
Editorial: In risk management, integrating the social, economic and technical aspects of cascading failures across interdependent critical infrastructures

Adrian V. Gheorghe

Swiss Federal Institute of Technology, Zürich, Switzerland
E-mail: gheorghe@mavt.ethz.ch

Lamine Mili

Virginia Tech, Alexandria Research Institute, Alexandria, USA
E-mail: lmili@vt.edu

1 Introduction

National security and the quality of life of any nation rely on the continuous and reliable operation of a complex integrated system of interdependent critical infrastructures that provide basic services to all segments of society. These may include:

- electric power systems
- oil, gas and other primary energy storage and transportation systems
- water supply systems
- road, rail, air and water mobility arteries
- telecommunication systems, including computer networks
- banking, finance and insurance systems
- health, fire and other emergency services
- government institutions.

An operational approach to critical infrastructures needs a framework or a definition. One outstanding objective of this journal is to eventually come up with one such definition, which would acquire, and deserve, a sufficient consensus and respectability on behalf of both the expert and stakeholder, worldwide. For the time being, one submits that:

“A critical infrastructure is a business entity of overall societal scope and relevance, consisting of capital investments in hardware and software systems, and human resources, providing marketable goods and/or services that are so vital in usefulness and/or importance that the incapacity or disruption of the respective entity would have a sizeable debilitating impact on the society and its traditional frameworks – the nation, the state, the region etc.”

Following the concerns raised by the growing vulnerabilities of these infrastructures to catastrophic events, their protection against all types of threat, be they man-made, technological, or natural, are receiving a great deal of attention from many state executives and government constituencies. The reasons being put forward to justify the need for new policies and protective actions include the following:

- 1 the significant increase in frequency and intensity of extreme natural phenomena across the globe, which is mainly imputed to the impact of human activities on the earth's climate
- 2 the propensity of operating the critical infrastructures closer to their capacity or stability limits, which is prompted by new technological and regulatory environments, in particular information technologies and deregulation
- 3 the occurrence of wide-area failures that are triggered by a local event and subsequently cascaded across infrastructures and through vast geographical regions, reaching, in some cases, a global scale.

The advent of large-scale cascading failures across critical infrastructures revealed the strong interdependencies that are building up between them as information technologies, and the digital economy that relies on them, expand over countries and continents. It is now evident that these infrastructures need to be viewed, and also modeled, not as isolated entities but rather as a single super-infrastructure composed of multi-layered networked systems. The degree of complexity of this system-of-systems is here magnified as many times as there are infrastructures that compose it, since each of them has a host of interconnected elements that are spatially distributed through broad geographical areas whilst exhibiting complex nonlinear dynamics over many timescales and featuring countless different missions and resources. Therefore, when modelling this super-system for risk assessment and management, the decision maker has to unveil the basic mechanisms underlying cascading failures to achieve model reduction that allows him to overcome the curse of dimensionality. But this is just one of many challenges that he faces. Other challenges are: real-time policy analysis; developmental and safety consolidation investment; contingency planning; emergency response; vocational/topical education and training; public awareness build-up; and crisis governance, to cite just a few.

2 Achieving trade-offs between resiliency and efficiency during the planning phase

The maintenance, protection and expansion of critical infrastructures take on particular importance to any nation, since the lack of or interruptions to their services might have adverse social and economic impacts. Consequently, it is reasonable to assume that the decision maker during the design process is risk averse, implying that he or she is prone to adopt a minimax strategy aimed at preventing a worst-case scenario. The goal of this strategy is to minimise the maximum conditional risk of a catastrophic failure over all possible actions that the decision maker might take, subject to limits on the costs of the design. The conditional risk is here defined as the product of the conditional probability of a cascading failure by its severity.

During the risk assessment stage of a planning endeavor for infrastructure expansion, it is reasonable to assume that the failure rates of system components (including the probabilities of failures that are only exposed during a fault, termed hidden failures) are known since they can be estimated from historical data. The companies and agencies that supervise and operate critical infrastructures routinely estimate component failure rates for reliability assessment purposes. However, frequency estimation of some man-made hazards (e.g. terrorist attacks, intentional sabotage, non-intentional human error) cannot be extrapolated into the future because the nature and magnitude of these hazards depend heavily on the unique political, social, economic and organisational environment in which they occur. It is then reasonable to assume that the probabilities of man-made hazards are unknown. Consequently, decision analysis is carried out in a situation where nature-generated failures have known probabilities, whilst some of the man-made failures have unknown probabilities.

Whilst we may define a catastrophic failure as a failure whose severity is larger than a given threshold, fixed a priori by the decision maker, it is not clear how to measure the severity of a failure. This calculation presents a research challenge because, unlike the direct impacts of a failure, such as damage to equipment and fatalities, the indirect impacts are not easily quantifiable, especially if they include impacts such as business interruptions and human suffering due to psychological stress or adverse health impacts. Some of these costs are not borne nor considered by the decision maker. One important research area is, therefore, the assessment of the conditional risks of cascading failures across these interdependent infrastructures together with the evaluation of the direct and indirect costs entailed by their impacts on the economic and social networks. To this end, methods of evaluation of cascading economic and social impacts of major infrastructure losses need to be developed based on appropriate models. Obviously, these models are to be validated by means of surveys and other real data sampling.

Once the risks and costs are assessed, they are to be integrated into the design decision rules. The minimax criterion is aimed only at providing security against extreme events. As a result, it does not guarantee good performance of the design under events with moderate severity or under the normal operating conditions of the system. Therefore, an appropriate trade-off between conflicting objectives of resiliency and efficiency must be determined.

Another area faced by the present engineering design and facility management community is the mitigation of new and emerging threats to the as-built infrastructure, termed *architectural surety*. In the wake of the World Trade Centre, Oklahoma City and Moscow house terrorist attacks, there is a growing awareness of indiscriminate public vulnerability. Spatial factors (e.g. long, distant pipelines) make it difficult to secure the supply infrastructure and to react promptly in cases of emergency. Agglomeration areas and mega-cities (conurbations with more than 10 million inhabitants by 2010) are highly vulnerable (e.g. increased risk of infectious diseases when sewage systems fail; high death or disease rates caused by accidents in chemical or nuclear facilities). Moreover, they also constitute a risk factor by themselves – since they contribute to pollution or uncontrollable drainage of resources. A multidisciplinary governance and risk and vulnerability management-based program has to be considered and implemented in order to cope with such challenges.

3 Early warning and emergency preparedness

Early Warning, as an emerging new systematic approach to the *risk governance toolkit*, anticipates and extrapolates the potential impacts of new research, technologies and innovation, for a wide area of systems interactions (e.g. welfare, environmental preservation, real and perceived risks, and public acceptance). It addresses issues and analyses consequences as early as possible, up to the level of available knowledge; it gives orientation on how to adopt pertinent and sound decisions. Early Warning is also associated with the practice of the *precautionary principle*.

Often, the Early Warning concept is also associated with *Emergency Preparedness*. However, the simple association is not always either correct, or necessary. Awareness of natural disasters (low frequency – high consequence) should address issues of emergency preparedness mainly in the case of natural catastrophes. Flooding events with impacts on infrastructures, which were built centuries ago, should deserve special emergency preparedness actions. Early warning actions for some distinct infrastructures (e.g. dams) would call for special design specifications and for applying adequate construction standards.

There is a clear distinction between various systems, in relation to risks. Hazards leading to accidents, e.g. from chemical systems, could have negative effects in a time frame of minutes and hours, whilst pollution risks could develop negative health impacts in decades. Other types of risk, such as global climate changes, could have impacts at the century time level, and the potential impacts from nuclear waste repositories, at the level of thousands to millions of years. All these require different early warning management approaches; they would have to introduce different generations of emergency preparedness measures. This simple classification asks for the enumeration of a different arsenal of solutions.

In dealing systematically with the concept of early warning, different categories of issues should be addressed, namely: time scales, damage types (e.g. fatalities, ecological losses), degree of damage in a time-space resolution (e.g. local, regional, mesoscale, global). Early warning and emergency preparedness are often at the extreme ends of a scale of decision ranking. There is a knowledge gap between the moment of asking for an early warning procedure and that when you have to apply procedures for emergency preparedness. As a cross-cutting activity, the pair ‘Early Warning – Emergency Preparedness’, should consider the use of quantitative risk and vulnerability assessment interactively with technological trends, innovation, perception of risks and other social factors. Again, the economics should play a substantial part.

Due to the magnitude and frequency of weather-related hazards that are being observed worldwide, there is an urgent need for the development of a *Global Information Infrastructure* for natural disaster management. This infrastructure would comprise disaster centres strategically located throughout the globe and having the computing power and the human resources to process and analyse the huge amount of data sensed by Earth observation satellites and gathered through communication satellites and the Internet. These centres could play a significant role in climate change modelling, natural hazard prediction and early warning dissemination about any incipient extreme events to local and state authorities and to a broader public.

4 Critical infrastructures risk taxonomy and governance

Risks induced by critical infrastructures are becoming of major public concern. Much attention is focused, in particular, on systemic risks and system breakdown risks, which have transsectoral and transnational impacts. The perception of major traditional risks has changed and important new risk issues have emerged. Some of these are affected by varying cultural differences. The public debate has grown in importance, whilst also taking unpredictable courses on several occasions over the past decades. The fate of nuclear power as an energy source and the emphasis on the environment are only two cases in point. The risk assessment business is challenged by the increasing complexity of its targets and abundant uncertainties, sometimes further compounded by scientific ignorance and ambiguity. Such effects do not spare the field of critical infrastructures.

Risk management and governance processes suffer from a loss of credibility. Too often, they are driven by crisis and swinging public opinion. One major explanation for this is that decision making in risk matters would often fail to successfully combine scientific expertise with careful consideration of the socio-cultural aspects of risk issues. People are not aware, or not willing to accept, that both the physically measurable outcomes (facts) and the socio-cultural attributes (values) form the content of the term 'risk'. Even if one focuses on man-induced large-scale risks, their characteristics differ considerably with regard to:

- the structure, extent, ubiquity and finality (irreversible, acute/late) of the damage, associated levels of probability and the aversion and mobilisation potential
- the risk-inducing initiator (rare severe event, or minor deviation from normal operation followed by malfunctions) and the vulnerability of the systems
- the nature, degree of ambiguity and uncertainties involved.

The available safety principles and forms of management ('strategies') are basically different, as they should take different risk characteristics into account, and/or are inconsistently interpreted and applied: 'ban-based/zero-risk' approach; resilience-based/precautionary principle; risk-based; discourse-based; 'trial-and-error', to cite a few.

Over recent decades, the decision making process has undergone significant changes. Different stages and levels of participation can now be observed. The processes themselves are important and have to take, along with differing risk characteristics and knowledge bases, differing contextual factors into account also, which, fortunately, are levelled down by globalisation trends. This may lead to an inefficient and unbalanced use of resources with regard to risk prevention or reduction. Risks and benefits are often unfairly distributed. Decisions often lack transparency and an adequate involvement of the stakeholders and the public. Decision makers proceed rather reactively, as opposed to proactively, often in an old-fashioned, ambiguous manner. Still, good governance seems to continue resting on three assets: knowledge, legally prescribed procedures, and social values. It has to reflect specific functions, from 'radar' to 'monitoring' to 'communication' as well as precaution, early warning and emergency preparedness.

Criteria such as a sound scientific expertise, burden of proof, consistency and coherence and cost-benefit examination should be part of a generic concept including procedures of 'good democratic' risk governance, which is based on overarching principles and proposes strategies, including transparency, openness, accountability,

effectiveness, and mediation of different/conflicting interests. Realisation of these principles presupposes a comprehensive and systematic approach to risk communication.

5 Editorial policy and objectives of the journal

Placing the topic of critical infrastructures into a wider perspective from the risk assessment and management standpoint is stressed within the editorial policy of this journal. A holistic approach to risk would greatly widen the area of research for the interested stakeholder spectrum, potentially providing answers to a large variety of practical, engineering, ecological, economic, managerial and political aspects of critical infrastructure performance and safety. The research issues to be considered include, but are not limited to:

- analysis and modeling of the interdependencies between critical infrastructures
- vulnerability identification and evaluation of critical infrastructures to catastrophic failures, including development of metrics, models, and methodological approaches
- direct and indirect economic and societal cost assessment of cascading failures across regions and over time
- stochastic modelling of extreme events, e.g. via long-range dependent or α -stable processes
- risks assessment and management of cascading failures within and across critical infrastructures
- evaluation of the impact of policies and governance on the vulnerability of critical infrastructures
- sensors and sensor networking for early warning, emergency control and restoration
- design of a global information infrastructure for disaster risk management to mitigate the impact of extreme natural hazards.

It is believed that this journal could act as a platform to help decision makers dealing with critical infrastructures to identify risks, frame and reframe design issues from a broader global perspective, for instance by bringing views together, by taking the cultural attributes and the physically measurable outcomes equally into consideration. A consensually agreed taxonomy of risks with respect to critical infrastructures could help as an input to define the dominating challenges for risk management and to establish adequate safety principles. The presentation of new ideas and methods will not be limited to experts well established in their respective fields, it will also be open to students, both at the undergraduate and graduate level, who will have the opportunity to share their studies and results in a section especially dedicated to them.

This first issue of the journal also features papers that have been presented at a workshop held on 10-11 September 2001, in Alexandria, Virginia, USA, under the joint patronage of the National Science Foundation (NSF, USA), the International Institute for Critical National Infrastructures (CRIS), the World Institute for Disaster Risk Management (DRM), and the International Institute for Information Technology (IIIT). Entitled "Mitigating the Vulnerability of Critical Infrastructures to Catastrophic

Failures”, this workshop brought together about forty experts in critical infrastructures and disaster risk management from North America and Europe. It gave them the opportunity to discuss various emerging concepts, such as hidden failure, vulnerability, cascading failure, interdependency, risk assessment, and self-healing, among others, and identify research topics aimed at laying the foundation for a new field of expertise dealing with the vulnerability of interdependent critical infrastructures.