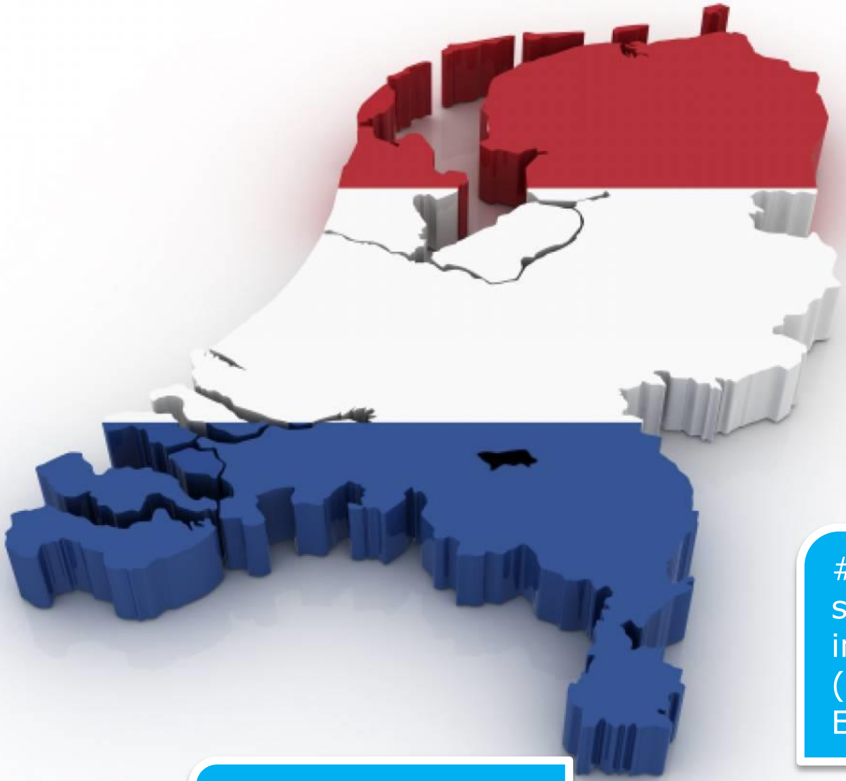
National Coordinator for Security and Counterterrorism
Ministry of Security and Justice

Netherlands Cyber Security Strategy

Michel van Leeuwen
Head of Cyber Security Policy
Ministry of Security and Justice

Netherlands: small country, big time vulnerable



#1
80% online banking

95% youth uses sociale media

#2
94% > 1 pc per family

#4 62% shops on internet (4th in EU)

#3
After VS en UK on internet

Internet ocean cable connects Europe through Amsterdam IX

Cyberthreat is substantial

- Hacking as much as bicycle theft in NL

- Risk e-fraude is 3,5% -> pickpockets 1,7%

(politieacademie, 2013)

- 13% van de Nederlanders slachtoffer van cyber crime

(Veiligheidsmonitor CBS , 2014)

The Netherlands: wake up calls (2011-now)

Diginotar

Leaktober

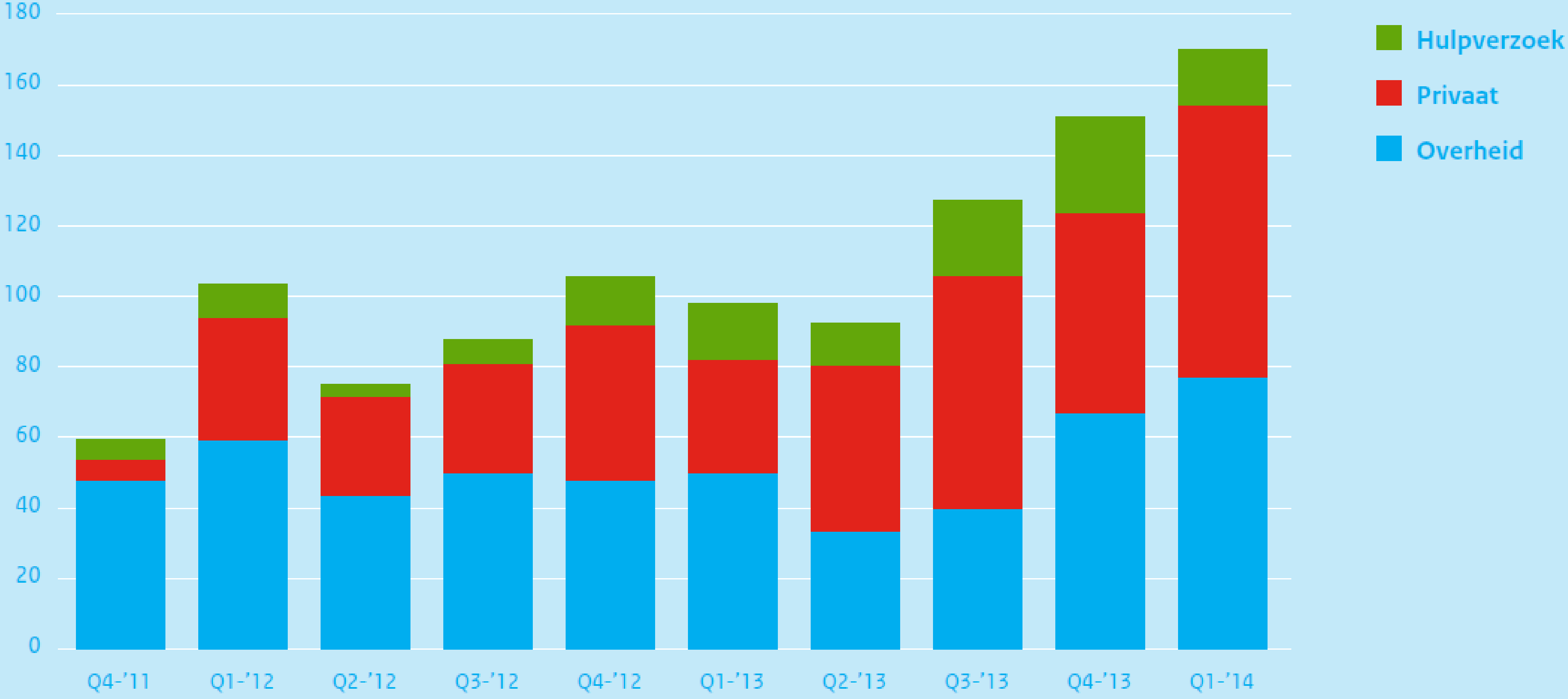
Pobelka

Dorifel

DDOS-attacks

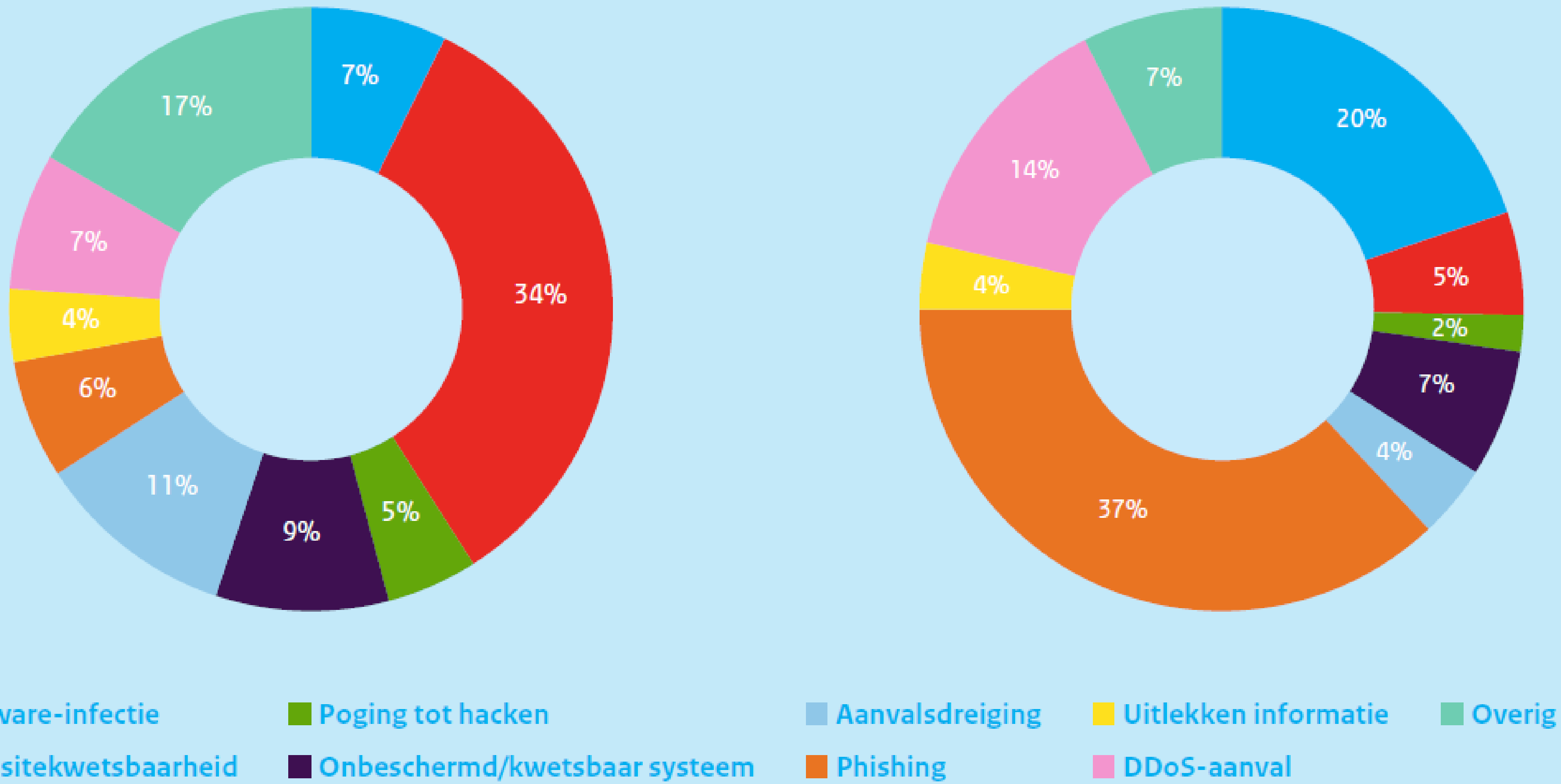
Hold Security

Door NCSC afgehandelde incidentmeldingen



Impact incidentmeldingen overheid

Impact incidentmeldingen privaat



Legislative framework

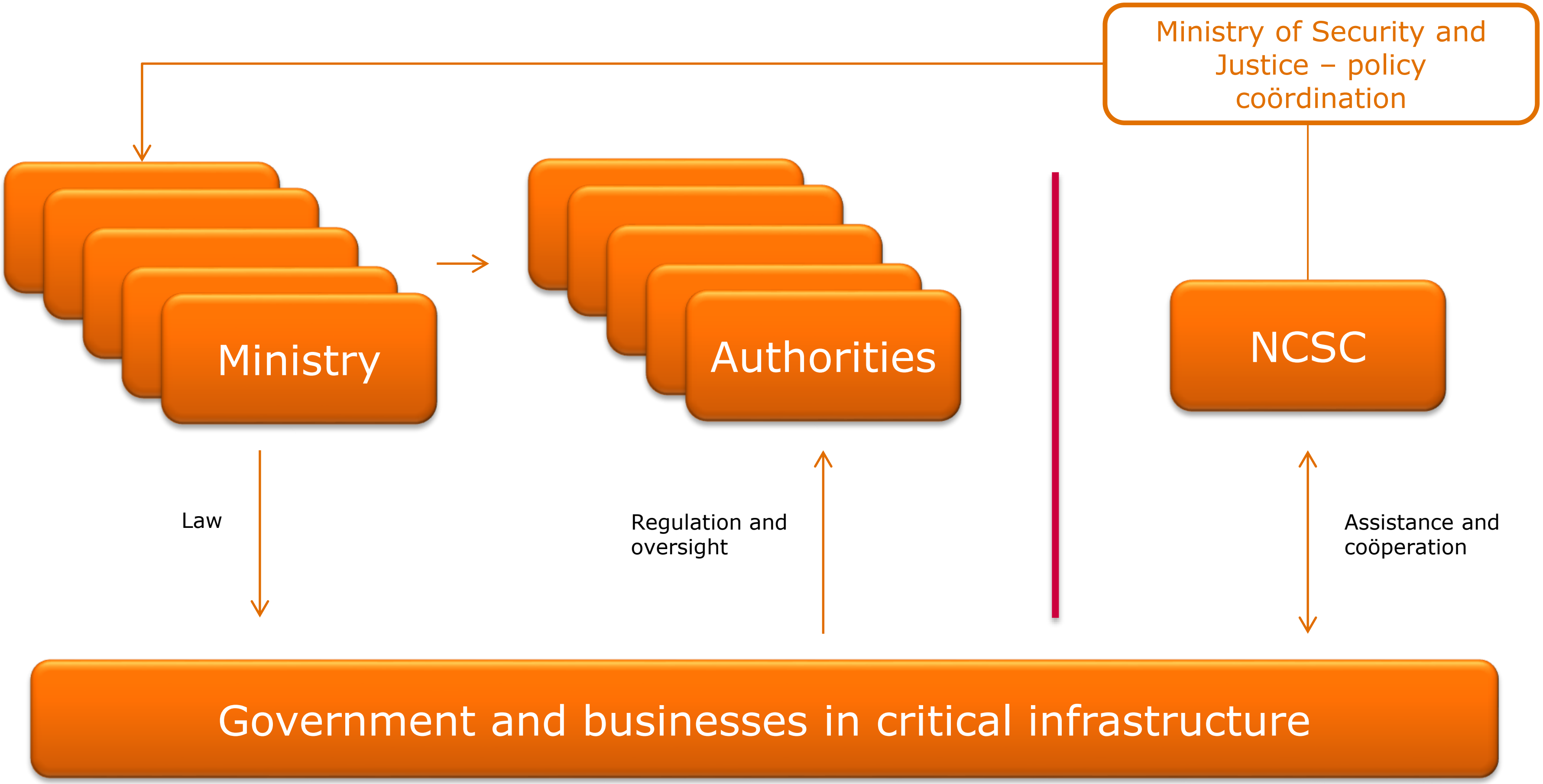
- Law - Security breach notification – in progress
- Law – Computer criminality III – in progress
- Budapest Convention
- EU – Directive Network and Information Security
- Law – Intelligence and Security Services
- Law – code of criminal procedure
- Guideline responsible disclosure

- Laws, directives and regulations on privacy, child abuse, financial sector, telecom ...

National cyber governance framework

NETWORK & INFOSECURITY	PROSECUTION	INTELLIGENCE	CONFLICT
NCSC	POLICE	AIVD	MOD
DEFCERT	Public Prosecution Service	MIVD	Military
Business-CERTs			NATO

Network & Infosecurity in the Netherlands



Ministry of Security and Justice – policy coördination

Ministry

Authorities

NCSC

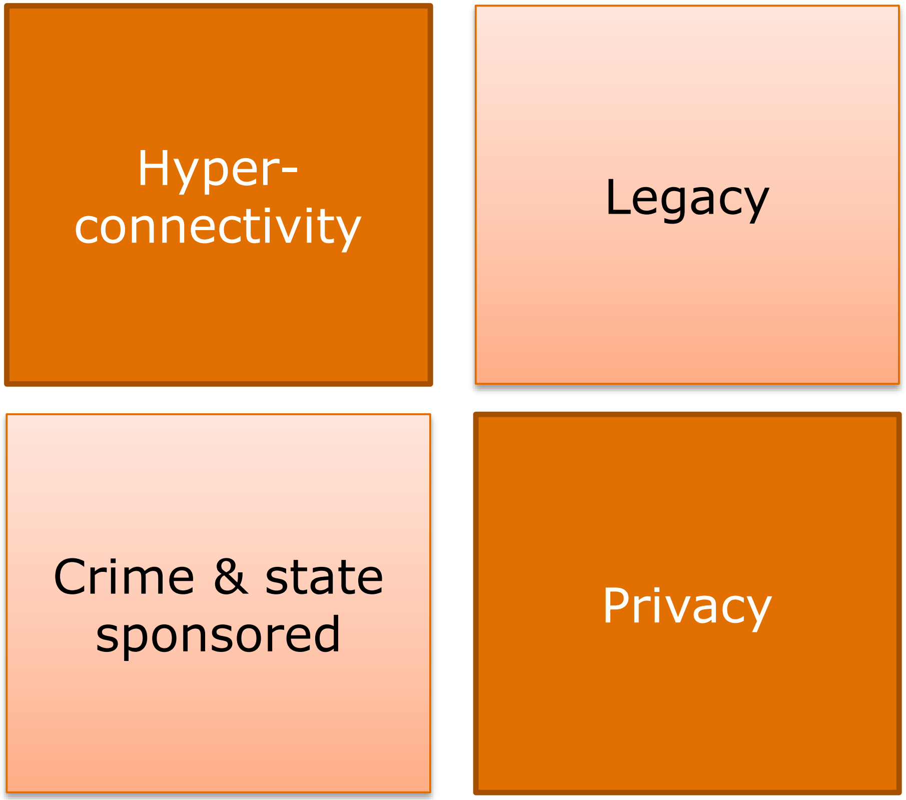
Law

Regulation and oversight

Assistance and coöperation

Government and businesses in critical infrastructure

Cyber security beeld: 4 belangrijke trends



Hyper-connectivity

Legacy

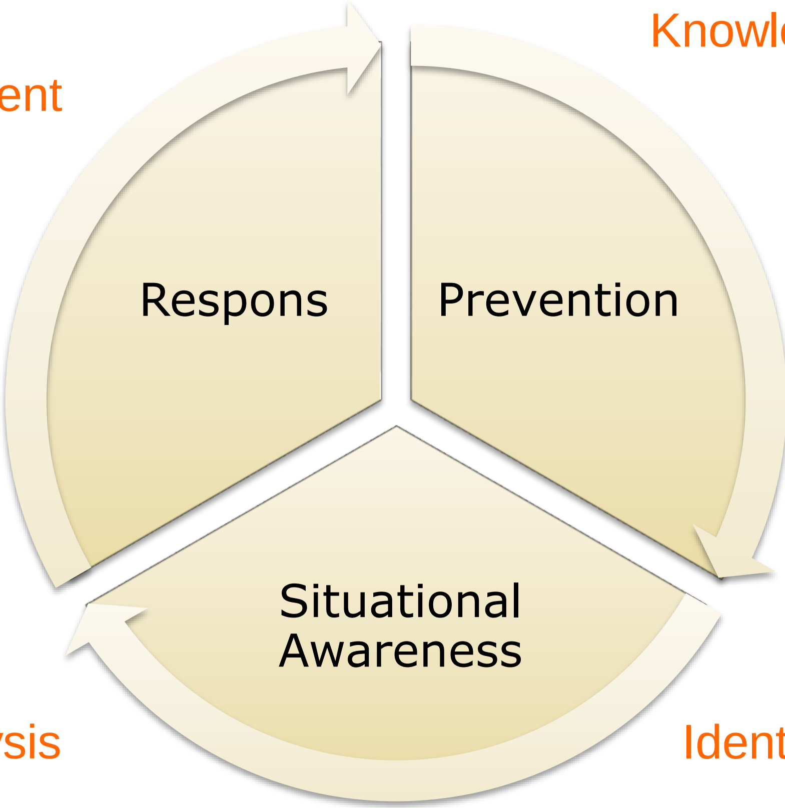
Crime & state sponsored

Privacy

Vision

The Netherlands, together with partners, are committed to create a secure digital domain in which the opportunities of digitalisation are used, threats are confronted an fundemental rights are protected.

Cyber Security: The state of the art in the Netherlands



Knowledge

Crisis management

Awareness

Prosecution

Security measures

Advise

Training

Threat Analysis

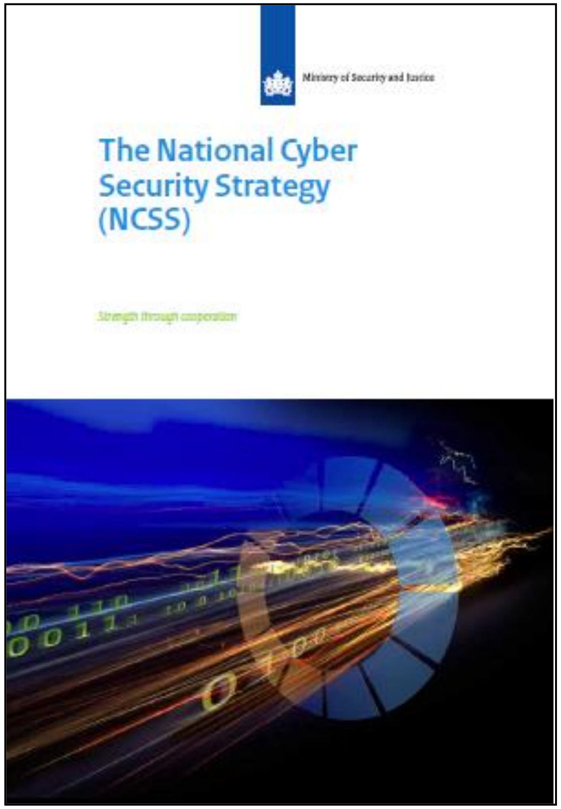
Identification/Interests

Detection

National Cyber Security Strategy I - 2011

- **Public Private Partnership**
- **First action programme:**

1. Setting up CS Council and National CS Centre
2. Setting up CS Threat Assessment
3. Increasing the resilience of critical infrastructure
4. Increasing response capacity on attacks/disruptions
5. Intensifying investigation and prosecution of cybercrime
6. Encouraging research and education



Ministry of Security and Justice

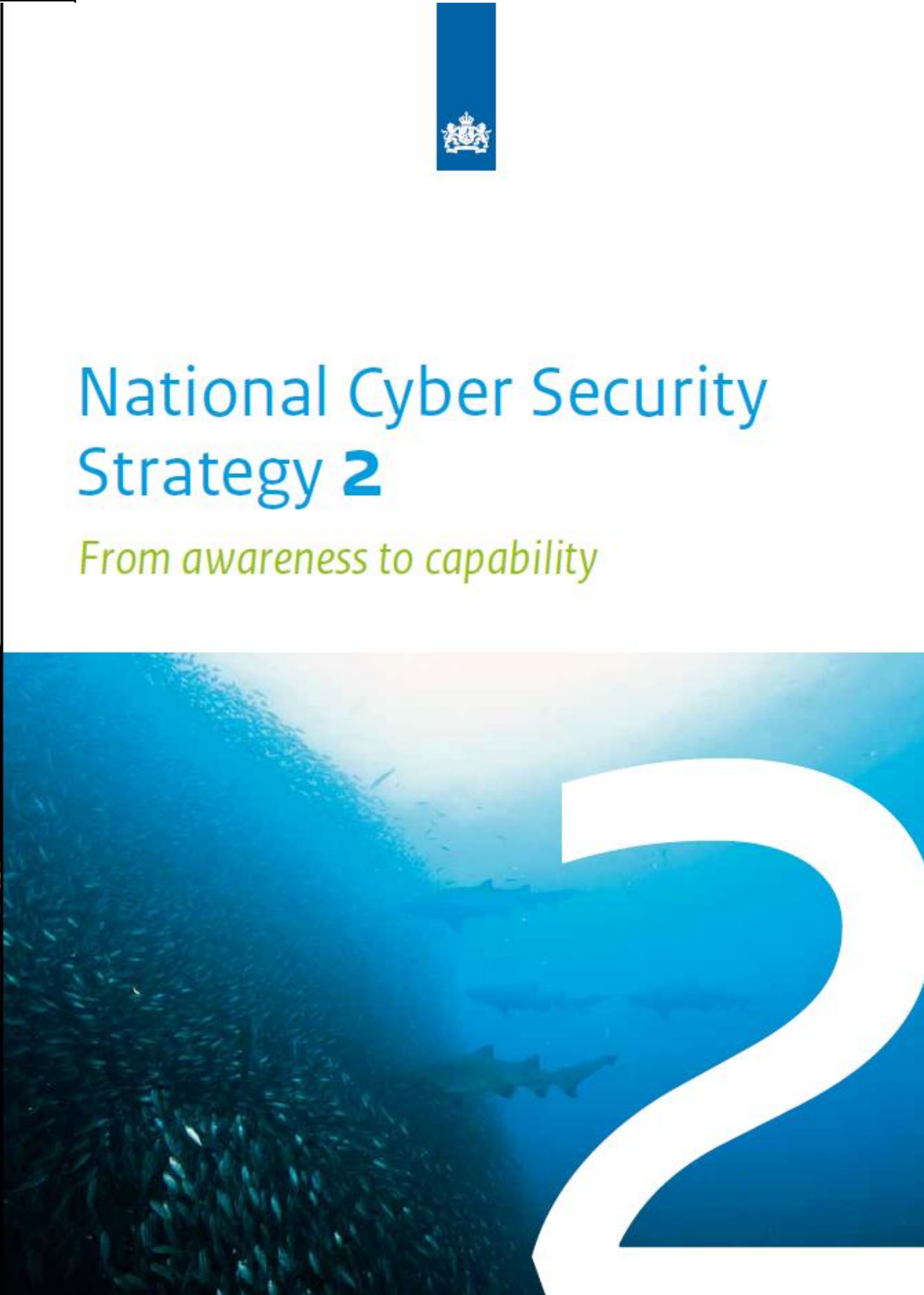
The National Cyber Security Strategy (NCSS)

Strength through cooperation

Ministry of Security and Justice

The National Cyber Security Strategy (NCSS)

Strength through cooperation

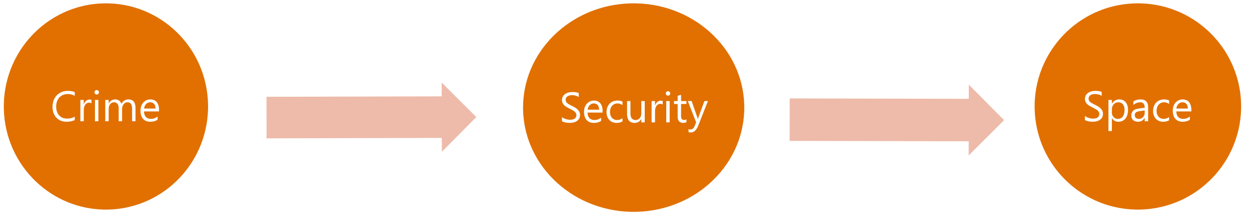


National Cyber Security Strategy **2**

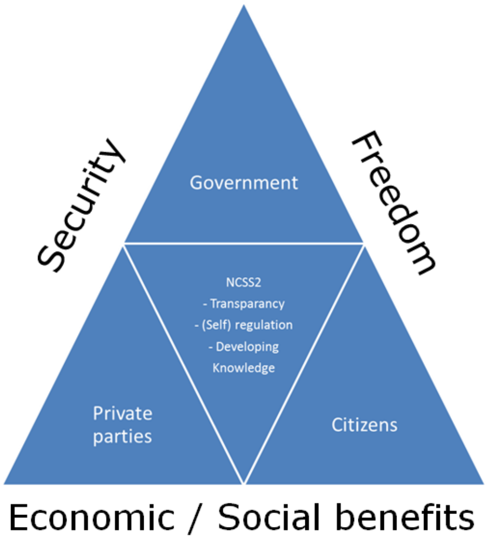
From awareness to capability

NCSS - 2011	NCSSII - 2013
Public Private Cooperation	Public Private Participation
Focus on structures	Focus on networks / strategic coalitions
Capacity building national oriented	Capacity building national as well as international
Do what you think is right (intuition)	Balance (as a result of knowledge / experience): - Measures throughout cyber chain - Threats, assets and controls.
Defining principles (for example, multistakeholder model, international cooperation).	Defining a vision: for example on governance
General approach	Risk based approach
Unaware → Aware	Aware → Skilled

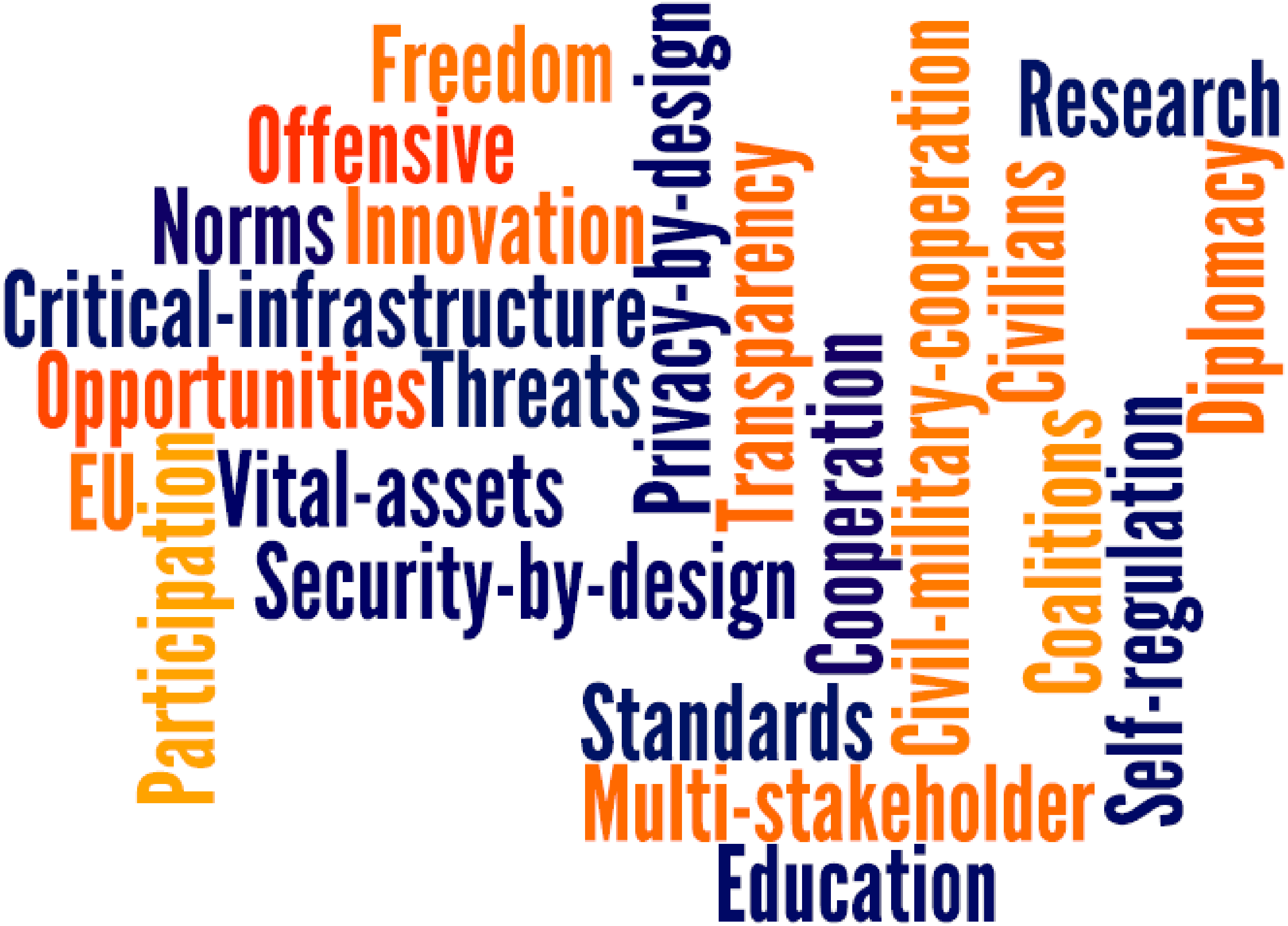
Developments

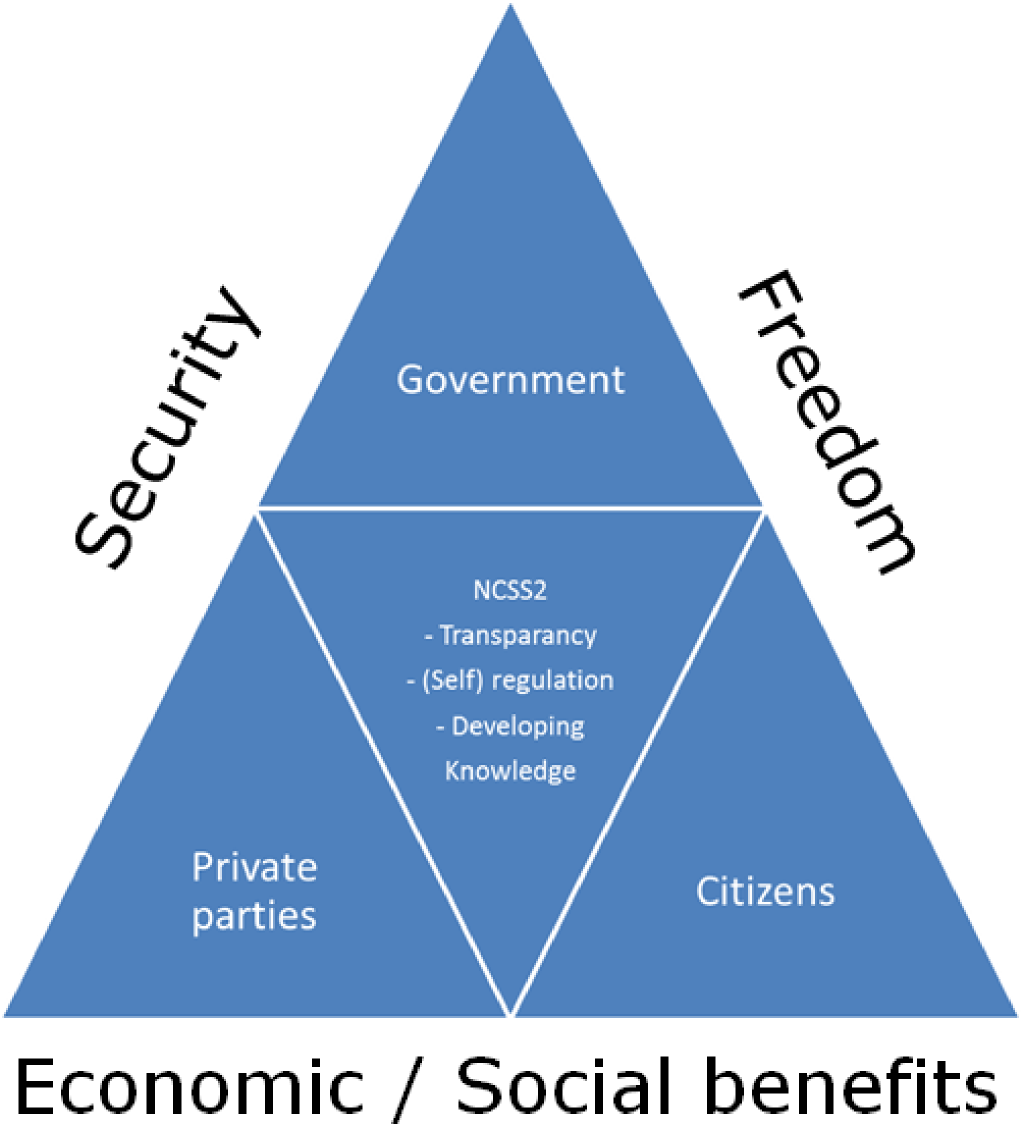


- Broad approach to “space” means triangle of:
  - Security
  - Freedom
  - Economic/social benefits
- A more international approach and increased number of actors
- Need for a comprehensive governance model



National Cyber Security Strategy II





Security

Freedom

Government

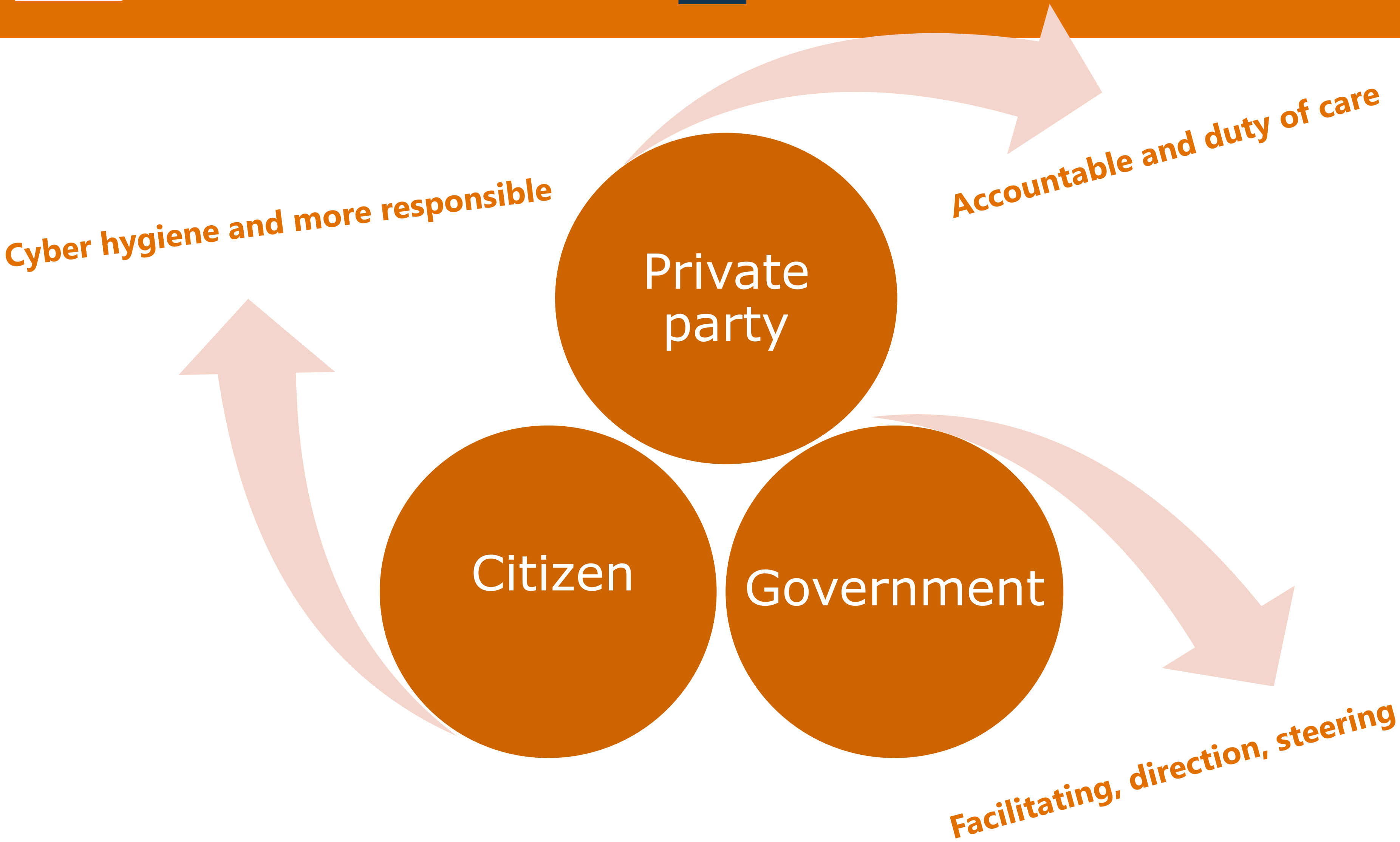
NCSS2

- Transparancy
- (Self) regulation
- Developing Knowledge

Private parties

Citizens

Economic / Social benefits



Private party

Citizen

Government

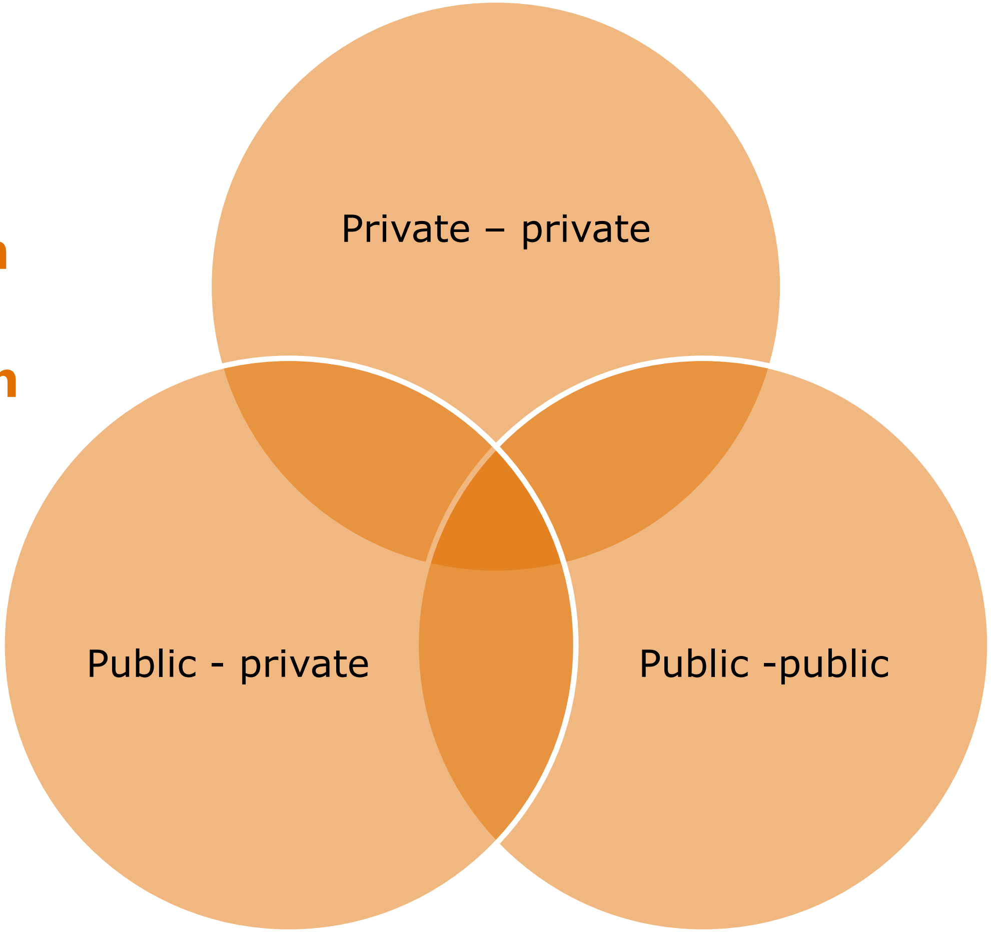
Cyber hygiene and more responsible

Accountable and duty of care

Facilitating, direction, steering

The Dutch Approach

Doctrine:
public private cooperation
&
private public participation



Relevant PPP cyber security fora

Strategic-policy level

Cyber Security Council

Committee Critical Infrastructure

NCSC Council

Tactical-operational level

ISAC’s

Liaisons

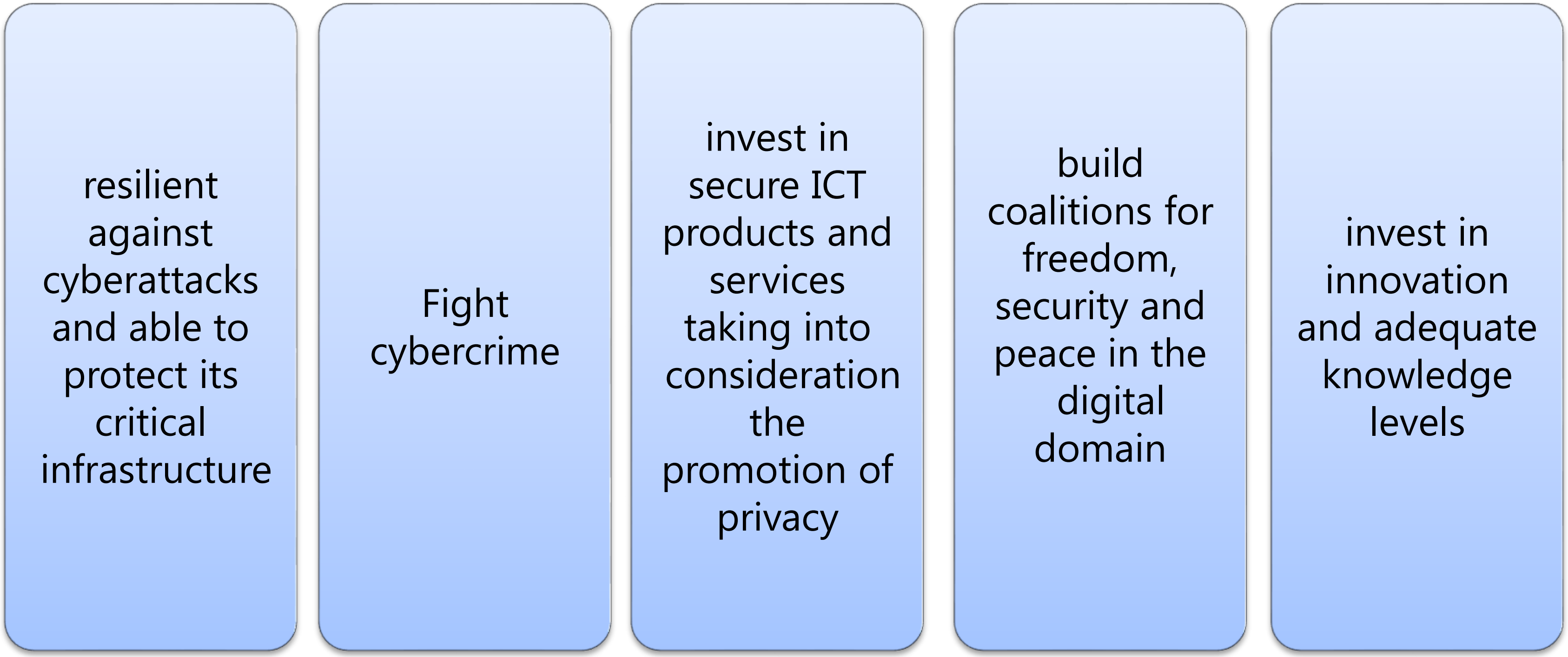
Incident Response Board

Operational level

Operational Incident Response Team forum

International CERT community

NL Cyber security



- resilient against cyberattacks and able to protect its critical infrastructure
- Fight cybercrime
- invest in secure ICT products and services taking into consideration the promotion of privacy
- build coalitions for freedom, security and peace in the digital domain
- invest in innovation and adequate knowledge levels

Action programme; some successes in 37 actions

- Trusted Network Initiative
- National detection and respons network
- Strengthening analysis capabilities
- Strengthening Military Cyber Defence capabilities
- Global conference on cyberspace 2015/GFCE
- Tender for the National Cyber Security Research agenda
- Public-Private taskforce cybersecurity education
- Fusion Cell – Economic Crimes Taskforce
- Engaging ethical hackers

Challenges for a secure Netherlands digital gateway to Europe

- Third Strategy? -> Netherlands Cyber Space Strategy
- The ‘harder’ things:
  - from awareness to responsible behavior
  - e-skills, e-government, e-bussiness
  - measuring effectiveness
  - getting private sector involved financially
  - responsible zero day usage
  - encryption/decryption
  - international standards
  - secure hard- and software
  - international norms
  - internetgovernance
  - future opportunities/threats – Big Data, Internet of Things