Policy brief

Managing and reducing social vulnerabilities from coupled critical infrastructures

international risk governance council

Further information

concerning this policy brief, please contact IRGC
email: info@irgc.org
tel: +41 22 795 17 30
or see www.irgc.org

IRGC's White Paper, Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures, can be downloaded from the Downloads & Links section of IRGC's website.

© International Risk Governance Council, Geneva, 2007

Introduction

The International Risk Governance Council (IRGC) is an independent foundation based in Switzerland whose purpose is to help the understanding and management of important, emerging global risks. It does so by identifying and drawing on the best scientific knowledge and, by combining it with the understanding of experts in the public and private sectors, developing fact-based risk governance recommendations for policy makers.

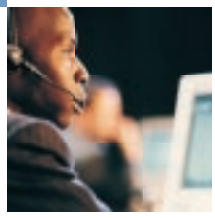
The establishment of IRGC was the direct result of widespread concern within the public sector, the corporate world, academia, the media and society at large that the complexity and interdependence of an increasingly large number of such risks was making the development and implementation of adequate risk governance strategies ever more difficult.

The aim of this report is to suggest ways to improve the risk governance of critical infrastructures

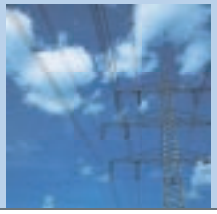
The risks associated with, and the vulnerabilities of, critical infrastructures have been a priority for IRGC since our founding. Our attention was drawn to them not only by the complexity of the infrastructures themselves, but also by the criticality of the services they provide, the increasing interdependence between them and by their being subject to fundamental changes in technology and in ownership and market structures. This report is the final product of a year-long project led by Professor Wolfgang Kröger, IRGC's Founding Rector and Director of the Laboratory for Safety Analysis at the Swiss Federal Institute for Technology, Zurich (ETH Zurich). The conclusions of this project, comprehensively detailed in a White Paper[1] prepared and reviewed by a team of scientific and technical experts and published in autumn 2006, led to the development of the risk governance options outlined in this report.

The aim of this report is to provide information to senior decision-makers, raise awareness of important big-picture issues, and suggest ways to improve the risk governance of critical infrastructures. The report is divided into the following sections:

- The five infrastructures under discussion
- Vulnerabilities of individual infrastructures
- Inter-dependence of different infrastructures
- Strategy for risk governance
- Technical options for better management
- Policy options
- Issues requiring further investigation



[1] IRGC White Paper No3, "Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures", IRGC, Geneva 2006 (available as a download from www.irgc.org)



Summary

Critical infrastructures provide many basic services without which society cannot function normally. This paper looks at how vulnerable society is to failures in five linked infrastructures that are indispensable in Western societies: electricity, gas, water, rail and communications. Each of these infrastructures has basic weaknesses, such as over-complexity and traded-off security factors, and faces multiple threats, including exposure to natural hazards and malicious attacks.

The vulnerability of all of these infrastructures is increased by their mutual interdependence. The electricity and communication networks are particularly vital for the smooth functioning of other infrastructures. In addition, intra-dependence means that the failure of one section of a network can have negative impacts on other parts: this is a major risk in electricity, rail and communications.

Successful management of critical infrastructures depends on assessing their criticality, in terms of the scale of the effect a failure would have on society, and the adequacy of the current risk governance arrangements. In particular, the electricity and communications networks require urgent action to reduce the potential effect of a failure or malicious attack and to establish a suitable framework for risk governance.

Potential actions to lessen the risk and effects of failure include adding spare capacity, ensuring that network expansion takes place in a coherent fashion, and installing back-up systems, and ensuring the adequacy and thoroughness of the risk assessment which support the necessary decisions.

Policy makers must play a large part in the changes needed to protect society. Our major recommendations for policy makers include prioritising the security of electricity supply a central principle, and mandating that the current public internet is not used to control critical systems. A number of key decisions need to be made with the full co-operation of stakeholders, including system operators and the general public.

A number of key decisions need to be made with the full co-operation of stakeholders, including system operators and the general public

Five infrastructures, with marked similarities, are considered

Infrastructures become critical when they provide some service without which society or the economy cannot engage in normal operations. This report focuses on five infrastructures which are essential for industrialised countries, in particular:

- The electricity supply system, including generators
- Gas supply
- Rail transport
- Information and communication (ICT)
- Urban water supply and waste water disposal

Each of these infrastructures relies on complex physical networks, involves a combination of private and public entities, and is regulated to some degree. In addition, they are all subject to multiple and inter-linked risk-shaping factors that affect their operation (see Figure 1).

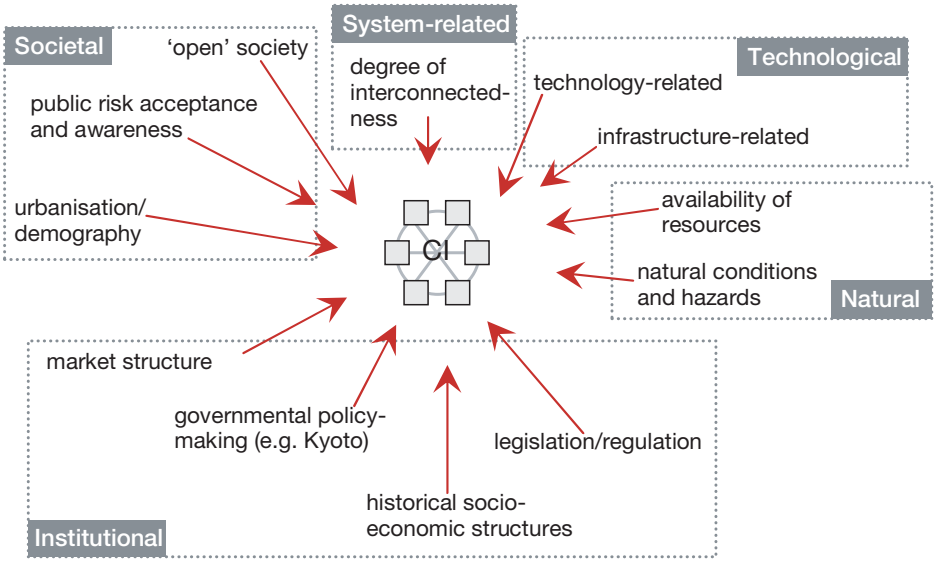


Figure 1

Factors shaping the risks facing critical infrastructures

Each infrastructure has unique vulnerabilities

Each of these infrastructures has weak points that are unique to the system and independent of other infrastructures. A sample of these weaknesses includes:

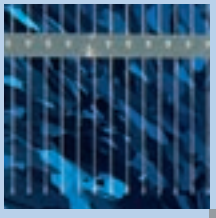
Electricity

Besides its positive effects, market liberalisation has led to major vulnerabilities in the power infrastructure

- Besides its positive effects, market liberalisation has led to major vulnerabilities in the power infrastructure. The opening of the market has resulted in the network becoming more integrated and complex, in it being used in ways for which it was not originally designed, and in a general lack of investment, particularly in new transmission facilities. As a result, the electric power system is being operated much closer to its limits and cascading outages, with potentially enormous costs, are more likely[2].
- The exchange of information between transmission system operators (TSOs) is inadequate. Within the European Union, the responsibility for ensuring a secure supply lies with the TSOs but the operators often lack the real-time data they need. This problem has been aggravated in part by the growing complexity of the network.
- Many power grids are governed by the N-1 security criterion which states that if one linkage goes down, the rest of the system will not suffer a failure from power overload. However, inaccurate applications of the N-1 criterion have led to blackouts, and the criterion does not deal with the possibility of multiple failures[3].

[2] The cost of the 2003 blackout in the Northeastern US and Canada has been estimated at US$2-10 billion.

[3] Some critics claim that the N-1 criterion should be revisited altogether, with account taken of the potential trade-off between security and cost.



Gas supply

- Gas currently constitutes approximately a quarter of Europe's primary energy consumption and dependence for imports on gas-producing countries is increasing. This may result in shortages for technological, geological or political reasons. Normal consumption may be affected because storage is limited and it is difficult to transfer supplies in unforeseen directions, such as North-South and vice-versa.
- Gas storage and transport systems (including tanks, pipelines and compressor stations, ships and terminals) are vulnerable to terrorist and, in parts, to cyber attack.
- Gas pipelines are subject to interruptions by, for example, construction work. Natural events (e.g. hurricanes, landslides, earthquakes) may destroy large parts of the system.

Rail transport

- The rail network is an open-access network that passes through crowded and sensitive areas such as stations and hazardous facilities; the system also features many bottlenecks. Both factors make it vulnerable to extreme natural or other events and a highly attractive target for terrorist attacks.
- The network is intra-dependent to a high degree, and an interruption of services in one area may lead to a loss of services in another.

ICT

- ICT services can be disrupted e.g. by attacking the actual infrastructure of the internet. This includes attacks on routers, operating systems, and applications, which are all uniform. The root name servers, which support the domain name system, are another target for attack.
- In addition, ICT can be disrupted by using the internet as a platform or vector for attacks. This includes denial-of-service attacks, 'phishing', and the spreading of viruses.

The rail network is vulnerable to extreme natural or other events

Urban water

- Almost all urban water systems are subsidised, and utilities are dependent on political decisions regarding water-related expenditures. These decisions frequently result in price increases that are below the amount needed to cover infrastructure maintenance and upgrades. The result of this is that leakages have become a major problem and threaten to endanger supplies.
- Water supplies can be contaminated through malicious or non-malicious acts. Potential malicious acts include contaminating the supply in the distribution system, in particular reservoirs – the system's open and mostly unmonitored end. Non-malicious acts include sewage treatment overflows in heavy rain and accidents in the transport of dangerous products. Since much contamination cannot be detected visually, people tend to feel very vulnerable to such threats.
- Pumping stations and treatment plants can be put out of action through human or non-human means. Natural hazards, industrial accidents and fires can all prevent water from being distributed or treated in its usual fashion.

Since much contamination cannot be detected visually, people tend to feel very vulnerable to such threats

The vulnerabilities of infrastructures are increased by the couplings between them

In addition to these independent weak points, the vulnerability of the infrastructures is increased by the couplings between them. Analysing these links shows how failure in one infrastructure can be caused by the failure of another infrastructure on which it relies. A sample of some of these dependencies includes:

Electricity

- The electric power network relies on the gas supply system, which provides fuel for generators; on the rail network, which transports other fuels such as coal; and increasingly on ICT systems[4], which control and manage electricity systems and markets. There is less dependence on urban water systems, since cooling water for power plants is typically drawn from different sources.

Gas supply

- The gas supply system relies on the ICT infrastructure for controlling the gas system and managing markets (and tends to do so using inherently insecure systems) and on the electricity network for powering pumps.[5]

[4] In the past, many infrastructure operators deployed dedicated technology and their own dedicated networks. In the meantime there is a tendency to change to commercial ware and open networks causing new vulnerabilities.

[5] External power is typically used in addition to the power from the gas plants themselves.

Rail transport

- The rail network relies on electricity from the general grid, and ICT systems for communication and control.

ICT

- ICT systems rely on electricity and to a certain degree on the rail infrastructure, since many communication lines follow train routes and could be disrupted in a rail accident or attack.

Urban water

- The urban water system relies on the electricity network for treating and pumping water; on ICT for operating and controlling systems; and on rail transport for delivering important supplies (e.g. disinfectants).

Figure 2 categorises how dependent each infrastructure is on the others, how dependent the others are on it, and also how strong the intra-infrastructure dependencies are (i.e. how reliant the infrastructure as a whole is on all parts functioning correctly):

Figure 2

Dependencies of critical infrastructures

	Electricity	Gas	Railways	ICT	Urban water
Dependence on other infrastructures					
Dependence for other infrastructures					
Intra-infrastructures dependence					

Major dependency

Moderate dependency

Minor dependency

Increasing dependency

The strategy for managing these infrastructures depends on their criticality and the adequacy of the current risk governance arrangements

The first step in managing the vulnerabilities of infrastructures is to assess the *overall criticality* of each infrastructure. Criticality can be measured in terms of three variables that cover the effects of failures of the infrastructure:

- *scope*, the geographical extent of the effect of a failure
- *magnitude*, the size of the effect in the afflicted area
- *time effect*, the speed with which a failure has an effect.

When the criticality of each infrastructure is understood, the adequacy of the current risk governance arrangements can be measured

These variables, for each of the five infrastructures, can be characterised as follows:

Electricity power network

- *Scope*: potentially international
- *Magnitude*: high
- *Time effect*: immediate

Gas supply system

- *Scope*: moderate
- *Magnitude*: high on local level, much lower on international level
- *Time effect*: low (owing to availability of storage facilities)

Rail transport

- *Scope*: moderate
- *Magnitude*: moderate
- *Time effect*: moderate

ICT

- *Scope*: high
- *Magnitude*: high
- *Time effect*: moderate (failure need not have immediate effect)

Urban water

- *Scope*: low (limited impact on other infrastructures)
- *Magnitude*: **low (limited impact on other infrastructures)**
- *Time effect*: moderate

When the criticality of each infrastructure is understood, the adequacy of the current risk governance arrangements can be measured. For this paper, risk governance arrangements have been measured in terms of:

- *awareness*, how aware stakeholders are of the risks
- *goal setting*, the adequacy of current goals for managing risk
- *process/means*, the suitability of the methods for managing risk.

All infrastructures suffer from inadequacies of risk governance, which vary from the moderate, in the case of urban water and rail transport, to the major, in the case of electricity and ICT.

The two factors of *criticality* and *inadequacy* of *risk governance* form a matrix that shows how urgently action is required (Figure 3):

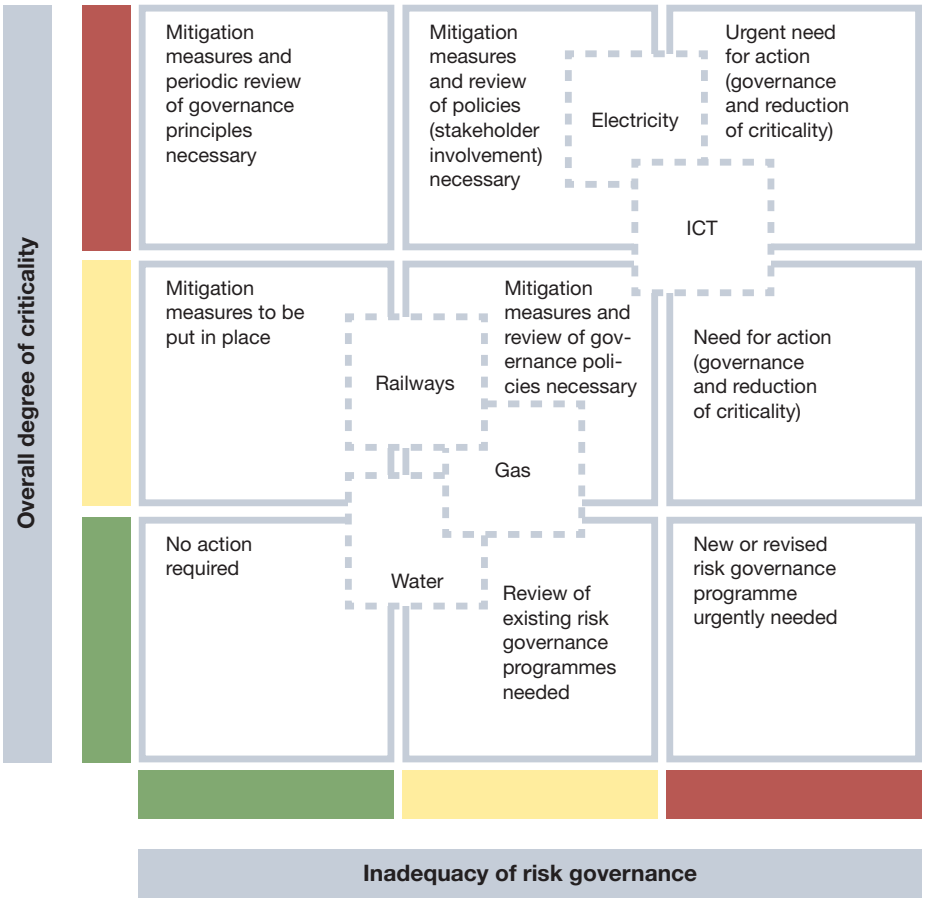


Figure 3

Criticality and risk governance matrix

Strategies for managing the infrastructures should be driven by the position of each risk on the matrix.

What are the technical options for better management?

Risk governance of infrastructures can be improved by various technical, management and organisational strategies that guard against the effect of an infrastructure failure. Strategies fall into two types: those that minimise the risk of infrastructure failure, and those that minimise the negative effects of a failure.

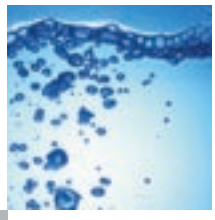
Strategies that can minimise the risk of infrastructure failure, together with their potential drawbacks, include:

- Adding independent, redundant or spatially separated capacity to systems; this reduces the risk of multiple 'common-cause' failures. However, as the extra capacity increases the complexity of a system, the system's performance becomes harder to predict.
- Ensuring that systems expand in coherent ways. A number of infrastructures suffer from the fact that they have grown in an unplanned fashion, sometimes without basic changes in operation and control. However, the desirability of systematic planning needs to be reconciled with the objectives of market competition and privatisation.
- New technology, such as SCADA[6] systems that monitor the transport of essential goods such as water and electricity, can play a role in relieving technical or institutional constraints. However, this may also introduce new vulnerabilities, e.g. cyber attack if insecure systems are used.

Strategies fall into two types: those that minimise the risk of infrastructure failure, and those that minimise the negative effects of a failure

Strategies that minimise the negative effects of failure include:

- Designing systems so that capabilities are degraded in a 'graceful' fashion. In ICT, for example, this may include reducing bandwidth and giving priority to certain traffic.
- Incorporating rapid-acting, distributed and autonomous computer control agents into systems.
- Undertaking careful contingency preparation, including the provision of real time information to operators and training operators in realistic simulations.
- Installing back-up systems so that the failure of one infrastructure does not lead to the failure of others. For example, a gas turbine peaking plant[7] can be installed near large pumps for water and sewer systems so that, even if the electricity supply fails, water and sewer services can be maintained.



[6] Supervisory control and data acquisition.

[7] A plant that only provides power in times of high demand.

What are the policy options?

Governmental policy can improve the risk governance of these infrastructures.

Because the management of almost all critical infrastructures requires trade-offs between various private and public objectives (i.e. balancing conflicting social needs), policy should be set with the cooperation of all parties responsible for risk management, which include system owners and operators as well as governmental departments, agencies and regulators. In addition, members of the public and NGOs have a strong interest in observing the risk governance process and participating in decision-making not least because, in any trade-off between system reliability and service price, consumers will be the group most directly affected by the decision.

In any trade-off between system reliability and service price, consumers will be the group most directly affected by the decision

We have both general and specific recommendations for policy options that will promote the adoption of desirable risk governance strategies. General recommendations include:

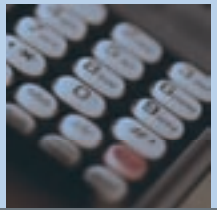
- A legal mandate for specific system structures and capabilities, and independent monitoring of compliance with these requirements
- Provision of institutions, involving all relevant players, to supervise infrastructures (while avoiding over-regulation)
- Encouragement of methods that can lead to the growth of effective standards without the need for regulation, such as certification and insurance
- Mandating of levels of investment in R&D that will help infrastructure providers address issues of security and reliability[8]

Specific recommendations for each infrastructure include:

Electricity power network

- Security of continuous supply should be addressed more explicitly and become a new overarching principle. Strategies to ensure an appropriate level of protection and resilience need to be promoted.
- Top-down political decision and rule-making processes should be revisited to include both an appropriate level of technical analysis and dialogue with stakeholders. Different governance approaches are needed that not only embrace all major players (including end-user groups) but also address key challenges (such as structuring tariffs so as to ensure adequate investment levels and establishing financial risk transfer mechanisms).

[8] For example, in electric power R&D investments are less than 0.5% of sales, which is much too low to meet societal needs.



Gas supply system

- There is a need to set up and make available an easy-to-use information system covering the location of gas pipelines, mainly to be used by civil engineering workers and emergency forces.

Rail transport

- Upgrading and revision of intergovernmental standards is needed on security, quality insurance, education, training, etc., in order to cope with the more challenging use of the railway system (higher density of timetables, tighter safety margins) and new threats (trans-border transport of dangerous goods and devices).
- More effective technical, organisational and socio-political measures against malicious attacks should be carefully considered and balanced against social values such as privacy, open society and comfort.

The public internet should not be used for any function which is vital to the supervision, operation, or control of any critical infrastructure

ICT

- System owners, operators and users should strive for, and share the implementation of, the organisational and technological measures needed to reduce the internet's vulnerabilities.
- The current public internet is not secure. Until efforts to develop much more secure internets in the future are successful, the public internet should not be used for any function which is vital to the supervision, operation, or control of any critical infrastructure. Instead, dedicated communication systems should be employed that involve no logical link to publicly accessible computer systems and networks.

Urban water

- Proceeding from studies determining their effectiveness, systems and measures should be considered to improve the monitoring of water and sewage systems.
- Restricting human access to critical water system components, including water works and better protecting/monitoring the open-access elements of distribution systems.
- In particular, dams should be adequately protected against terrorist attacks.

Issues requiring further investigation

This report takes a high-level view of a limited number of critical infrastructures from a Western perspective. Additional work needs to be done that, inter alia, examines:

- Other critical infrastructures, such as air transport and provision of health care
- Critical infrastructures from the perspective of non-Western or industrialising countries
- Ways of reducing social vulnerabilities by maintaining services when critical infrastructures fail
- The long-term, rather than short-term, impact of critical infrastructure disruptions.

international risk governance council

Chemin de Balexert 9
1219 Châtelaine
Geneva ▪ Switzerland

tel +41 (0)22 795 17 30
fax +41 (0)22 795 17 39

info@irgc.org
www.irgc.org