SYSTEMS AT RISK AS RISK TO THE SYSTEM

BY MYRIAM DUNN CAVELTY

SYSTEMIC RISK IN FINANCE refers to at least three things, according to George G. Kaufman and Kenneth E. Scott: It connotes a macro shock that produces nearly simultaneous, large, adverse effects in most or all of the domestic economy or even international financial system. It can also refer to the risk of a chain reaction of falling interconnected dominos or a type of spillover that involves weaker and more indirect connections.

In this short essay, I would like to move beyond this more recent and specific articulation of systemic risk in the financial sector by looking at a broader, though closely related kind: The potential for large-scale disasters or catastrophes characterized by both extreme uncertainty and a potential for extensive and perhaps irreversible harm. This type of systemic risk takes center stage in the highly publicized OECD report on 'Emerging Systemic Risks' (2003). The report with its focus on cross-sectoral risk management issues was occasioned by a number of events such as severe storms, the BSE crisis, major blackouts, and last but not least 9/11. It is influenced by German sociologist Ulrich Beck, who coined the term 'World Risk Society', a society responsible for and faced with universal risks with the potential for the gravest of consequences, which he himself occasionally calls systemic risks to contrast it from individual, local or localized risks.

In specific, the report describes 'a marked future increase in the probability of major vital systems (technological, infrastructural, ecological, etc.) being severely damaged by a single catastrophic event (natural or man-made), or a complex chain of events' (page 32). A systemic risk is defined as one that affects 'the systems on which society depends' (page 30). In the policy domain, these 'systems on which society depends' are usually called critical infrastructures and the need to protect them is a contemporary preoccupation among many policymakers. If we compare the lists of critical sectors identified in various countries, we most often find finance, government services, telecommunication, electricity, health services, transportation, logistics and distribution, and water supply. The systemic risk to the financial sector can therefore be seen as specific and very prominent variant of the larger critical infrastructure debate.

Interestingly enough, the word-conglomerate 'systemic risk' is not native to the critical infrastructure protection (CIP) debate itself, but its two components 'system' and 'risk' are.

System: Infrastructures are always depicted as systems and networks. In a variety of disciplines, particularly the natural and the information sciences, different kinds of systems have been studied at least since the 1940s. Systems research is mainly interested in the behavior of systems be they ordered, chaotic or complex. All three types have relevance for system risk thinking, but it is research on so-called complex adaptive systems (systems that self-organize, change and adapt to the broader environment) that has provided most of the vocabulary for the systemic risk language. CIP practitioners are particularly concerned about two types of system effects: cascades and surprise effects. Cascade effects are those that produce a chain of events that cross geography, time, and various types of systems; surprise effects are unexpected events that arise out of interactions between agents and the negative and positive feedback loops produced through this interaction.

Risk: Because CIP is primarily concerned with technical systems, it is the analytical frameworks developed for accidents with hazardous materials in the chemical industry and nuclear power plants that provide the backdrop for how risks are primarily approached in this debate. According to the standard definition of risk found in the technical domain, it is a function of the *likelihood* of a given *threat source* displaying a particular potential *vulnerability*, and the resulting *impact* of that adverse event. The concept of vulnerability, and more specifically, system-vulnerability, takes center-stage in this. Outcomes of the risk assessment process are used to provide guidance on the areas of highest risk, and to devise policies and plans to ensure that systems are appropriately protected.

The problem with this risk conception is that it only works for systems with clear boundaries that *can* be managed. The reality looks a little different, though: individual infrastructure systems are increasingly bridged and interlinked by information-pathways. Continuing reliance on information technologies for their control and maintenance brings forth an increasing number of networks, nodes, and growing interdependencies in and among these systems. The result is a convergence between two previously separate traditions: of system-vulnerability thinking and complexity theory. The two types of system effects described above are where the notion of system meets the notion of risk: By its very nature, a (complex) system contains the risk of large-scale, catastrophic events that are not bounded or localized, but sweeping. Therefore, the very connectedness of infrastructures poses dangers in terms of the speed and ferocity with which perturbations within them can cascade into major disasters.

Advances in information and communication technology have thus augmented the potential for major disaster (or systemic risk) in critical infrastructures by vastly increasing the possibility for local risks to mutate into systemic risks. In addition, the cyber-moment has elevated the discourse to another urgency-level through a change in the spatial dimension of the threat. In the 1980s, the contemporary CIP discourse began in the US government from a concern with government information systems or rather, the classified information residing on them, which seemed easy prey for tech savvy foreign intelligence agencies, a fear based on various well-publicized break-ins (by teenage boys in most cases). In the late 1980s and especially the 1990s, widespread fear took root in the strategic community that adversaries likely to fail against the US war machine might instead plan to bring the US to its knees by striking against vital points at home, namely, critical infrastructures. Laws of nature, especially physics, do not apply in cyberspace; there are no linear distances, no bodies and no physical co-presences. 'Computer weapons' seemed to reformulate space into something no longer embedded into place or presence. This results in two significant characteristics of the threat representation: First, the protective capacity of space is obliterated; there is no place that is safe from an attack or from catastrophic breakdown in general. Second, the threat becomes quasi universal because it is now everywhere.

At the same time, the image of modern critical infrastructures is one in which it becomes futile to try and separate the human from the technological. Technology is not simply a tool that makes life livable: rather, technologies become constitutive of novel forms of a complex subjectivity, which is characterized by an inseparable ensemble of material and human elements. From this 'ecological' understanding of subjectivity, a specific image of society emerges: society becomes inseparable from critical infrastructure networks. This way, systemic risks understood as risks to critical infrastructure systems are risks to the entire system of modern life and being.

This view is ultimately problematic, because it results in generalized and highly diffuse anxiety based on a sense of 'imminent but inexact catastrophe', lurking just beneath the surface of everyday life. The downside of this is that the systemic risk debate as studied in this essay is reduced to a distressing limbo state of not-safe-but-waiting-for-destruction/disaster, a disaster, which is construed as inevitable. But one of the great lessons of risk sociology is that risks 'are' not, they are made by humans and more importantly, as they are not manifest yet but situated in a highly uncertain future, they can be shaped by human choices in the present. What the systemic risk debate needs to be politically stimulating rather than a fear and anxiety trap is a move away from a doomsday-automatism linked to propensities of system effects towards a focus on human action and human responsibility. ☐

MYRIAM DUNN CAVELTY *is Senior Researcher at Eldgenössische Technische Hochschule in Zurich.*

PHOTOGRAPH BY ARSSENEV