Cross-Sectoral Scanning of Critical Infrastructure

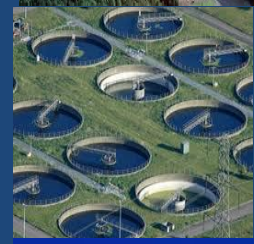


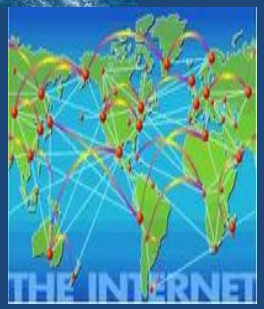
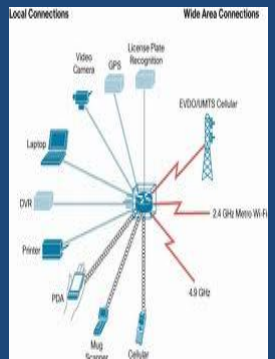


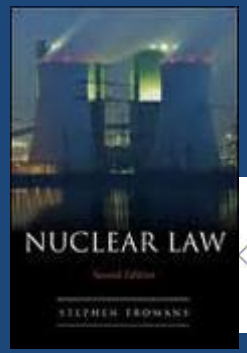








Iztok Prezelj

University of Ljubljana

Conference on Energy Reality in SEE, 2012, Ljubljana

SCENARIO – Northeast blackout in USA and Canada, blackout in Italy in 2003

- failure/loss of one line (Sammis-Star line in case of the US blackout and the line connecting Switzerland and Italy).
- Initial failures instantly created major and unsustainable burdens on lines in adjacent areas (overload), and the cascade spread rapidly as lines and generating units automatically tripped by protective relay action to avoid the physical damage.
- Cascade of failures and interruptions within the subsector (domino-like sequence of line outages)
- Effects other sectors + what they tell us about our readines for holistic crisis management

Facts about Critical Infrastructures

- CI consists of a **number of infrastructural sectors** that in turn embrace various sub-sectors, industries, services and products
- Problem of infrastructural complexity: CI involves **networks and complex systems of closely and increasingly interdependent elements ,** multiple layers
- A broad range of threats and risks to CI, increasing dependence from CI (risk society)

- A considerable **policy fragmentation** has been observed in the field of homeland security and related CIP due to the large institutional fragmentation and lack of multidisciplinary integrated analysis at the national and international levels
  - Sectoral and Bottom-up approaches are neccessary, but not sufficient. They have been fundamental in CIP due to the great differences in functions and structure among sectors. However, they paradoxically led to high policy fragmentation and competition, preventing the achievement of an integral response and preparedness.

- A call for new Critical Infrastructure protection policy:
  - Shaping a COMPREHENSIVE and INTEGRAL CIP POLICY, cross-sectoral approach based on an integral strategy, interconnected preparedness (Michel-Kerjan, 2003: 134; Auerswald, Branscomb, La Porte and Michel-Kerjan, 2006), a network and asymmetric approach (Lewis, 2006: 12-21) and a "system of systems" logic (Perenboom, 2001; Le Grand, Springinsfeld and Riguidel, 2003: 3 and Hellstrom, 2007: 416).

- How to achieve this? Methodological and policy problem

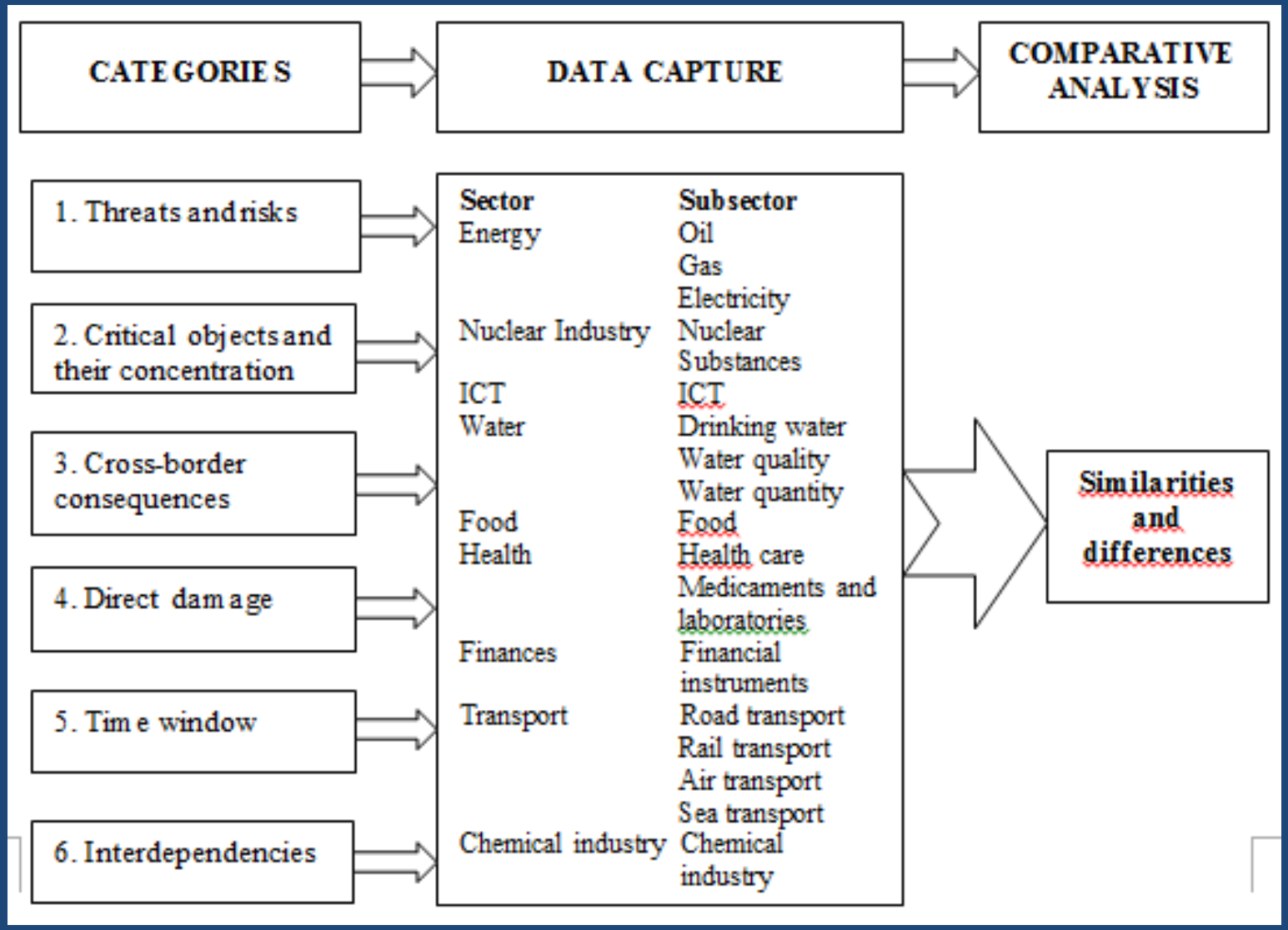
Cross-Sectoral Scanning of Critical Infrastructure – ICS

- **National research project "Definition and protection of Critical Infrastructures in Slovenia":** Structure - Researched topics:
  - **conceptualization** of critical infrastructures and their protection (theory),
  - **analysis of national concepts**, approaches, policies and systems for protection of critical infrastructures (case studies of Netherlands, Sweden and Germany),
  - **analysis of the EU approach** to conceptualization and protection of European Critical Infrastructures,
  - **Sectoral analysis of critical infrastructure** and protection mechanisms
  - **Cross-sectoral analysis and synthesis** of critical infrastructure and protection mechanisms,
  - **Recommendations** to Slovenian Government on how to proceed with the policy in this field.

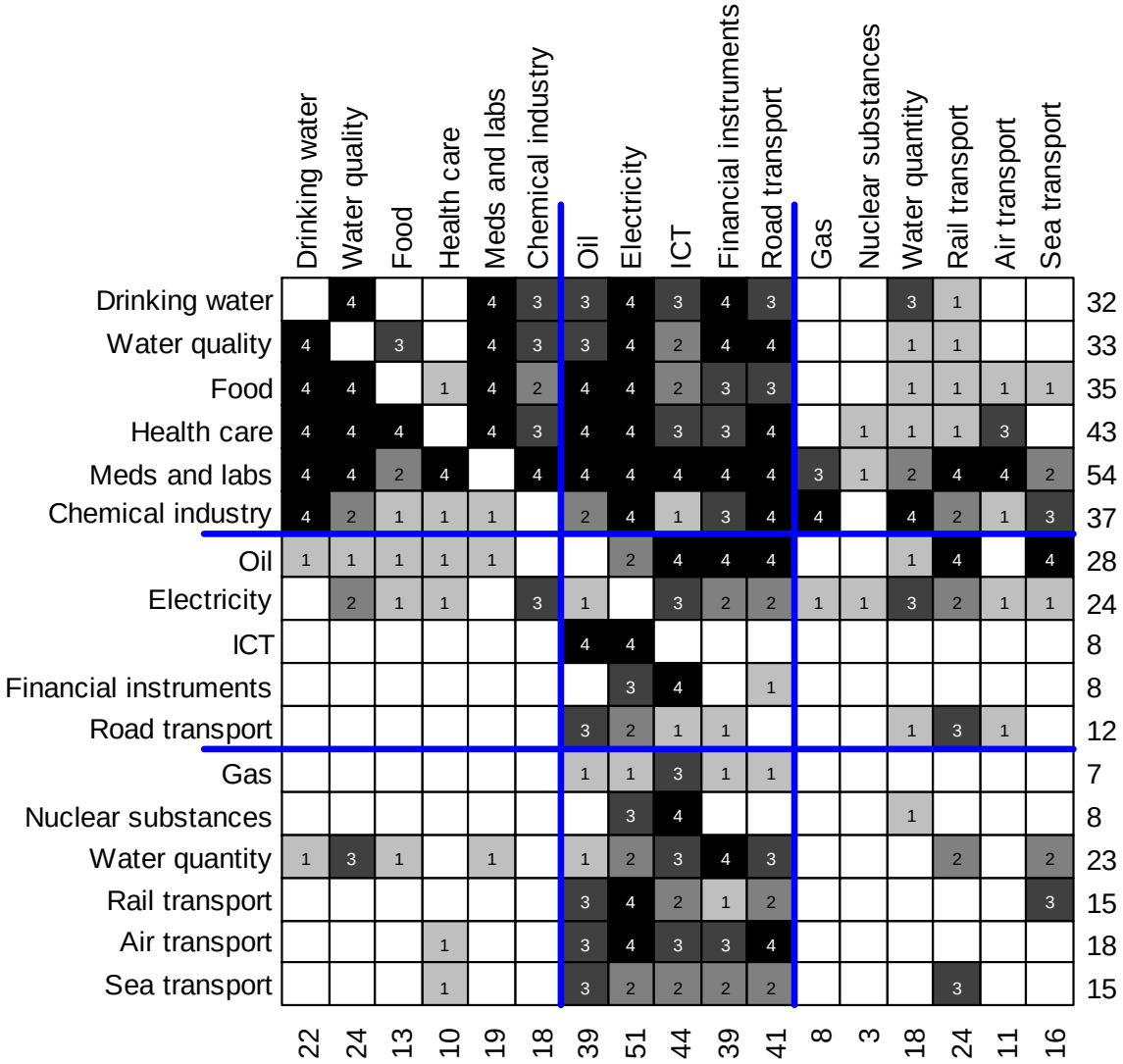
Data collection – testing the ICS approach

- Questionnaire containing the same variables to be assessed in various subsectors
- Test case SLOVENIA: developed and small
- joint preparatory workshop, 17 subsectoral workshops,
- Sample: 121 relevant experts representing owners, managers and administrators, relevant security agencies
- CONSENSUS by EXPERTS on workshops
- Cooperation with Governmental Interagency Coordination Group for Critical Infrastructure protection and ministries

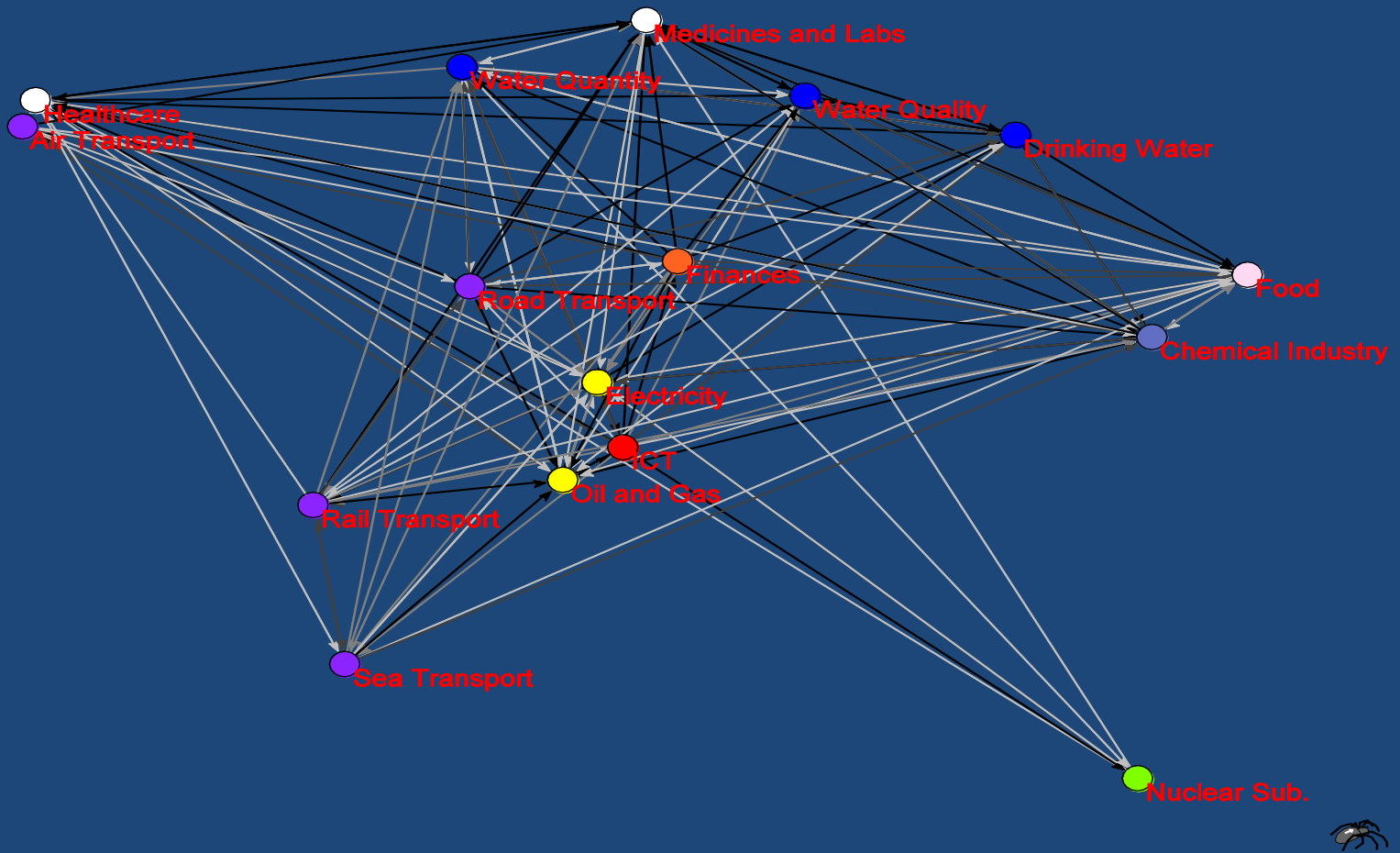
Integral Cross-sectoral Scanning:



Interdependency Matrix (on the scale from 0 to 4)



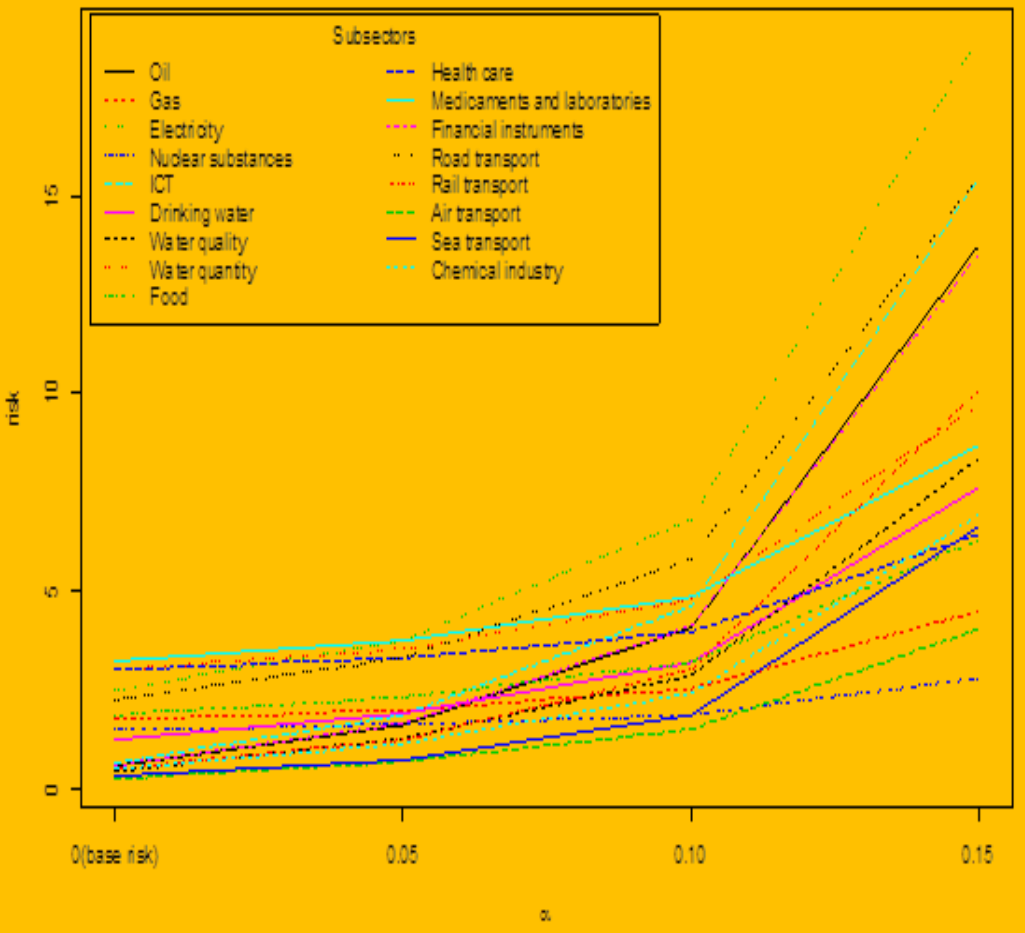
Network of national critical infrastructure (based on calculation of ALPHA CENTRALITY)

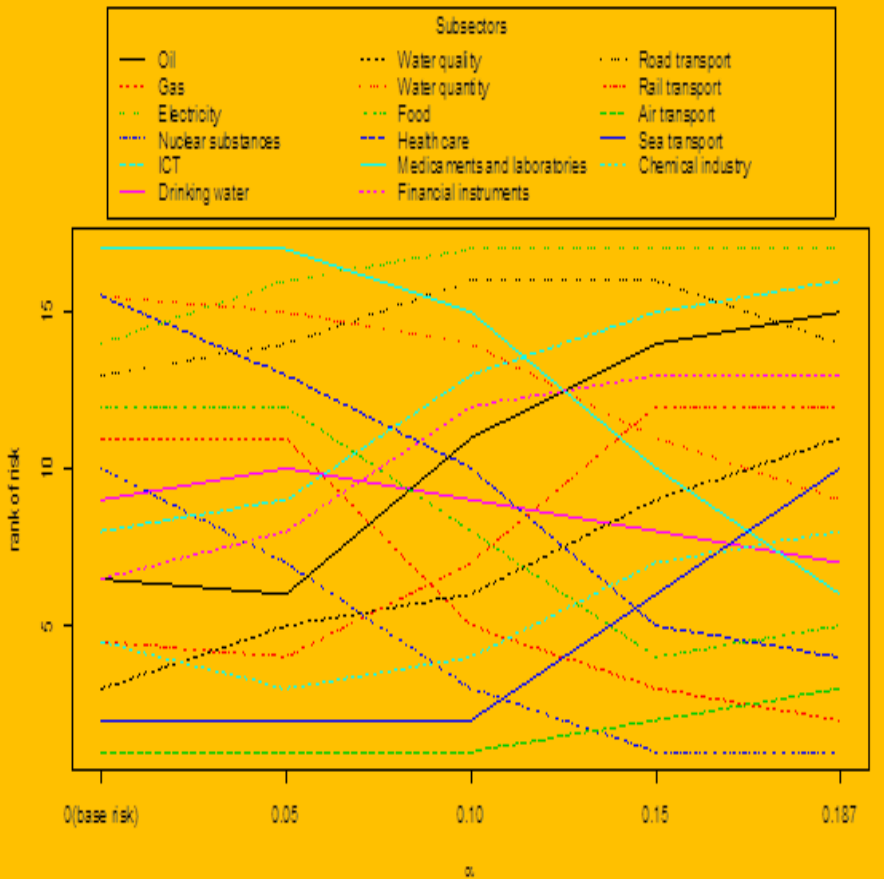


Input and output conections

Subsector	Number of output connections	Sum of output connections	Normalized sum of output connections	Number of input connections	Sum of input connections	Normalized sum of input connections
Oil and Gas	13	40	0,666667	12	28	0,466667
El. Energy	15	50	0,833333	14	24	0,4
Nuclear Substances	3	3	0,05	3	8	0,133333
ICT hardware	15	42	0,7	2	8	0,133333
Drinking water	7	22	0,366667	10	32	0,533333
Water quality	8	24	0,4	11	33	0,55
Water quantity	10	19	0,316667	11	23	0,383333
Food	7	13	0,216667	14	35	0,583333
Health provision	7	10	0,166667	14	48	0,8
Medicaments and laboratories	8	20	0,333333	15	51	0,85
Financial infrastructure	13	39	0,65	3	8	0,133333
Road transport	13	40	0,666667	7	12	0,2
Rail transport	11	24	0,4	6	15	0,25
Air transport	6	12	0,2	6	18	0,3
Sea transport	7	16	0,266667	7	15	0,25
Chemical industry	6	19	0,316667	14	35	0,583333

Network-based Risk

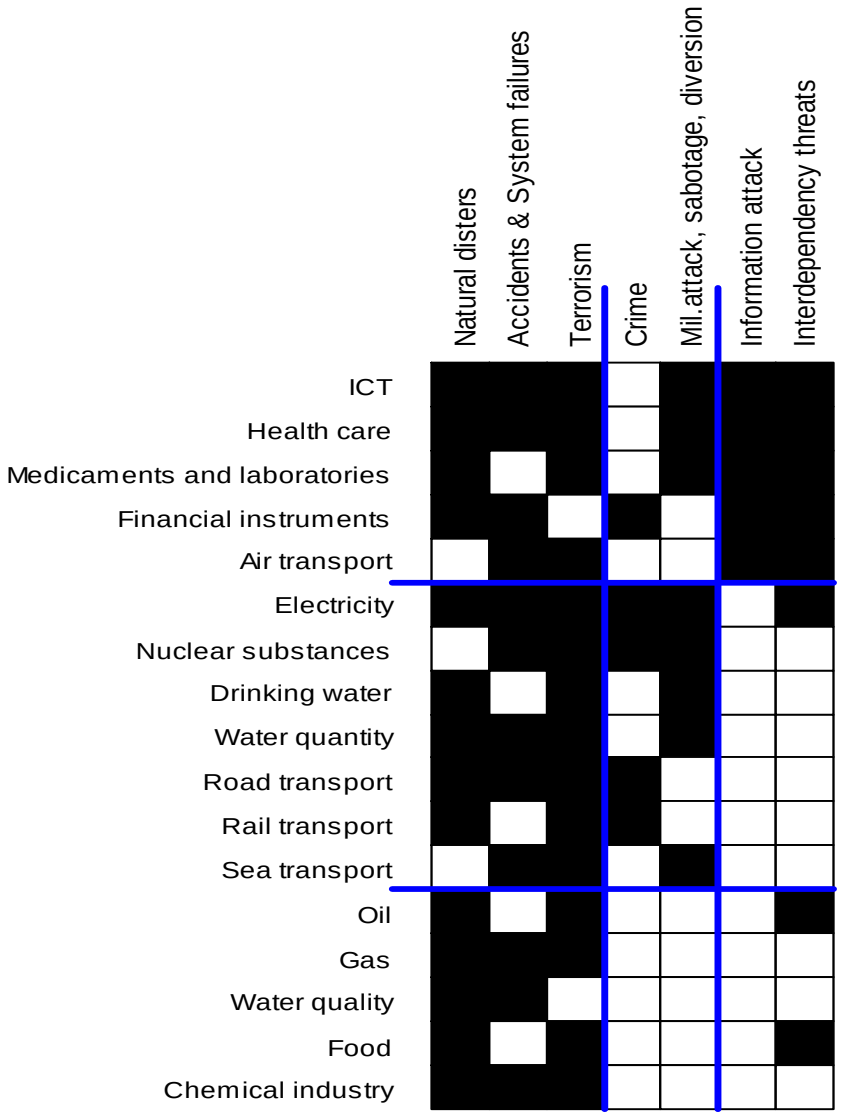




Time before complete disruption creates a crisis

Time window for serious impact on society:				
Subsector	0-12 hours	12 to 48 hours	2 days to one week	More than one week
Electricity	X			
Gas	X			
Pre-hospital care	X			
Medicaments, pharmaceuticals and laboratories	X			
Road transport	X			
Water quantity monitoring	X			
Nuclear substances	X			
Food		x		
Hospital care		x		
Drinking water		x		
Financial instruments			X	
Oil			X	
ICT software			X	
ICT communication and hardware			X	
Rail transport			X	
Sea transport				x
Air transport				x
Chemical industry				x
Water quality				x

Matrix of similarly threatened subsectors



Joint threats

Sectorally specific threats

What Social Consequences would Follow a Subsectoral Malfunction?

	Categories									
Subsectors	**c1) Population**	**C2) Econ. damage**	**C3) Public effects**					**C4) Environ. effects**		**C**
			C3.1) public services	C3.2) public trust	C3.3) public/social order	C3.4) end users (% of affected population)	C3.5) geopol. effects	C4.1) useless territorial area (% of national territory)	C4.2) share of homeless popul. (%)	
Oil	0	3	0	4	4	3	2	0	0	**1,75**
Gas	0	3	0	4	2	0	4	0	0	**1,75**
Electricity	2	4	4	4	4	4	3	0	0	**2,5**
Nuclear substances	1	1	0	4	3	0	2	0	0	**1,5**
ICT	0	4	4	4	1	3	3	0	0	**2**
Drinking water	2	4	2	4	1	4	3	0	0	**2,5**
Water quality	1	3	1	3	1	2	2	0	0	**1,75**
Water quantity	2	4	2	4	2	0	3	2	0	**3**
Food	4	4	4	4	4	4	3	0	3	**3,75**
Health care	4	4	1	4	4	1	3	0	0	**3**
Medicaments and laboratories	4	4	4	4	4	2	4	0	1	**3,25**
Financial instruments	0	4	1	3	1	0	0	0	0	**1,75**
Road transport	2	4	0	3	0	2	2	0	0	**2,25**
Rail transport	0	3	1	3	0	0	1	0	0	**1,5**
Air transport	0	1	1	3	0	0	2	0	0	**1**
Sea transport	0	2	0	3	0	0	1	0	0	**1,25**
Chemical industry	2	2	0	4	1	0	2	0	0	**2**
SUM	**24**	**52**	**25**	**51**	**32**	**25**	**40**	**2**	**4**	

Critical objects and geographic areas of their concentration

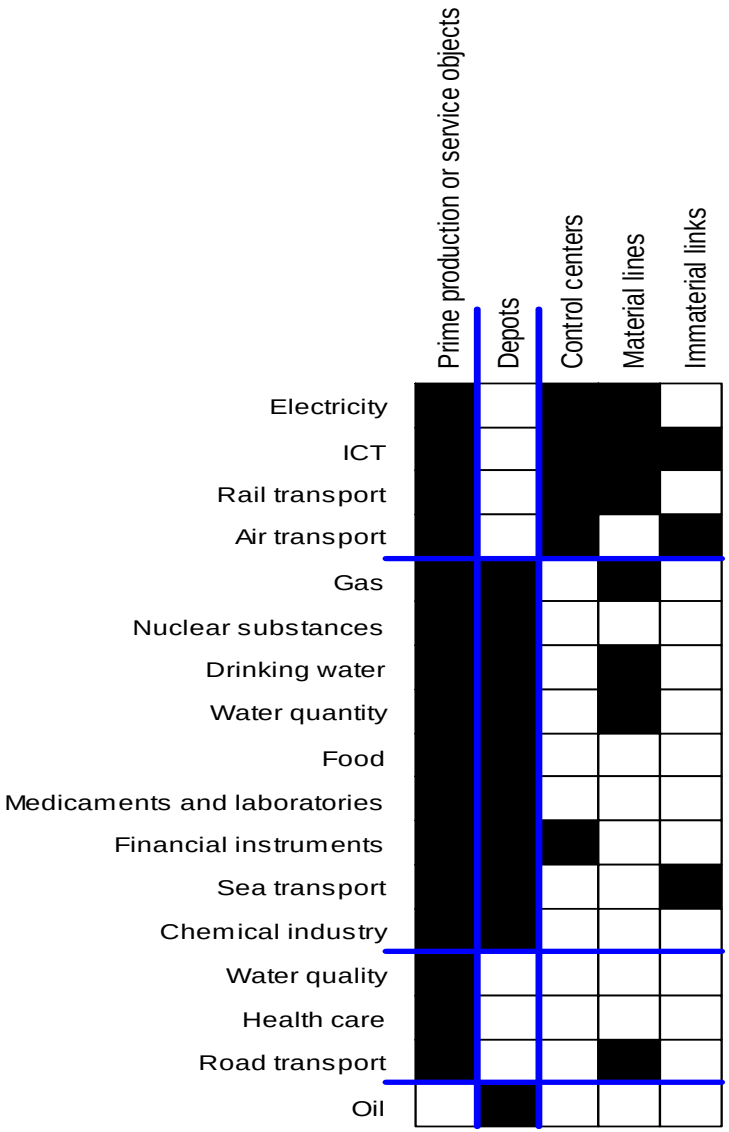
- Workshops led to identification of hundreds of critical objects that can be put in the following categories:
  - critical objects,
  - critical links (link as a critical object)
  - critical crossings of the same or different infrastructures, and

- ICT as critical element of the most subsectors

- Need to supplement the material concept of critical objects with non-material objects: air corridors, maritime corridors, wireless connections (ICT)

- Asymmetric disposition in the country - Areas of condensation: In principle higher condensation in urban areas
- Area of Ljubljana the most critical + MULTICRITICAL areas

Matrix of critical facilities



Cross-border effects in case of sectoral malfunction

- Most infrastructures is embeded in European infrastructures
- Inherently international sectors : less international sectors
- Relevance of border control decreased
- Predominant dependence from international infrastructure
- malfunction of almost all subsectors would have cross-border effects. We classified them as local (neighboring countries), regional (Europe/part of Europe) or global. It appears that malfunctions of most subsectors would predictably cause local or regional cross-border effects. Global effects would expectedly appear in the case of nuclear substances, where even a small failure triggers a formal international response.

Conclusion: Basic policy lessons

- Sector energy and related subsectors are strongly embedded in the network of national and international critical infrastructures. Especially, electricity plays electricity plays a central role in this network of networks. Its malfunction would seriously affect all other infrastructures.
- The sector energy shares many threats and risks with other national critical infrastructures.
- The malfunction of the subsector electricity would create very high social consequences in terms of human, economic and public effects.
- The malfunction of the subsector electricity and to some extent also the subsector gas would instantly create a social crisis.
- Many infrastructural objects related to energy are collocated with other infrastructures, thus, increasing the risk and cross-sectoral transfer of damage from one infrastructure to another.

- shaping CIP policy only in a sectorized manner creates a risk of **addressing complex infrastructural problem too narrowly** and missing the core complexity of critical infrastructures.