain collaboration

Guide



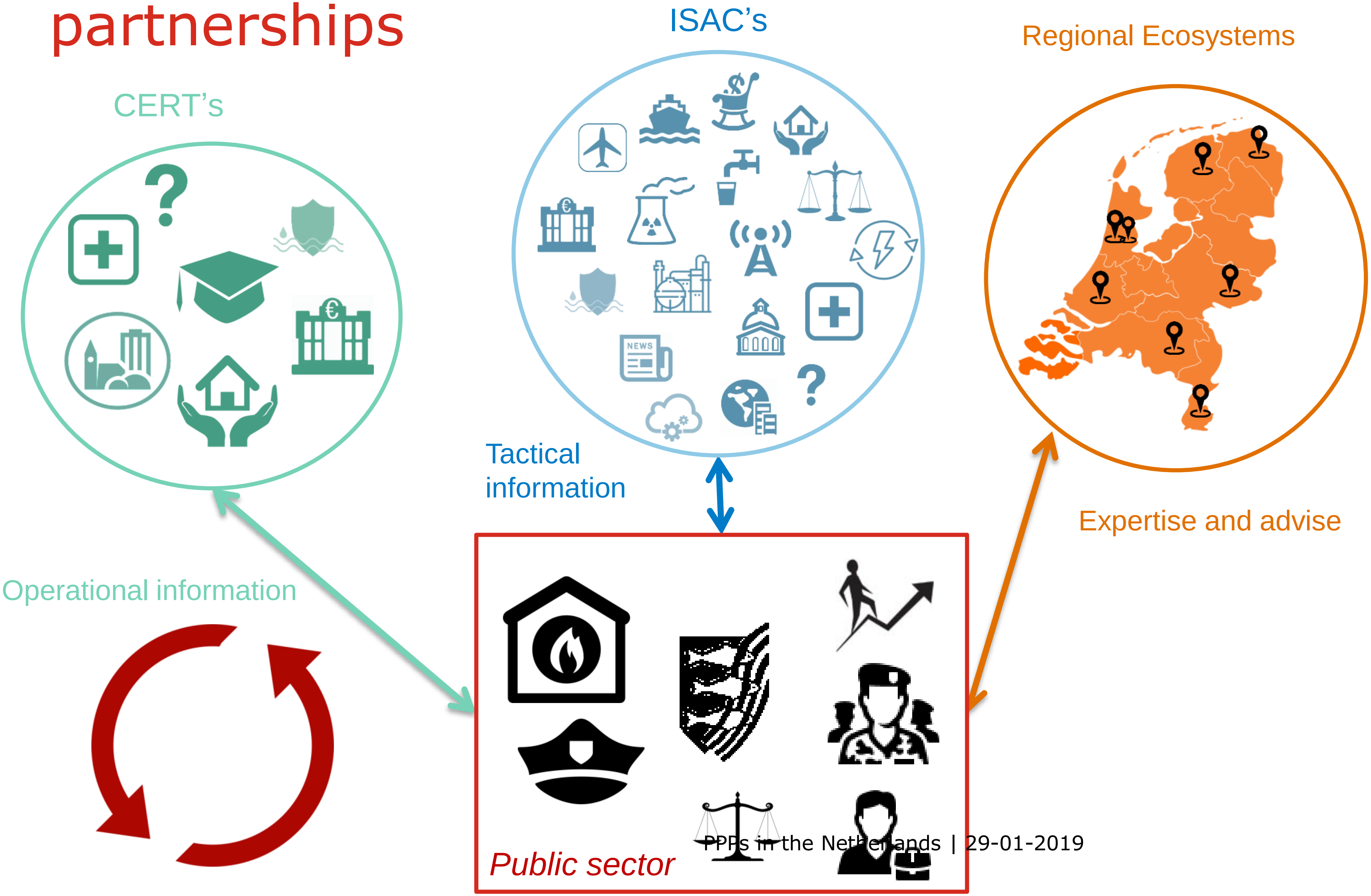
DTC

NCSC

Expertise and advise

Public sector

A nationwide network of cybersecurity partnerships



ISAC's

Regional Ecosystems

CERT's

Tactical information

Expertise and advise

Operational information

Public sector

ENISA and PPPs

- We welcome support of ENISA for ISACs,;
- Important to connect to existing structures;
- (European) ISACs are not a goal in itself;
- We would like to invite ENISA to also support MS in setting up national PPP structures.

I hacked the Dutch government
and all I got was this lousy t-shirt

Thank you, questions?

Gijs.peeters@ncsc.nl