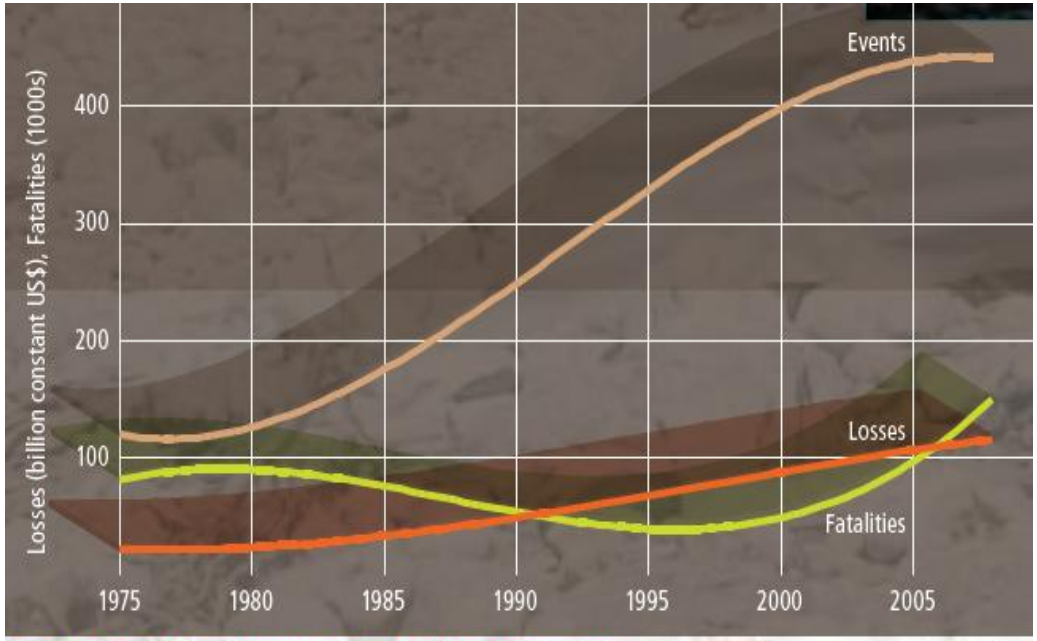
ULKOPOLIITTINEN INSTITUUTTI
UTRIKESPOLITISKA INSTITUTET
THE FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

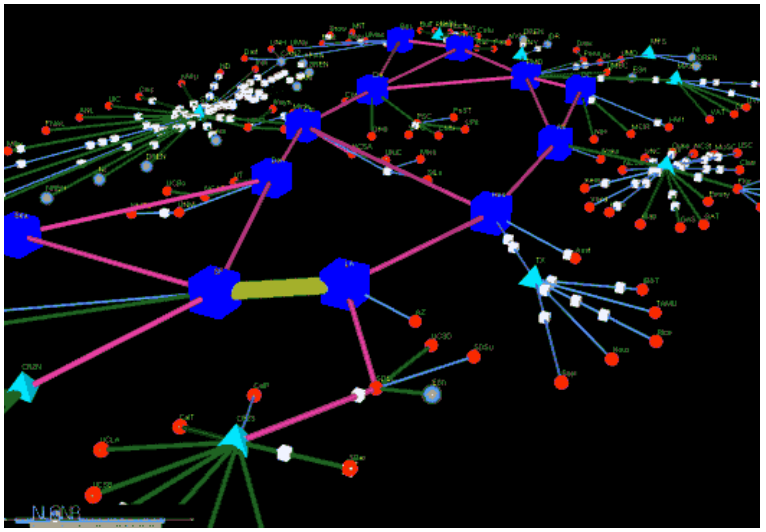
Critical infrastructure protection: an evolution of Russian policy

Katri Pynnöniemi
Phd, Researcher
The Finnish Institute of International Affairs

Globalization up-side-down: interdependency as a source of vulnerability



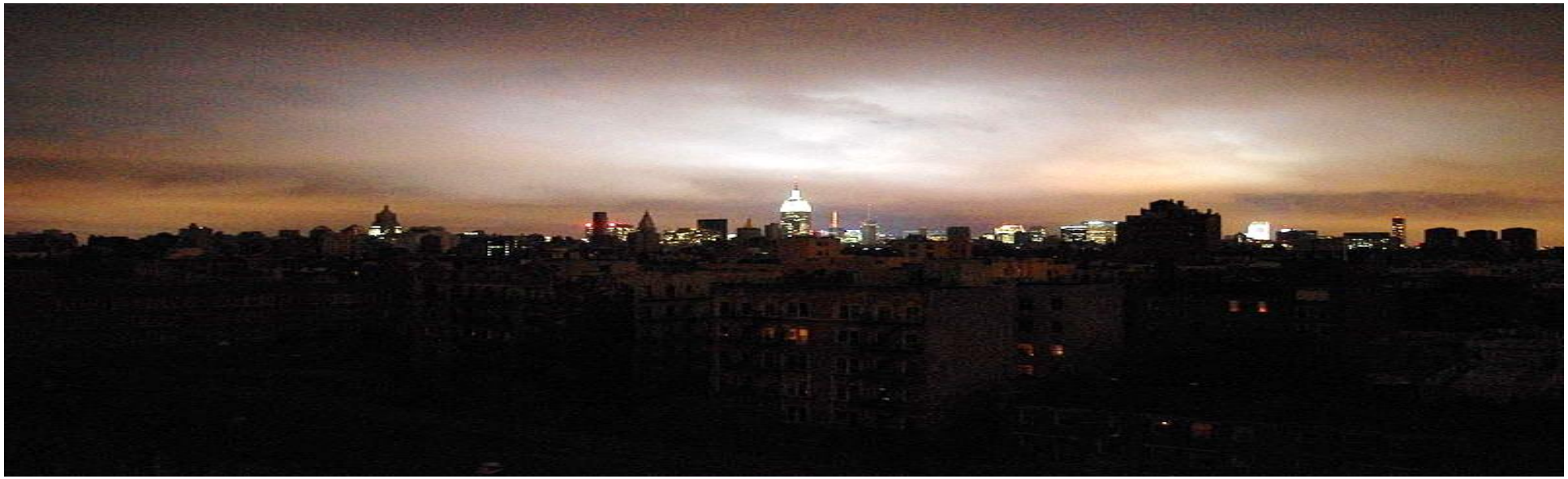
GLOBAL TRENDS IN THE NUMBER OF LARGE DISASTER EVENTS, and associated loss of life and monetary losses
Data source: EM-DAT: International Disaster Database, Centre for Research on the Epidemiology of Disasters Université Catholique de Louvain, Belgium.



"Network Performance Visualization: Insight Through Animation"
by J.A. Brown, McGregor A.J and H-W Braun.

IIASA , *Options,* Summer 2009 ”increasing resilience to extreme events”

Critical infrastructure protection (CIP) against threats to ’our way of life’



- TECHNOLOGICAL HOMOGENEITY: the emergence of interconnected globe and the pervasiveness of information technologies
- MEGA-TRENDS : climate change, cyber war
- ECONOMIC RESTRUCTURING: Private efficiencies vs public vulnerabilities

Russia as a ’society of all-encompassing risk’

- The degeneration of infrastructures critical for the country’s economic and social development
- A hybrid regime more vulnerable than others for CI risks
- Climate change in particular a challenge for Russia

Research on Russian critical infrastructures: three levels

1) The evolution of Russian policy on critical infrastructure protection
2) Threats to critical infrastructure and state responses: the case of the forest fires 2010
3) Re-reading critical infrastructures: a view from the indigenous communities of the Russian Arctic

NOTE: Purpose is not to model risks or provide overall assesment of CI risks in Russia

The problem of CI in Russia: an overview

Strategic objects (state prestige)

Dangerous objects (population & territory)

'space of flows' (economy)

Photo by Katri Pynnöniemi

Critical asset: knowledge

Known knowns - known unknowns - unknown unknowns

Definition of 'critical infrastructures' reflects threat perceptions, values and traditions of the given community

Maturing of CIP policy in Russia

1990s'

- Focus on 'population and territory'
- Threat perception: natural emergency or technological accident, ecological security

2003 - mid-2000

- Monitoring of 'critically important objects', sectoral approach
- Threat perception: terrorism, (de-modernization)

2009 - present day

- CIP as a part of national security strategy (2009)
- Threat perception: terrorism, climate change, cyber attacks

Photos from Getty Images, Wikimedia commons, yandex

The main vulnerabilities and dangers

- Increasing danger and intensity of technology generated and naturally occurring emergencies,
- increasing number of potentially dangerous objects, many of which are located in big cities and densely populated areas,
- physical depletion and technological backwardness of systems and complexes designed to improve safety of dangerous objects,
- low level of education and training of the personnel, weak technological discipline, low level of safety culture,
- inadequate level of financing of measures aimed at improving safety of population and management of the dangerous objects
- increasing danger of international and internal terrorism, increasing level of criminality and narcotic business in the society.

Concept paper for CIP policy, 2006

Conclusions

- The conceptualization of CI in Russia has evolved along lines similar to those adopted in the US and the EU
- Focus on ‘critical infrastructures’ from mid-2000’s, key threat perception terrorism -> cyber
- The governance: monitoring and risk assessment emphasized, administrative structures blurred
- WHAT NEXT? Analysis of discursive levels of CIP