

The International Risk Governance Council's risk governance framework and its application to natural disaster risk planning

Convenor: Christopher Bunting, International Risk Governance Council, Geneva

Session Summary Report

This well-attended session on the second day of the conference was an opportunity for the IRGC to present its risk governance framework, elaborated in the 2005 white paper on 'Risk Governance', and facilitate discussion about its usefulness within natural disaster risk planning. This report contains an overview of the meeting and the critical issues discussed, followed by a summary of each individual presentation.

The session opened with a presentation by Norio Okada ([below](#)) about a retrospective test of the framework using the Nagara River Estuary Barrage Conflict as a case study. The presentation began by situating the conflict historically and socially and describing how public perception had changed from one of acceptance to opposition. This change was a consequence of changing social and structural dynamics, in particular with regard to environmental sustainability. The case study concluded that: pre-assessment could help to understand the path of the conflict, leading to a much faster resolution; an appropriate risk appraisal could have helped government and citizens reach a better understanding of each other before the plan was decided and put into practice; and participatory discourse is a vital part of conflict resolution, although in this case the antipathy of the opposing group may have reduced the potential for an agreeable trade-off to be reached.

The second speaker was Ortwin Renn ([below](#)) who presented the IRGC framework to the assembled participants. Prof. Renn described the framework as addressing the two key problems of risk governance models: first, the challenges of complexity, uncertainty and ambiguity in knowledge, interests and values; and second, the need for a model to be applicable to multiple risk scenarios. The core components of the risk governance process were described as pre-assessment (framing of the problem and identification of different perspectives), risk appraisal (risk assessment and concern assessment), tolerability and acceptability judgement, risk management (dependent on the level of knowledge and stakeholder involvement) and communication. Prof. Renn concluded with an overview of the framework's test applications, which will be published early in 2007, and an analysis of the refinement that the framework still needs to undergo.

The third speaker of the session was Jeff McNeely ([below](#)) who used the loss of ecosystem services as a case study with which to test the IRGC framework. Dr. McNeely began by describing the Millennium Ecosystem Assessment (MEA) and in particular the MEA model which expresses how human welfare is directly linked to ecosystem services and biodiversity. The case study used the example of medicinal species to conclude that: in pre-assessment and risk appraisal, ecosystem services can be framed as important components of human welfare (e.g. as sources of medicines and therapies), tolerability of risk can be judged by considering whether or not services could be synthesised; and risk management options could include processes such as monitoring of the status and trends of medicinal species. Dr. McNeely also agreed that risk communication and stakeholder involvement are essential to the risk governance process, and in particular the inclusion of local peoples as stakeholders.

The final speaker, Wolfgang Kröger ([below](#)), did not address the IRGC framework directly but rather more described an IRGC project on critical infrastructures at risk, including electric power and gas supply and information and communication services. The study identified several factors which have promoted tighter integration, interdependency and hence greater vulnerability in industrialised countries, including changes in the economic, environmental, legal and regulatory settings. Prof. Kröger concluded by recommending that: security of supply should become an overarching political goal and principle; strategies to ensure an appropriate level of protection and resilience need to be promoted; governance approaches should embrace all major players (including end-user groups) and address key challenges (e.g. tariff structures to ensure adequate investments and establish financial risk transfer

mechanisms); and the public Internet should not be used for any function which is vital to the supervision, operation, or control of any critical infrastructure.

Critical issues discussed

Can the framework be assessed using a retrospective approach?

It could be argued that any framework will work when tested retrospectively because actual events can be squeezed to fit an empirical model. In the Nagara Dam example, the main driver in the conflict was a major shift in public perception - even given the important role of concern assessment in the framework - would this model have been able to predict a change of this type? A retrospective analysis can show the different paths and outcomes that could have been taken by decision-makers; however, the true test of a model is when you can use it proactively.

Is the framework sensitive to changes in knowledge, interests and values?

The circumstances under which risk issues develop change over time, so do we need to revisit the framework as the dynamic of preferences change e.g. in political priorities? Furthermore, different preferences can exist at the same time and when undertaking pre-assessment different frames may be equally appropriate e.g. nanotechnology can be framed as the new big risk issue but also as a key area of innovation. Adaptive risk assessment and management processes need to be designed so that there is an appropriate feedback system. This is particularly important in the natural environment as ecosystems are dynamic and are constantly changing so that the rate of change can be rapid e.g. as we are seeing with climate change. Are changes and differences in knowledge, interests and values able to be taken into account? Can the framework be made sensitive to changes in peoples' attitudes?

Does the framework just contain obvious conclusions?

Some of the framework does seem to be obvious but this is necessary or else it would not work. Moreover, some aspects of the framework appear to be obvious but policymakers are not doing them as general practice. In particular, there is a lack of concern analysis being carried out e.g. when the US proposed to have sewage sludge disposed of on farmland there was a technical risk analysis but they didn't take into account the real issue which was resident concern. Resident protests eventually stopped the disposal but only after US\$3 million had been spent on machinery. The aim of developing the framework is to systematise a good risk governance process so that it has a chance of being implemented.

Norio Okada, Kyoto University

A New Perspective and Methodology Adaptively Tested for Integrated Governance of Disaster Risks and Conflicts – A Japanese Case Study

Our research challenge has been to retrospectively test the IRGC risk governance framework using the Nagara River Estuary Barrage Conflict as a case study.

The Nagara River Estuary Barrage Conflict

The Nagara River flows out of the mountains of the Gifu Prefecture in central Japan. For roughly a half of its 136-kilometer course it runs south through narrow valleys. Then, flowing through high dykes, it makes its way across the Nobi Plain before emptying into Ise Bay, and into the Pacific Ocean. The purpose of the barrage is flood control (Nagaragawa Estuary Barrage, which prevents the inflow of saltwater, enables us to implement large-scale dredging and realise the safe water flow of Nagara River in case of flooding) and water supply (the barrage prevents upstream intrusion of saltwater, thereby making it possible to provide fresh water for domestic purposes and industrial water supplies for Aichi Prefecture, Mie Prefecture and Nagoya City).

Originally the barrage had been approved by the local community and construction had begun in 1988. However, at the beginning of the 1990s the situation started to change due to: a long time lag between inception and completion of the project; a drop in industrial water demand (heavy industries were recycling water in the plants and Japanese industry changed from materials-based (iron and chemical) to manufacturing-based (automobiles and electric

equipment)); the economy became increasingly focused on sustainability rather than economic growth; and nature preservation was subject to increasing public awareness.

These changing social and structural dynamics, alongside the loss of some rare fish in the estuary, increased the level of opposition from both local fishermen and environmentalists. Crucial conflicts occurred among government officials, internal and external societal groups with diverse values, and non-unified social movement groups. The National Ministry of Construction was unexpectedly challenged by this public opposition.

Application of the IRGC framework

Based on the IRGC framework let us assume that we can anticipate what happened (Retrospective What-If analysis).

- *Pre-assessment.* Had they conducted pre-assessment would they have anticipated the publics' preference change for the environment? Probably no, nobody would be able to anticipate such a crucial preference change in the future. But, provided with tools such as problem framing, early warning, screening and determination of scientific conventions, citizens could have benefited from better access to information and we could have avoided the then still "conflict in embryo" caused by mutual distrust and suspicions. Pre-assessment could therefore change the quality of the path of conflict leading to much faster resolutions.
- *Risk appraisal.* Concern assessment, undertaken with citizen participation, could have made the situation better. Both government and citizens could have reached a better understanding of each other before the plan was decided and put into practice. Furthermore, risk assessment, by way of hazard identification, exposure and vulnerability assessment and risk estimation, might have activated more pro- and con- debates. However, the value split would still have been wide and not easy to overcome.
- *Risk characterisation and management.*
 - The conflict can be described as "complex" but there was not necessarily an ambiguous value split. The opposing group was found to be constantly antagonistic to the project, and thus there was not much room for participatory discourse.
 - The type of conflict was cognitive, evaluative and normative, but it was not an ambiguity-induced risk problem.
 - Definitely, public participation is needed even for this type of conflict situation. Some indirect democracy (like public voting?) which links to tolerability and accessibility judgment.

What makes disaster governance risks and conflicts special? As a general agenda nobody disagrees, although as an individual you may disagree and may or may not take any action. There tends to be a lot of internal conflicts about issue prioritisation with a focus on risk awareness and preparedness.

Key messages

- It is useful to review and formalise lessons learnt from what has already occurred. Social conflict should be viewed as a part of disaster management.
- How to implement the framework as a proactive scheme may need further study (such as how to apply it to preliminary or ongoing conflicts of similar structures).
- There are two purposes which this framework may serve: as a top-down approach for institutional design of risk/conflict governance schemes; and as a bottom-up approach for adaptive management of multi-stakeholder-involved regional risks/conflicts (e.g. as part of community action).
- There is room for more defined applications and guidelines. Risk characterisation may need more multi-dimensional considerations for critical conflicts which tend to entail multi-stakeholder involvement. Communication is often difficult among stakeholders with very different standpoints and backgrounds - even if they use the same words, they mean different things.

- Taxonomy helps but in actuality internal observation and knowledge development have vital limitations. We need additional external knowledge that tells us about the current status of the positioning in the framework (e.g. the idea of a risk management escalator is helpful but those who promote the projects are not sure they are really placed in the correct step of the escalator).
- Finally, the framework will evolve dynamically over time and thus the communication platform should not be closed.

Ortwin Renn, University of Stuttgart

Risk Governance: Towards an Integrative Framework

The IRGC framework contributes two significant innovations to the field of risk governance. First, it allows us to address the three challenges of risk management: complexity, uncertainty and ambiguity, and second, it helps us to assess and manage all different sorts of risk, such as technological risk and natural hazards, within one flexible framework.

The three challenges of risk management

The first of these challenges is the complexity involved in assessing causal and temporal relationships. For example, if you consider the causes of cancer you will need to model through a whole set of layers before you begin to arrive at a plausible answer. The second challenge is uncertainty which involves the consideration of issues such as: variation among individual targets e.g. the likelihood of different members of the community developing an illness; measurement and inferential errors; genuinely stochastic (random) relationships; and, system boundaries and ignorance e.g. who is the target of our management efforts - is it the individual, the household or the community? The third challenge, ambiguity in interpreting results, is very different as we are asking what the situation means to and how it is interpreted by different individuals. There are two elements to ambiguity: interpretative ambiguity (what does it mean e.g. is it an act of god?); and normative ambiguity (is it tolerable?).

The management of different types of risk

What kind of hazards can the framework be applied to? The aim of the IRGC white paper on 'Risk Governance' was to find a consistent and overarching framework flexible enough to cover all of these hazards. We can classify hazards by their different agents (causes) such as: physical agents (e.g. noise), chemical agents (e.g. environmental pollutants), biological agents (e.g. viruses), natural forces (e.g. avalanche), social-communicative hazards (e.g. terrorism and sabotage) and complex hazards combinations (e.g. technologies).

Furthermore, the framework needs to be adaptable to the new challenges in handling these risks, such as: plural values and knowledge claims, expert dissent on risk and benefits, the trans-boundary nature of risks, social amplification and attenuation via perception and social mobilisation, pressure from the global economy, lack of organisational capacity in many countries and the lack of effective governance structures. Additionally, there is an emergence of systemic risk that crosses national and sectoral boundaries (ripple effects) resulting in the need for integration of both risk and sustainability policies.

The core risk governance process

The core risk governance process of the framework consists of pre-assessment, risk appraisal, tolerability and acceptability judgement, risk management and communication.

The key components of *pre-assessment* are: problem framing, early warning, screening (risk assessment and concern assessment policy) and scientific conventions for risk assessment and concern assessment. Two important elements of pre-assessment are the framing of the problem and the identification of different perspectives in how the issue is being conceptualised. For example, if we look at the many countries in the world there will be many differences in how a hazard is conceptualised. In the former Soviet Union there was a deeply held mistrust in the use of external agencies to assess and manage natural hazards, this impacted on their risk assessment and management procedures and, as a consequence, led to the internalisation of risk governance.

For *risk appraisal* we make a clear distinction between knowledge, interests and values by separating risk appraisal into risk assessment (hazard identification and estimation, exposure assessment and risk estimation) and concern assessment (socio-economic impacts, economic benefits and public concerns (stakeholders and individuals)). Some critics believe that this is a completely artificial distinction, however if we do not make this distinction interests and values can creep into the knowledge sector. For example, in the BSE crisis political interests became merged with scientific knowledge until the two became indistinguishable.

As a consequence of the results of pre-assessment, risk appraisal and a tolerability and acceptability judgement there will be a need for different *risk management strategies*. Different strategies will depend on whether we are dealing with routine, mundane risks, complex and sophisticated risks (high degree of modelling necessary), highly uncertain risks (high degree of second order uncertainty), highly controversial risks (high degree of ambiguity) or imminent dangers or crisis (need for fast responses).

We have a whole mix of things which would be classed as complex, uncertain and ambiguous and which require different types of risk management. Using the level of knowledge available to assess a risk also allows us to bring together different risks which may not initially appear to have much in common. For example, complexity-induced risks include: industrial plants containing hazardous material, large dams, bridges and highways, LNG Terminals, weapon complexes, dense settlements, classic infectious diseases and deterministic health risks (threshold). Uncertainty-induced risk problems include: "green" biotechnology, internet sabotage, new epidemics (new mutations), BSE, endocrine disruptors and extreme weather events due to global climate change. Ambiguity-induced risk problems include: "red" biotechnology and genetic engineering, "industrial" food production, biochips for human implementation, electromagnetic fields, globalization of consumer technologies and geo-engineering projects.

As well as the level of knowledge, a second important element of risk management is who will be involved in deciding the appropriate strategies and how these will be undertaken. Very often it is politically correct to say that we need to involve all stakeholders for all risks, however in this manner it becomes impossible to reach any type of recommendation and decision. There is a dilemma here as the more differences in opinion offered the more knowledge is learnt but also the more difficult it becomes to find a solution. The IRGC framework can help in differentiating between circumstances to see what is truly required. The risk management escalator allows us to determine both the type of discourse needed and which stakeholders should participate. For example, time is a scarce resource and participants need to want to be involved in participation. In Germany NGOs often do not attend meetings to discuss simple risk problems, not because they are not interested, but because they do not have the time to be involved. At the other end of the scale, the more controversy there is about an issue the more public participation is needed.

The IRGC framework suggests that four risk management regimes should be used:

- *simple risk management*: standard risk assessments
- *risk-informed management*: expanded risk assessments; seeking expert consensus and epistemological clarification
- *precaution-/resilience-based management*: negotiated safety level under uncertainty; seeking stakeholder consensus and relying on containment and resilience
- *discourse-based management*: value-based orientation; seeking more public input and stakeholder involvement for interpretative variability and normative controversy

Overview of test applications

The IRGC framework is undergoing external test applications that will be published in an 'edited volume' on risk governance early in 2007. The cases studies that have been undertaken are:

- Listeria in raw milk soft cheese, Ewen Todd et al, Michigan University, USA
- Genetically modified crops, Joyce Tait, Director of INNOGEN, University of Edinburgh

- Nagara River Estuary conflict, Norio Okada et al, Disaster Prevention Research Institute, University of Kyoto, Japan
- Nature-based tourism, Jeff McNeely, Chief Scientist, World Conservation Union, and Caroline Kuenzi, IRGC
- Acrylamide in food, Dr. Bonneck, University of Cologne
- Energy security for the Baltic region, Warner North, Northworks Inc and Stanford University
- Nanotechnology, Alexander Jäger and Ortwin Renn, University of Stuttgart and DIALOGIK gGmbH

Refinement of the framework

We already know that the framework needs refinement. Some critical issues that have been raised are:

- The framework is based on a rationalist (western approach). *It is true that the people who have worked on the framework do come from a western background; however people from other cultures have observed that the framework is a logical, rather than a fixed process, and therefore is also applicable to their needs, albeit requiring expression in different ways.*
- The framework misses the point as the real problem is distribution of power. *This may be true; however there is not much that risk managers can do to change the current power systems. We therefore need to work to improve the system we have.*
- The framework lacks dynamics and iteration. *The framework is a circular rather than a linear process but there are no feedback loops within the framework. Maybe we need to make it clearer that at the end of each stage we need to assess what has happened and revisit the previous stages.*
- It is an abstract model without clear practical applications. *The reason for the case studies is to see if the model can work or if indeed each application has its own realm of parameters.*
- There are too many boxes and not enough flexibility. *This is true but it is a personal bias that I feel helps to organise the framework and put some order to it.*
- This model demands too many institutional changes. There are already institutions in place that are unlikely to change. *The model does not ask for wholesale change but it does ask for small changes that can be implemented within the current model. For example, when performing risk assessment consider also how concern assessment will impact on the required strategies. Change is good and we need to strive for this.*

Jeff McNeely, The World Conservation Union (IUCN) *Environmental Risks*

I've tried to really test the framework and push the ideas to the limit. I've been working on conservation for about 30 years, but it is only in the past couple of years that we have developed a new way of linking environmental risks to ecosystem services.

Millennium Ecosystem Assessment

About 1300 scientists have been working on the Millennium Ecosystem Assessment (MEA) over the past 5 years. Synthesis reports have been developed for the private sector and government, amongst other stakeholders. Longer and more in depth Technical Assessment Volumes have also been developed. The total pages of the MEA reports are about two point five times the height of the Eiffel tower; however the whole thing can be captured in the MEA model which expresses how biodiversity supports the ecosystem services which are constituents of well-being for humans. This is a pregnant image as it expresses that there are many elements in the ecosystem which can give birth to others e.g. biodiversity (in genes, populations, species, communities and ecosystems) can give birth to ecosystem services, subdivided into supporting services (e.g. provision of oxygen), provisioning services (e.g. food), regulating services (e.g. protection from landslides) and cultural services where each individual cultures define how they think about ecosystems and the services that are provided where they live. All of these relate to well-being and how we think as human-beings e.g. security, basic materials for good life, health, good social relations and freedoms and choice.

There are five major drivers of change in ecosystems: habitat change, climate change, invasive species, over-exploitation and pollution. All of these drivers are constantly changing and developing themselves and are on the most part increasing. In terms of the impact that these drivers have on ecosystem services, the results of the MEA show that four ecosystem services are being enhanced by these changes, five have mixed consequences and fifteen are being degraded. The bottom line is that 60% of ecosystem services are being degraded.

Application of the IRGC framework

I have applied the IRGC framework to the loss of ecosystem services in order to assess the role of these services in a risk governance context.

- *Pre-assessment.* If you consider ecosystems as critical infrastructures this gives us a totally different way of thinking about the services that they provide. This approach can be readily applied to many ecosystem services. One easy application is to the role of plants and animals in influencing human health as sources of medicines and therapies. For many people most of their medicines come from plants (e.g. aspirin comes from the willow). What happens if we lose these benefits? Ecosystems are also stimulants for new discoveries (e.g. the study of a chimpanzee peeling bark from a tree led to the discovery of a drug for the treatment of malaria). A third service is as models for health research (e.g. polar bears do not lose bone mass while hibernating, however humans do when in a coma and astronauts do when in space. How can we learn from polar bears how to prevent the loss of bone mass? Polar bears are being threatened by climate change so will we lose this potential source of knowledge?). What are the other services that we might lose?
- *Risk appraisal.* What if medicinal species are lost (e.g. medicinal plants like St. John's Wort and Ginkgo)? What if insights into human health are lost (e.g. one type of frog (now extinct) nurtured its eggs in its stomach and gave birth to a baby through its mouth. What happened in the frogs' stomach while this was happening? Could this have provided insights into gastroenteritis)? What if we lose our sentinels of impending disaster (e.g. the Nile virus was initially found in wild and captive birds. Without the ability to investigate this virus in birds would we have found it much more difficult to identify and cure in humans)?
- *Characterisation and evaluation.* Ecosystems are already being overexploited both in harvesting and trade. It is possible that many of the services can be synthesised, but what about those that can't?
- *Possible approaches to risk management.* We should monitor the status and trends of medicinal species, limit the impact of medical research on medicinal species, address medicinal species concerns as part of international agreements, incorporate human health issues in protected area management and limit habitat changes likely to affect human health.
- *Communicating risk to a larger public.* The current material communicating health ignores the value of plants and animals, but this is a risk to human welfare that needs be communicated to the wider public.
- *Stakeholder involvement.* Relevant stakeholders should be involved in discussing risks. Local peoples are often offered compensation for harvesting local resources which they cannot refuse, leading to depletion and overexploitation of the resource. If we involve them more effectively, we will be a lot better off.

This framework can be applied to all of the other ecosystem services as well as those highlighted today so I am intending to apply this approach much more widely. I hope that this will help to bring the conservation community together with the wider community so that we can have a more influential involvement in how to deal with these risks, both for the benefit of ecosystem diversity and human well-being.

Wolfgang Kroger (Co-convenor) ETH Zürich*Coupled critical infrastructures at risk: strategies and policy options to promote protection*

IRGC project focused on the risk governance of five critical infrastructures in industrialised countries (Western Europe, USA), assuming that the basic resources (fuels, water, etc.) for their operation are available:

- electric power and gas supply
- information and communication services – particularly as provided by the Internet as well as ICT used for industrial control
- urban water supply and waste water treatment; and
- rail transport.

All involve distributed complex physical networks, organised along similar value chains with elements embedded within the socio-political-economic framework and subject to similar threats; operating strategies and end-user behaviours are subject to significant contextual changes and (increasing) risk-shaping factors.

Factors which have promoted tighter integration, interdependency and greater vulnerability

- Integration of smaller systems into larger systems (facilitated by modern ICT), thus creating greater complexity and enabling trans-boundary propagation of disturbances
- Changes in the economic, environmental, legal, and regulatory settings in which the systems operate, including pressures which have squeezed out 'slack' or redundancy in systems and thus reduced operating margins
- Use of off-the-shelf technology, including information and control systems, motivated by short-term economic efficiency
- Lack of adequate awareness of vulnerabilities, of the limitations to achievable reliability, or of concern for low probability but high consequence failure modes, etc.
- Lack of adequate penalties or costs to private actors if, and when, system disruptions cause broader societal consequences
- Inadequacy of back-up measures to continue system operation when problems develop.

A few centuries ago the European electricity supply system only connected internal national supply systems whereas now it is connected from Lisbon to Bucharest serving 450 million people about 10% of which involves trans-border exchange. Are these systems at risk? There have been some major blackouts in recent years (e.g. London, August 28, 2003 and Tokyo, August 14, 2006). The costs of these blackouts are very high and the recovery times differ substantially depending on the preparedness of the risk managers and the systems themselves.

Findings

The rank of reliability and security of electricity supply within our society, and the question of what constitutes adequate levels, needs to be addressed from a broad perspective:

- Short and long-term social vulnerabilities and 'willingness to pay' issues, public-private partnerships
- Political issues (reliability goals or targets, set of threats to be taken into account, trans-boundary data exchange, mechanisms to deal with trade-offs, cost assignment, responsibilities, financial risk transfer instruments, e.g. insurance)
- Regulation and standards (investment planning, mandatory operational rules, availability of adequate data on power flows and transmission system components)
- Technical fixes (adding generation and transmission paths, reactive power support, proper maintenance, alignment of protection schemes and settings, closer to real time system monitoring and simulation, improved situational awareness, scenario-based operator training in contingency recognition and response)
- Special issues (improved modelling capabilities, professional accident investigations, refrain from use of Internet (without adequate security), size of the interconnected synchronous grid, integration of dispersed intermittent generators (wind, solar)).

The evaluation of blackouts identifies a common pattern and clearly confirms that the risks involved are systemic in nature:

- Each system has been developed in the past 50 years with a view to assuring mutual assistance. These systems are now operated often beyond the original design parameters, mainly due to market liberalisation
- A minor single event (e.g. tree flashover due to inadequate tree-cutting or line-overload) may snowball into massive problems for a highly burdened electrical power system with long transmission distances
- The malfunction of critical equipment (possibly due to inadequate diagnostic support) and the behaviour of protective devices complicated the management of these events; available system automation turned out to be insufficient
- Most aggravating factors were human-related and contextual, including a general lack of situational awareness of potentially far-reaching failures and short-term emergency preparedness, rather than purely technical
- The impacts on other infrastructures and our societies are significant although in the studied incidents the affected population reacted calmly

These systems are interconnected and this needs to be taken into account when formulating policy options. An important question is to what degree Information and Communication Technology (ICT) is being used to control the other critical infrastructures.

What are the high level recommendations?

- *The Electric Power Supply System*. Directives and goals (e.g. the EU internal market Directives and Regulations), national legal and regulatory institutions as well as provisions are still all market-focused. Reliability criteria are often traded-off against other factors in liberalised markets. Therefore:
 - 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 an appropriate level of technical analysis and dialogue with stakeholders. Governance approaches are needed, that not only embrace all major players (including end-user groups) but also address key challenges (e.g. tariff structures to ensure adequate investments and establish financial risk transfer mechanisms)
- *Communication and Information (Internet)*. Until research efforts, under way 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 lines, and/or dedicated communication systems, should be employed that involve no logical link to publicly accessible computer systems and networks

We did not formally apply the IRGC risk governance framework to this project. But we want to do this within our follow-up projects:

- Assessing and reducing vulnerabilities of transcontinental gas transport systems
- Vulnerabilities of infrastructures to “upset conditions”, e.g. influenza pandemic, natural hazards, political crises
- Comparative study on robustness / resilience strategies in selected regions (US, EU, JP)
- Geological and ocean sequestration of CO₂ – regulatory frameworks