COMMENTARY:

Changing the resilience paradigm

Igor Linkov, Todd Bridges, Felix Creutzig, Jennifer Decker, Cate Fox-Lent, Wolfgang Kröger, James H. Lambert, Anders Levermann, Benoit Montreuil, Jatin Nathwani, Raymond Nyer, Ortwin Renn, Benjamin Scharte, Alexander Scheffler, Miranda Schreurs and Thomas Thiel-Clemen

Resilience management goes beyond risk management to address the complexities of large integrated systems and the uncertainty of future threats, especially those associated with climate change.

The human body is resilient in its ability to persevere through infections or trauma. Even through severe disease, critical life functions are sustained and the body recovers, often adapting by developing immunity to further attacks of the same type. Our society's critical infrastructure — cyber, energy, water, transportation and communication — lacks the same degree of resilience, typically losing essential functionality following adverse events. Although the number of climatic extremes may intensify or become more frequent[1], there is currently no scientific method available to precisely predict the long-term evolution and spatial distribution of tropical cyclones, atmospheric blockages and extra-tropical storm surges; nor are the impacts on society's infrastructure in any way quantified[2]. In the face of these unknowns, building resilience becomes the optimal course of action for large complex systems.

Resilience, as a property of a system, must transition from just a buzzword to an operational paradigm for system management, especially under future climate change. Current risk analysis methods identify the vulnerabilities of specific system components to an expected adverse event and quantify the loss in functionality of the system as a consequence of the event occurring[3]. Subsequent risk management has focused on hardening these specific system components to withstand the identified threats to an acceptable level and to prevent overall system failure.

Two factors make this form of protection unrealistic for many systems. First, increasingly interconnected social, technical and economic networks create large complex systems and the risk analysis of many individual components becomes cost and time prohibitive. Second, the uncertainties

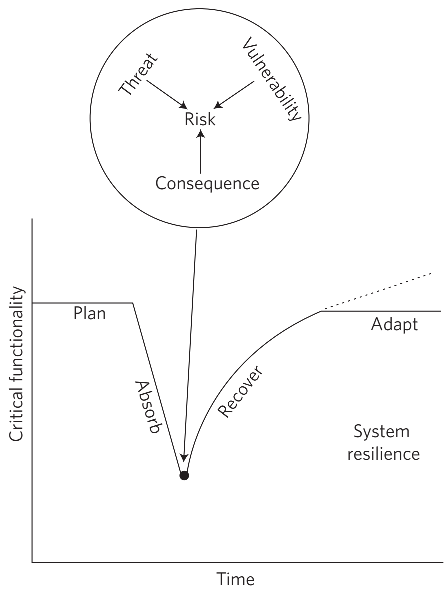

Figure 1 | A resilience management framework includes risk analysis as a central component. Risk analysis depends on characterization of the threats, vulnerabilities and consequences of adverse events to determine the expected loss of critical functionality. The National Academy of Sciences definition of resilience places risk in the broader context of a system's ability to plan for, recover from and adapt to adverse events over time. In the system functionality profile, risk in a system is interpreted as the total reduction in critical functionality and the resilience of the system is related to the slope of the absorption curve and the shape of the recovery curve — indicating the temporal effect of the adverse event on the system. The dashed line suggests that highly resilient systems can adapt in such a way that the functionality of the system may improve with respect to the initial performance, enhancing the system's resilience to future adverse events.

associated with the vulnerabilities of these systems, combined with the unpredictability of climatic extremes, challenges our ability to understand and manage them. To address these challenges, risk analysis should be used where possible to help prepare for and prevent consequences of foreseeable events, but resilience must be built into systems to help them quickly recover and adapt when adverse events do occur.

A roadmap for enabling the development of such capability should include: (1) specific methods to define and measure resilience; (2) new modelling and simulation techniques for highly complex systems; (3) development of resilience engineering; (4) approaches for communication with stakeholders. Strategies for communicating with policy makers are needed to support the shift to resilience management by legislative, regulatory and other means.

The National Academy of Sciences (NAS) defines resilience as "the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events"[4]. Conceptually, risk analysis quantifies the probability that the system will reach the lowest point of the critical functionality profile. Risk management helps the system prepare and plan for adverse events, whereas resilience management goes further by integrating the temporal capacity of a system to absorb and recover from adverse events, and then adapt (Fig. 1). Resilience is not a substitute for principled system design or risk management[5]. Rather, resilience is a complementary attribute that uses strategies of adaptation and mitigation to improve traditional risk management. Strategies to build resilience can take the form of flexible response, distributed decision making, modularity, redundancy, ensuring the independence of component interactions or a combination of adaptive strategies to

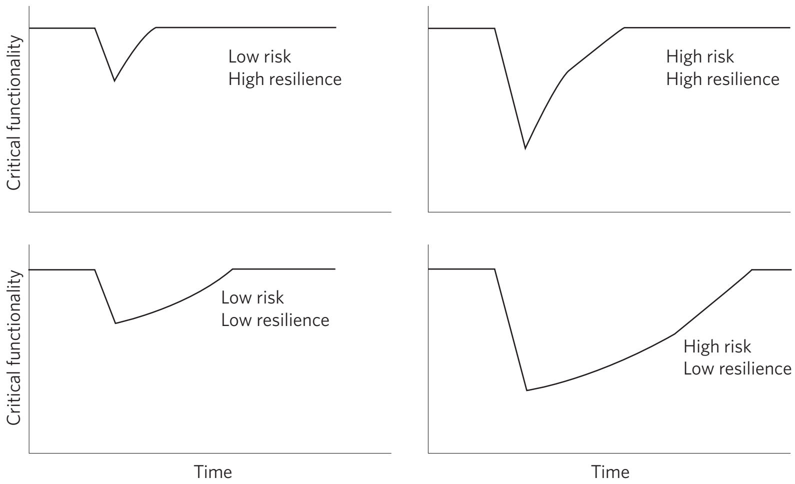

Figure 2 | Schematic representations of changes in critical functionality over time show the interplay of risk and resilience in a system's performance during an adverse event. The size of the initial perturbation reflects the total risk to the system while the shape of the recovery curve is controlled by the system resilience. The area under the curve is indicative of the overall system functionality. Systems that face high risks with high resilience perform better than those facing similar risks but with low resilience. Systems with low risk but also low resilience may perform the same as, or possibly worse than, systems with high risk and high resilience.

minimize the loss of functionality and to increase the slope of the recovery (Fig. 2).

Identifying the need for system resilience requires defining the system. Current efforts often focus on defining systems in just one domain (for example, the physical or information domain), but the complexity of threats affecting multiple domains, and increasing interdependencies between them, requires expanding this definition. In one effort, the concept of military network-centric operation across physical, information, social and cognitive domains was combined with the NAS's definition of resilience[4] to build a resilience matrix where four life-cycle stages of a resilient system (plan, absorb, recover and adapt) are assessed in each domain[6,7]. Of course, assessing resilience either through this matrix approach or otherwise requires a detailed understanding of a system's behaviour and functions, especially during catastrophic events[8]. Modelling and simulation of complex, interconnected socio-technical systems allows system managers to identify weak spots, plan counter-measures in advance, fix errors and prepare, in a comprehensive way, for diverse and heterogeneous threats and vulnerabilities. Growing complexity and the emergence of *ex ante* unprecedented and unpredicted threats necessitate sound principles, innovative thinking, databases, models, methods and simulations of socio-economic technical systems (especially concerning cascading effects) and the application of systems theory and network science in resilience analysis.

Once the system is defined and models to support resilience quantification are developed, the next step is to design interdependent infrastructures to be more resilient. Unlike risk-based design, which focuses on one component at a time, resilience engineering identifies critical system functionalities that are valuable to stakeholders and society. It also involves the development of customized socio-technological methods and solutions to ensure these functionalities are sustained under broad categories of threats. Thus, resilience engineering builds resistance, adaptability and the ability to recover quickly in the face of adverse events (for example, see ref. 9). Examples of technologies for resilience engineering are self-healing, adaptive materials or energy-self-sufficient and automated sensor networks. Such technologies alone do not improve the resilience of a system, but they can be used as components to help reduce unanticipated risks and guide efficient recovery where it is most necessary.

Recent natural disasters and their effects on local socio-techno-economic systems provide examples where resilience management could supplement risk management to improve outcomes following the events. In 2012, Hurricane Sandy struck the Atlantic Coast of the United States, flooding major metropolitan areas in New York and New Jersey, and leaving large populations without fresh water or sanitation facilities. The US Army Corps of Engineers, among other agencies, has traditionally used risk management to address flooding in this region. Building resilient systems to reduce the impact of future events and speed recovery will involve the integration of a combination of structural measures (such as seawalls and levees), non-structural measures (for example, the management of floodplains) and natural and nature-based features (such as beach-dunce complexes and wetlands)[10]. Developing a better road infrastructure and training emergency staff could improve the overall resilience of coastal communities where flooding hampers transportation, communication and the deployment of crucial services.

Management strategies for one network (for example, telecommunications, water, gas, electricity or transportation) often rely on the functionality of another network so that all could be considered part of an overall system of systems. Resilience can be enhanced by studying and improving the interconnectivity of networks. For example, during Hurricane Sandy, power remained off in many coastal areas because street flooding prevented repair trucks from accessing damaged facilities. Systems-level resilience analysis can help identify the need for alternative capacities and the functional autonomy of a given network in the case where multiple networks are concurrently impacted.

Enhancing social networks is also a component of resilience. The meltdown of nuclear reactors at the Fukushima Dai-ichi power plant in 2011 following an earthquake and tsunami led to a crisis situation from which Japan is still recovering. In some ways, Japanese society has proven resilient in the face of this calamity as communities have come together to rebuild and move forward. At the same time, radiation has turned some communities into ghost towns and daunting efforts are required to decontaminate large stretches of land. Resilience must be considered over different time horizons — immediate (for example, evacuation and medical services), intermediate (establishing temporary communities to maintain social connections and clean-up operations) and long-term (permanent relocation and funding to rebuild). Japan has persevered in the face of a large calamity, but it has also experienced policy shortcomings that have further strained affected communities and prevented rapid recovery[11].

Climate change, among other stressors, might produce events that cannot be precisely predicted, analysed or prepared for with traditional risk analysis techniques. Moving forward, resilience will be a key component of sustainable development — striving to meet the needs of the present without compromising the ability of future generations to meet their own needs[12]. Resilient systems share qualities of sustainable systems because they are able to minimize the negative impacts of adverse events on societies and sustain or even improve their functionality by adapting to and learning from fundamental changes caused by those events.

In summary, risk analysis and risk management based on probabilistic quantitative methods have been widely adopted and have been useful for dealing with foreseeable and calculable stress situations. Benchmarks and thresholds for risk analysis are built into the regulations and policies of organizations and nations; however, this approach is no longer sufficient to address the evolving nature of risks in the modern world. Moreover, the increased complexity and interdependency of many of society's critical networks presents a fundamental challenge to even the most comprehensive and sophisticated risk analysis. Therefore, early integration of resilience into the design of systems and the regulatory structures of systems management is needed to address the emerging issues associated with complexity and uncertainty. An urgent need exists to complement the existing knowledge-base of risk analysis and management by further developing frameworks and models enabling system-wide and network-wide resilience analysis, engineering and management. Although research and development on methods and tools is progressing, establishing channels of communication for transparent dialogue on resilience management with stakeholders, such as industry associations and policymakers, is essential for the timely and broad acceptance of resilience concepts. ❐

Igor Linkov[1], Todd Bridges[2], Felix Creutzig[3], Jennifer Decker[4], Cate Fox-Lent[1], Wolfgang Kröger[5], James H. Lambert[6], Anders Levermann[7], Benoit Montreuil[8], Jatin Nathwani[9], Raymond Nyer[10], Ortwin Renn[11], Benjamin Scharte[12], Alexander Scheffler[13], Miranda Schreurs[14] and Thomas Thiel-Clemen[15] are at [1]United States Army Corps of Engineers — Engineer Research and Development Center, Environmental Laboratory, 696 Virginia Road, Concord, Massachusetts 01742, USA, [2]United States Army Corps of Engineers — Engineer Research and Development Center, Environmental Laboratory, 3909 Halls Ferry Road, Vicksburg, Massachusetts 39180, USA, [3]Mercator Research Institute on Global Commons and Climate Change, Torgauer Straβe 12–15, 10829 Berlin, Germany, [4]Embassy of Canada, Leipziger Platz 17, 10117 Berlin, Germany, [5]Swiss Federal Institute of Technology Zürich (ETH), Scheuchzerstrasse 7, 8092 Zürich, Switzerland, [6]University of Virginia, 151 Engineer's Way, Charlottesville, Virginia 22903, USA, [7]Potsdam Institute for Climate Impact Research, Telegrafenberg A 31, 14191 Potsdam, Germany, [8]Université Laval, 2325 Rue de l'Université, Québec G1V 0A6, Canada, [9]University of Waterloo, 200 University Ave W, Waterloo, Ontario N2L 3G1, Canada, [10]RNC Conseil and Ecole Centrale de Paris, 56 Rue Charles Laffitte, 92200 Neuilly-sur-Seine, France, [11]University of Stuttgart, Seidenstraβe 36, 70174 Stuttgart, Germany, [12]Fraunhofer Institute for High-Speed Dynamics, Eckerstraβe 4, 79104 Freiburg, Germany, [13]Hamburg University of Technology, Kasernenstraβe 12, 21073 Hamburg, Germany, [14]Free University of Berlin, Ihnestraβe 22, 14195 Berlin, Germany, [15]Hamburg University of Applied Sciences, Lohbrügger Kirchstrasse 65, 21033 Hamburg, Germany.*
**e-mail: igor.linkov@usace.army.mil*

References

1. IPCC *Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation. A Special Report of Working Groups I and II of the Intergovernmental Panel on Climate Change* (eds Field, C. B. *et al.*) 582 (Cambridge Univ. Press, 2012).
2. Levermann, A. *Nature* **506,** 27–29 (2014).
3. Linkov, I. *et al. Env. Sci. Tech.* **47,** 10108–10110 (2014).
4. National Research Council *Disaster Resilience: A National Imperative* (The National Academies Press, 2012).
5. Park, J., Seager, T. P., Rao, P. C. S., Convertino, M. & Linkov, I. *Risk Analysis* **33,** 356–367 (2013).
6. Linkov, I. *et al. Environ. Syst. Decisions* **33,** 471–476 (2013).
7. Roege, P. *et al. Energy Policy* (in the press).
8. Dauphiné, A. & Provitolo. D. *Annales de Géographie* **654,** 115–125 (2007).
9. Lambert, J. H., Tsang, J. & Thekdi, S. *Am. Soc. Civ. Eng. J. Infrastr. Syst.* **19,** 384–394 (2013).
10. Bridges, T. *et al. Coastal risk reduction and resilience* (US Army Corps of Engineers, 2013).
11. Hollnagel, E. & Fujita, Y. *Nuc. Eng. Tech.* **45,** 1–8 (2013).
12. World Commission on Environment and Development *Our common future* (Oxford Univ. Press, 1987).

Acknowledgements

This paper resulted from discussions at a workshop on the use of risk and resilience assessment methodologies in guiding policy development, held at the Embassy of Canada in Berlin, Germany on 4 February 2014. Partial financial support for the workshop was provided by grant W911NF-13-1-0168 to RNC Conseil, Neuilly-sur-Seine, France. Additional funding was provided by the German National Academy of Technology and Engineering (Acatech), the Helmholtz Association, the Embassy of Canada and the Society for Risk Analysis. Permission was granted by the USACE Chief of Engineers to publish this material. The views and opinions expressed in this paper are those of the individual authors and not those of the US Army or other sponsor organizations.

COMMENTARY:

Capturing provenance of global change information

Xiaogang Ma, Peter Fox, Curt Tilmes, Katharine Jacobs and Anne Waple

Global change information demands access to data sources and well-documented provenance to provide the evidence needed to build confidence in scientific conclusions and decision making. A new generation of web technology, the Semantic Web, provides tools for that purpose.

The topic of global change covers changes in the global environment that may alter the capacity of the Earth to sustain life and support human systems[1]. This includes changes to climate, land productivity, oceans or other water resources, atmospheric composition and/or chemistry and ecological systems. Data and findings associated with global change research are of great public, government and academic concern and are used in policy and decision making, which makes the provenance of global change information especially important. In addition, because different types of decisions benefit from different types of information, understanding how to capture and present the provenance of global change information