On the European experience in critical infrastructure

DCAF
a centre for security, development and the rule of law

Valeri R. RATCHEV

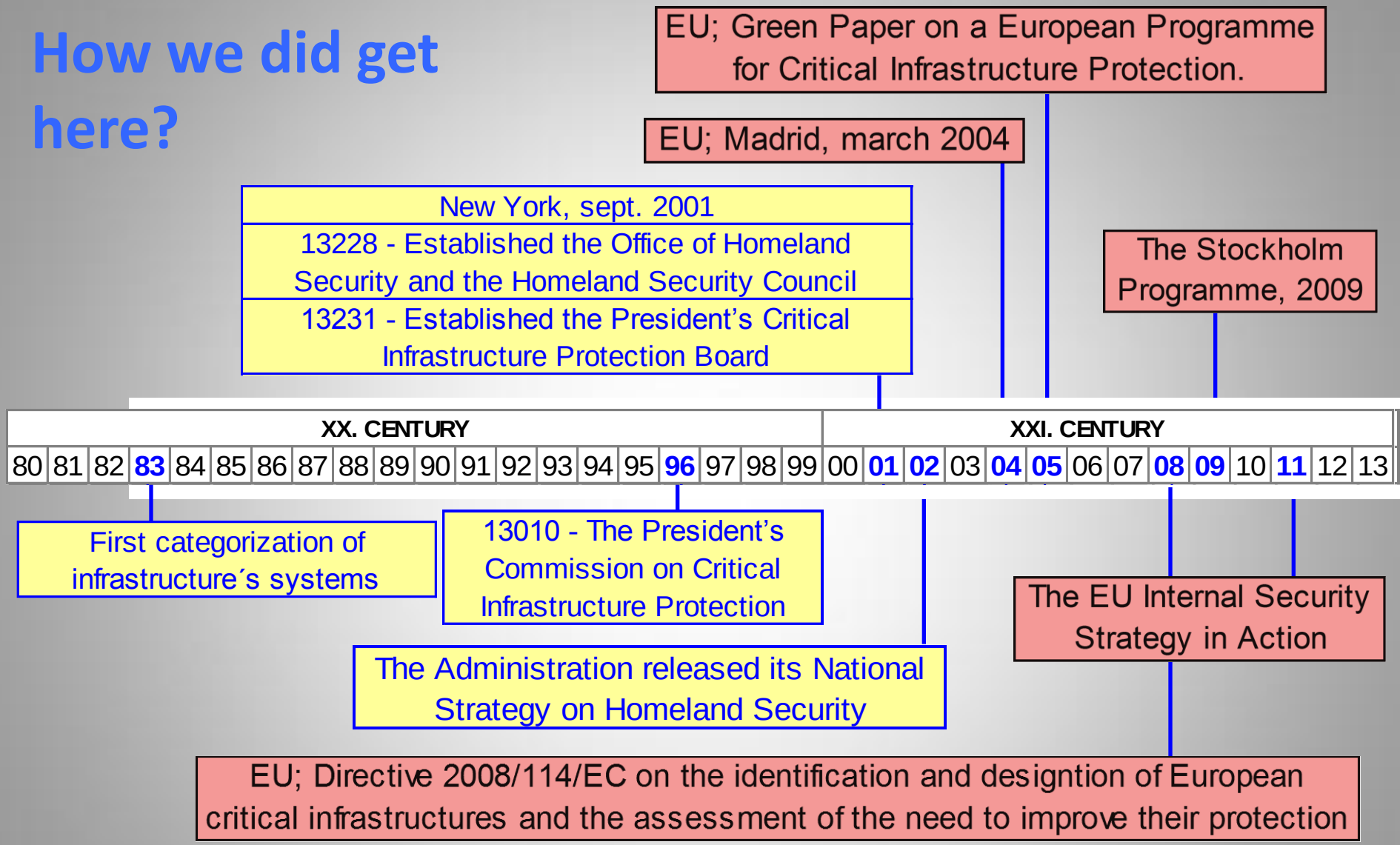
ratchevv@yahoo.com
@ratchevv

This presentation is about:

- Facts
- Observations
- Conclusions

… to read, understand and use the international experience

How we did get here?



European CI

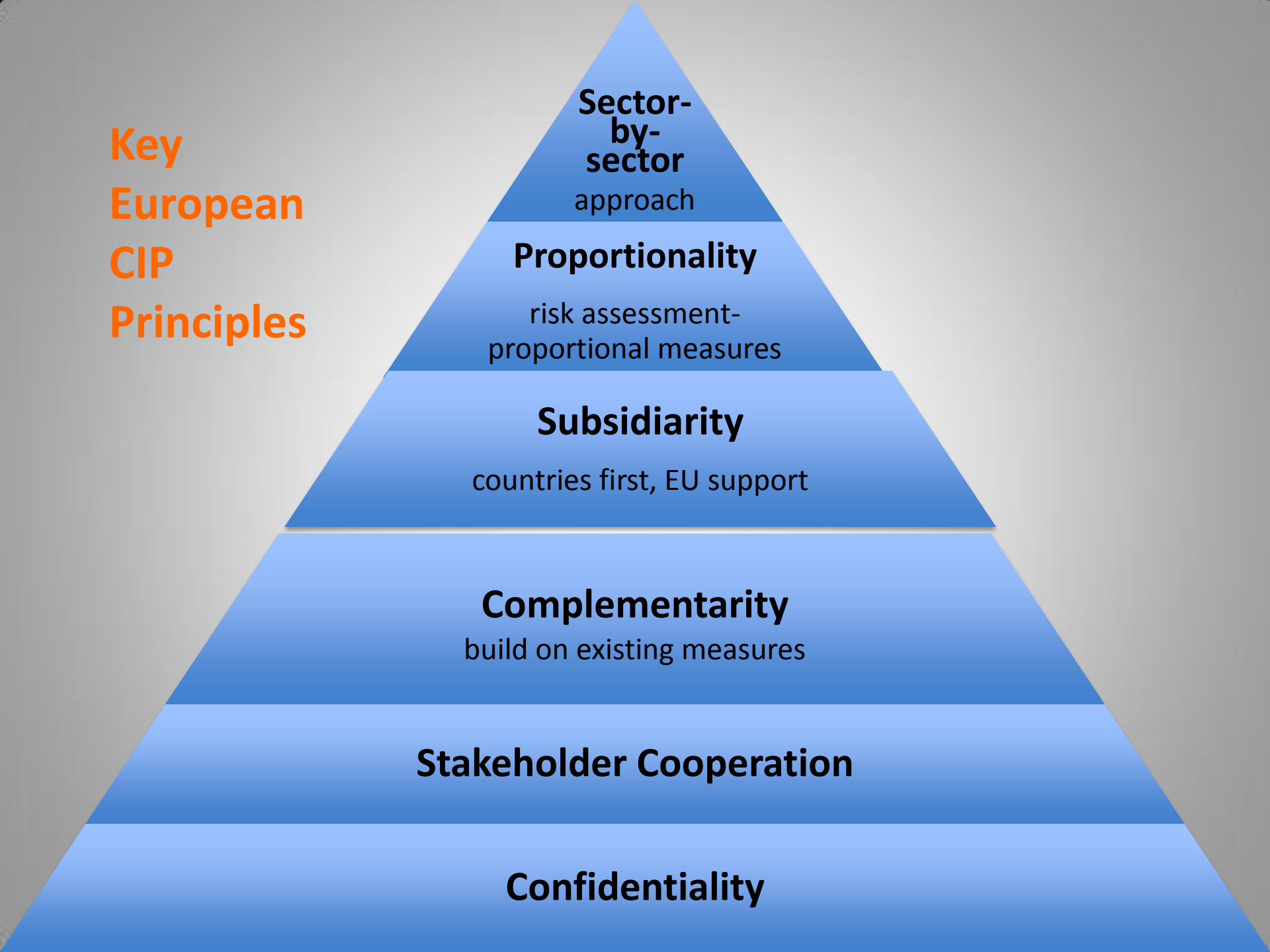
- Increasingly global
- Highly concentrated
- Complex – the weakest component determines the overall level of security of the system/state
- Unbounded or at least trans-border
- Networked through ICT
- Private (>85%) and public, internationally owned,
- More quickly developing than security standards
- Depends on political and business decision-makers
- **Vulnerability - an expanding phenomena**

EU paradigm: "Secure Societies" in Horizon 2020:

Specific mission areas

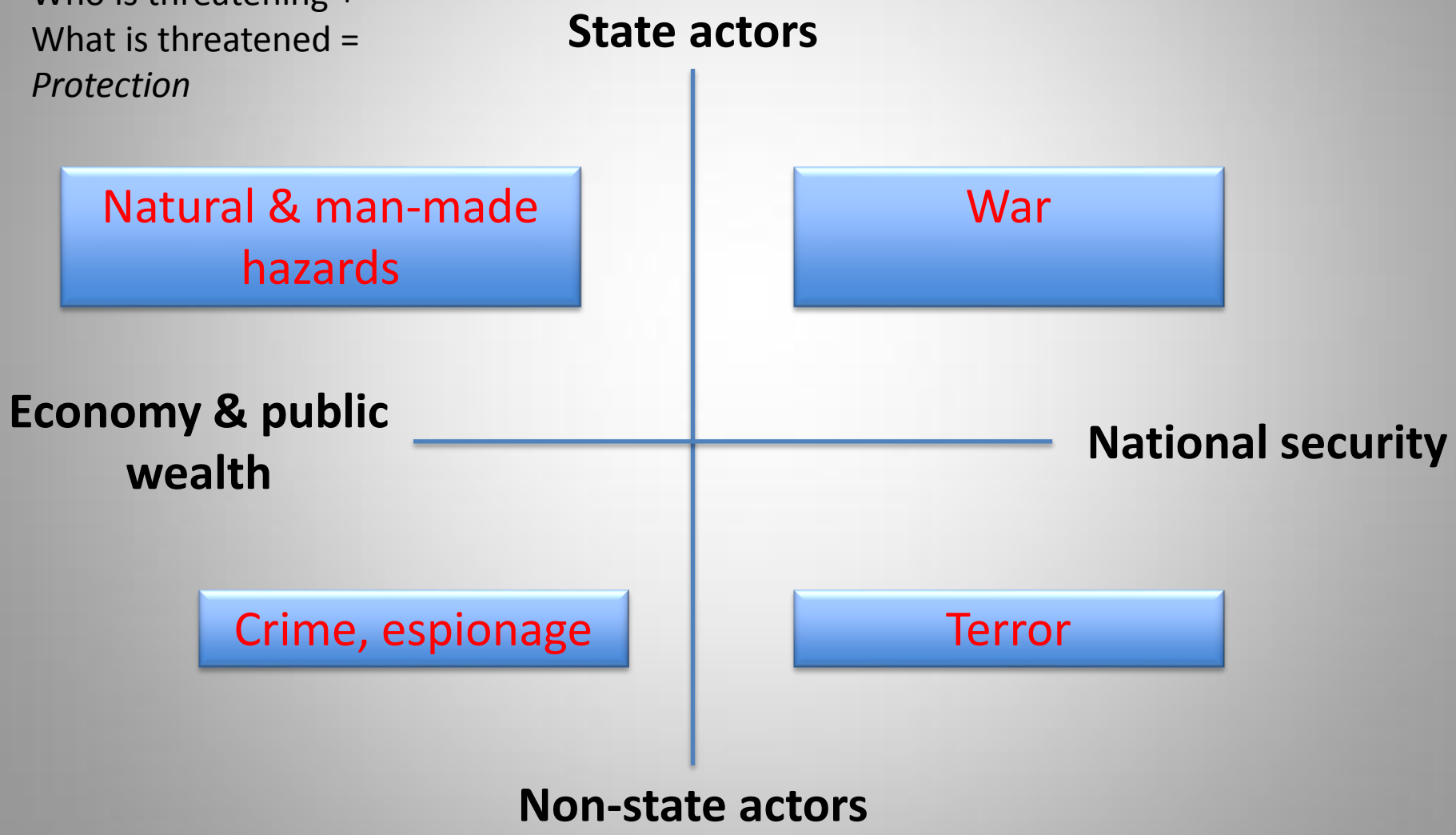
- Fighting crime and terrorism
- Strengthening security through border management
- Providing cyber security
- Increasing Europe's resilience to disasters **(including critical infrastructure protection)**
- Ensuring privacy in the Internet and enhancing the societal dimension
- CFSP related issues ('dual-use' – Civil focus)

Key European CIP Principles



Threat perception on CIP

Who is threatening +
What is threatened =
Protection



Definition

European Commission	"An **asset, system or part thereof** located in member states that is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact on a member state as a result of the failure to maintain those functions."
NATO	"Critical Infrastructure is those facilities, services and information systems which are so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economy, public health and safety and the effective functioning of the government."
Germany	"Critical infrastructures are **organisations and physical structures and facilities** of such vital importance to a nation's society and economy the community that their failure or degradation would result in sustained supply shortage, significant disruptions to public safety and security, or other dramatic consequences."
The Netherlands	"Critical infrastructure refers **to products, services and the accompanying processes** that, in the event of disruption or failure, could cause major social disturbance. This could be in the form of tremendous casualties and severe economic damage… "
The United Kingdom	The Critical National Infrastructure comprises of **those assets, services and system that support the economic, political and social life** of the UK whose importance is such that loss could: 1) cause large-scale loss of life; 2) have a serious impact on national economy; 3) have other grave social consequences for the community; or 4) be of immediate concern to the national government'

EU goes to Horizon 2020

- The EU Internal Security Strategy in Action (2010)
- Towards a stronger European disaster response: the role of civil protection and humanitarian assistance,(2010)
- The EU Action Plan on combating terrorism
- The Security Industry Policy Action Plan (2012)
- Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace COM (2013)
- The EU Strategy towards the Eradication of Trafficking in Human Beings 2012–2016
- European Programme for Critical Infrastructure Protection (2006)
- Civilian Headline Goal (2008)

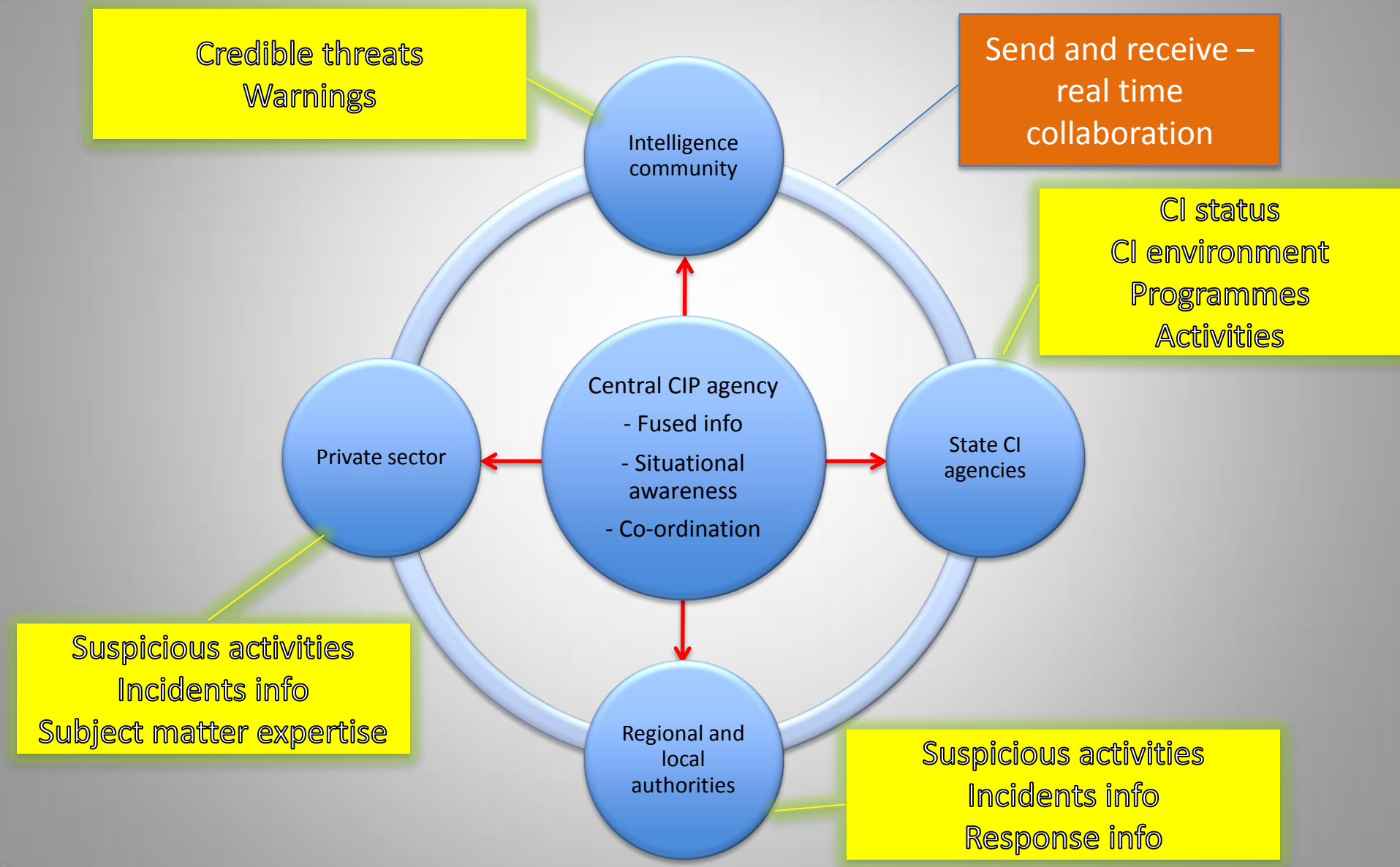
Sectorial coverage of CIP

Sector	Netherlands	UK	Germany	EU
Energy	x	x	x	x
ICT	x	x	x	x
Finance	x	x	x	x
Health care	x	x	x	x
Food	x	x	x	x
Water	x	x	x	x
Transport	x	x	x	x
Safety	x	Emergency med.		x
Government&PA	x	x	x	x
Chemicals	x			x
Defence industry	x			
Others	Judicial		Media & culture	Space and research facilities

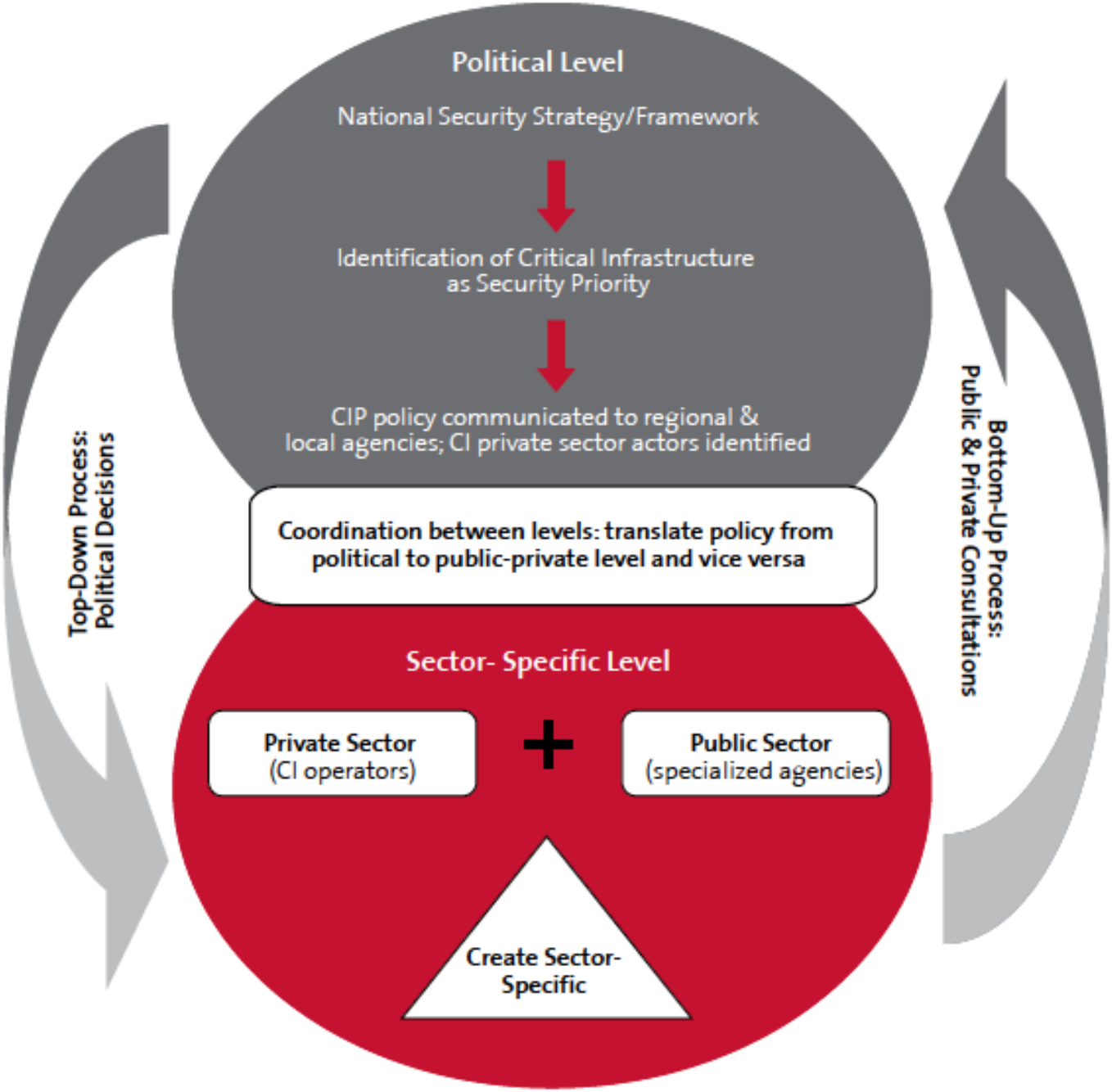
Largest number of CI sectors: USA

1. Agriculture and food
2. Energy
3. Public Health
4. Emergency Services
5. Government
6. Defense Industrial Base
7. Information & Telecommunications (Cyber)
8. Water Supply Systems
9. Transportation
10. Banking and Finance
11. Chemicals and Hazardous Materials
12. Postal
13. Ports and Shipping

Information sharing



CRITICAL INFRASTRUCTURE PROTECTION FRAMEWORK



CIP planning
(different approach – different results

- Scenarios
  - Context ("Alternative futures")
  - Situational
- Modeling and simulations
  - Data fusion: People and their institutions, Nations and international relations, Earth and its resources, Technologies and their exploration
- Capabilities based planning
  - Sectorial, but
  - Integrated

Organisational models

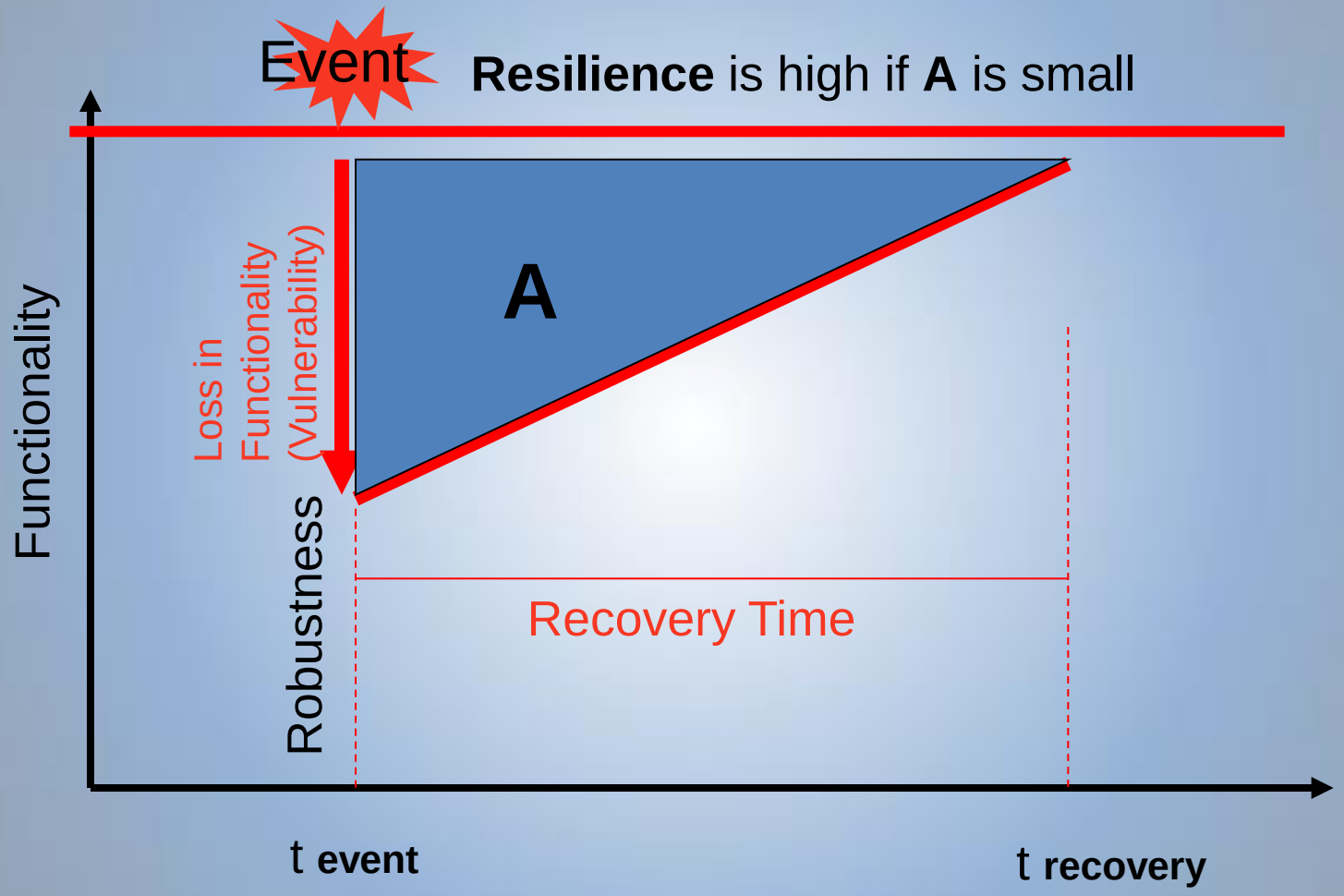
- **USA** – Department of Homeland Security
- **Canada** - ("Total defence") Office of Critical Infrastructure Protection and Emergency Preparedness
- **UK** – state: National Infrastructure Security Co-ordination Centre; pub./pra.: Information Assurance Advisory Council
- **Netherlands** – state: strategy, laws, innovations; private: "Electronic, Commerce, Platform Netherlands"
- **Switzerland** – state: political-military function (FDD,CP&S), no central body, no integration of private sector
- **Sweden** – ("Total defence") state: Swedish Emergency Management Agency + Technical competence Centre + CovCERT; private: fully integrated into SEMA
- **Finland** – ("Total defence") National Emergency Supply Agency
- **Germany** – MoI leads through Office of Civil Protection and Disaster assistance, Federal Office for Information Security, Police, FI Technical Support Service

Observations on European CIP policy

Complicating environment, difficult solutions

- Government (economy first), business (national and foreign) and society (liberal) are increasingly dependent on infrastructure
- Critical infrastructures are increasingly dependent on each other; urbanisation and re-industry will further complicate
- Our knowledge of the causes of failure or attack to infrastructure is still limited
- Complicated security context Disaster management, Terrorism, Climate change, National, Homeland, Societal, … security, Peace, Crisis, War, International
- EU member states still have fragmented CIP policies (highest interest in USA, Switzerland, Netherlands & Sweden; growing in Germany, France,)

The way ahead: protection through resilience



Conclusions on CIP policy

- The need to protect critical infrastructure is real, and potentially determines a trade-off between (short-term) efficiency and (long-term) resilience and sustainability.
- The key foundations of a CIP policy are a widely communicated **vision** and a forward-looking **strategy**, coupled with strong **political commitment**.

CIP policy recommendations

- **CIP policy should be:**
  1. An application of a more holistic all-hazards approach and focused on long-term resilience;
  2. Based on unified taxonomy, metrics and risk management;
  3. Centralised in a limited number of bodies;
  4. Inclusive of the cyber-dimension;
  5. Sector specific;
  6. Build sector-by-sector
  7. Internationally bounded.