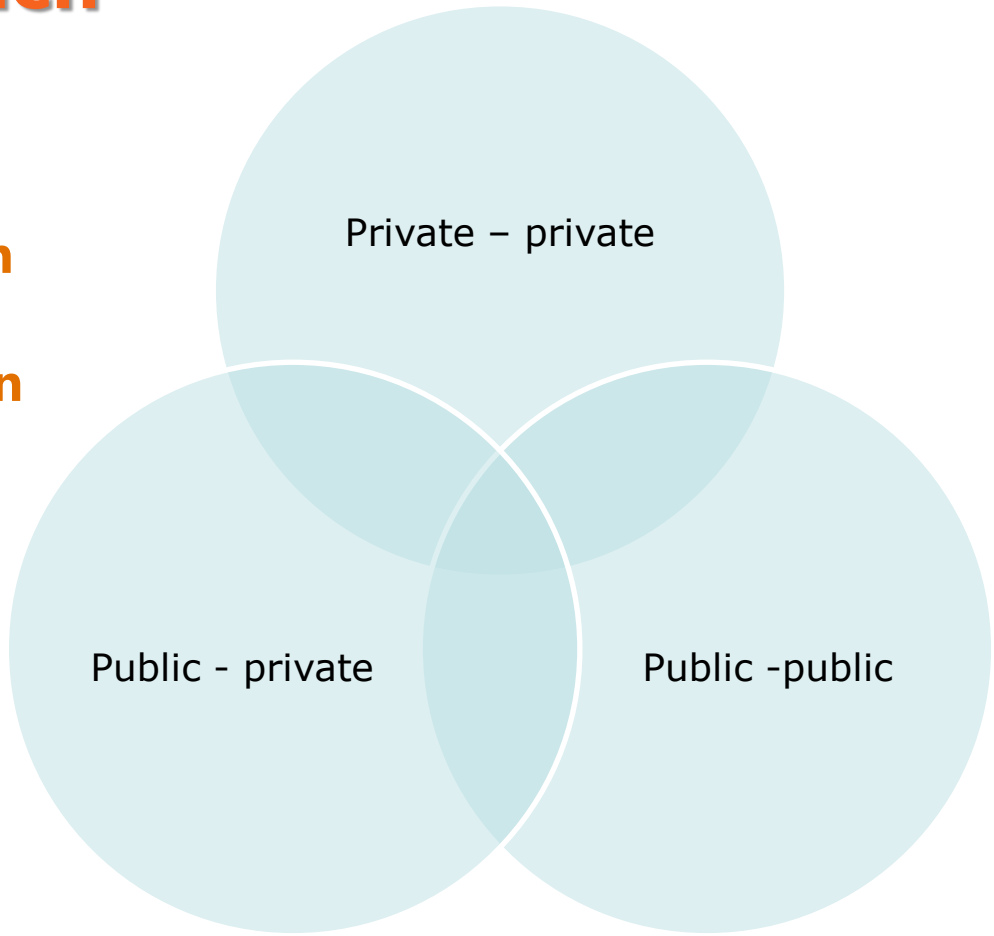
National Coordinator for Security and Counterterrorism
Ministry of Security and Justice

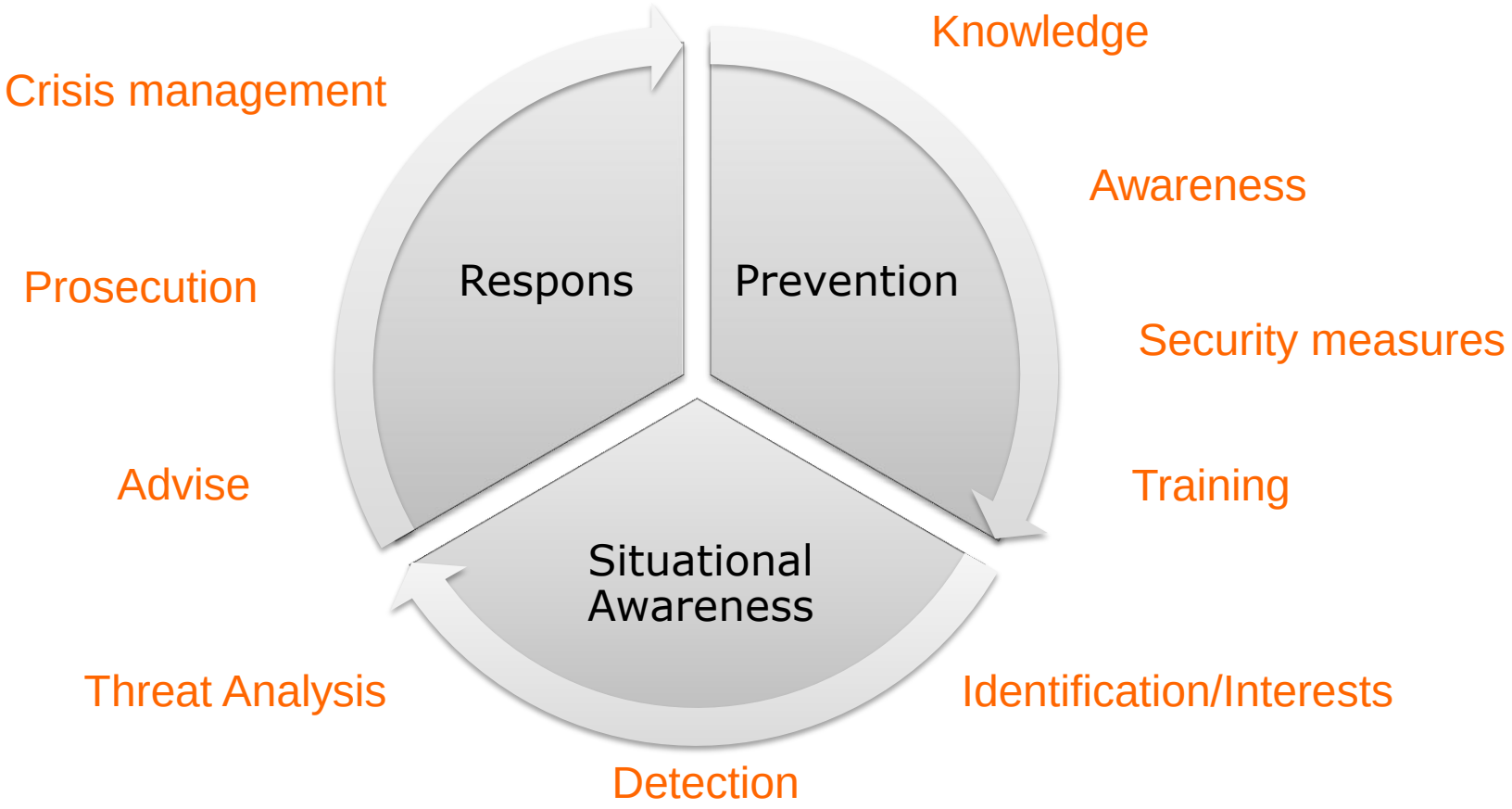
Cyber Security in the Netherlands

The Dutch Approach

Doctrine:
public private cooperation
&
private public participation



Cyber Security: The state of the art in the Netherlands



Cyber Security Assessment Netherlands (CSAN)

The CSAN is published annually. It is drafted by the NCSC together with its partners. It is accompanied by a policy brief.

Findings 2016 – published September 6, 2016.

- Professionals criminals have developed into advanced actors and execute long-term and sophisticated operations.
- Digital economic espionage by foreign intelligence services put pressure on Dutch competitiveness.
- Ransomware has become common and even more advanced.
- Advertising networks are still unable to counter malvertising.

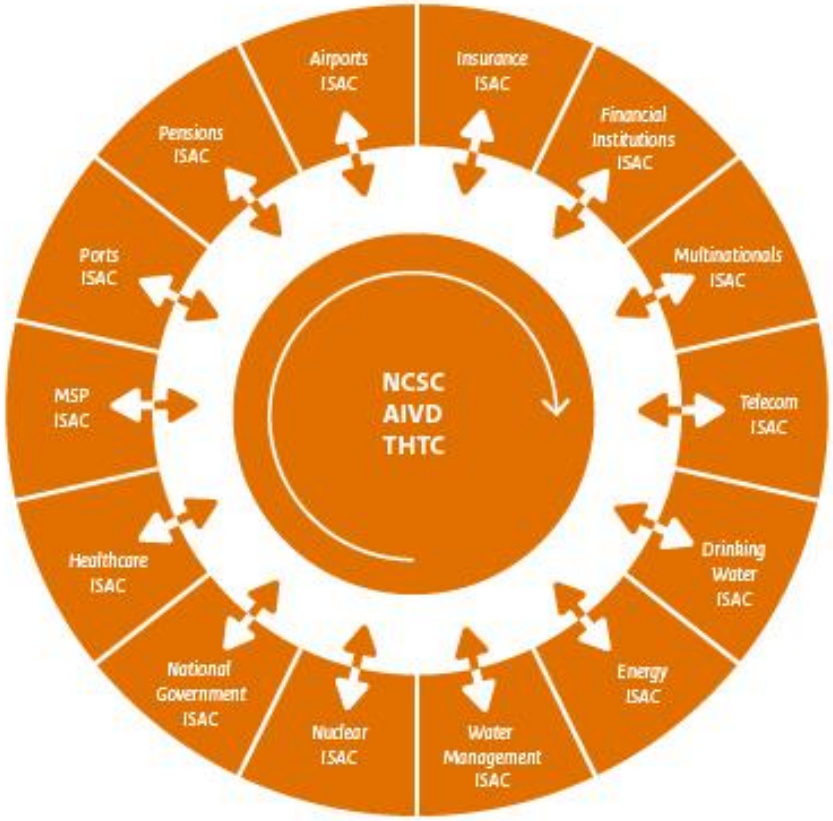
CERT-to-CERT information sharing

Most important for CERT-to-CERT cooperation: TRUST!

Various venues for information sharing

- Bilateral contacts
- Groups of CERTs, such as FIRST
- New addition: the CSIRT Network

Information sharing private sector – ISACs



Challenge: keep the number of participants at a level that still promotes trust and information sharing.

PPP Topics

- Incident response
- Crisis management
- Trends and threats analyses
- Development of capabilities
- Policy and regulation
- Networks

➢ Four PPP conditions:

1. Shared interests
2. Trust
3. Equality
4. Results

Next steps for European cooperation

- Making the CSIRT Network (and the Cooperation Group) a trusted and effective network is an important task.

- The national structures for cyber are different per country. Different Ministers are responsible. This makes it hard to have a meeting/conversation at the political level, which would be important. We need to find ways to engage the CSIRT Network.