IDRiM(2014)4(1) ISSN: 2185-8322
DOI10.5595/idrim.2014.0087

Journal of Integrated Disaster Risk Management

Original paper

Dealing with Disasters: Some Warnings from Science and Technology Studies (STS)

Steve Matthewman[1]

Received: 18/11/2013 / Accepted: 21/12/2013 / Published online: 24/07/2014

Abstract Science and technology are often offered as the source of society's salvation, yet a generation of sociological work on risk seems to reverse this stance. Science and its technological application are positioned as today's greatest sources of ruination. Put differently, our biggest threats and gravest disasters seem to be internal to society itself. Ulrich Beck (1992), Anthony Giddens (1990) and others suggest that they are nothing less than the side effects of industrial modernity. For risk society theorists we clearly now dwell in an era of "manufactured uncertainty" in which various risks keep accumulating (Beck 2009). Such statements beg for empirical elaboration, something which the grand theorists of the risk society have been loath to engage in. Fortunately there is an abundance of material available to us from Science Technology Studies (STS). This can be brought into a critical dialogue with risk society material. In this presentation we consider the two literatures to ask the question: can we identify specifically modern forms of risk and disaster? The argument will be made that we can. There are historically novel forms of risk related to the power, complexity, openness and vulnerability of the socio-technical systems that sustain us. There are also novel consequences too in terms of the temporality and spatial distribution of the risks that they generate. In The Next Disaster Charles Perrow (2007) argued that the two great contemporary risk factors are the concentration of energies and the concentration of populations. In this paper I suggest a third: the concentration of information. The rise of Big Data also brings novel risks that we must attend to. Having made these arguments we will then offer some answers to a follow-on question: what can be done to mitigate such risks and disasters?

Key words Disasters; Science and Technology Studies; Sociology; Risk society

Introduction: Disasters on the Rise

We need not look very far to see that industrial accidents and disasters, "natural" and otherwise, are increasing in scale, frequency, cost and severity. These findings come from sources as diverse as the International Risk Governance Council (Kröger 2007), the Swiss reinsurance industry (Bevere *et al.* 2011), chroniclers of 'disaster capitalism' (Klein 2007: 415) and scholars of 'normal accidents' (Perrow 2007: 1). Accidents and disasters appear to be syndromes of our times. One of the most recent reminders of this comes from the United Nations Office for Disaster Risk Reduction. In May 2013 Secretary-General Ban Ki-moon said that economic losses from disasters were 'out of control', and that direct

[1] University of Auckland, New Zealand. E-mail: s.matthewman@auckland.ac.nz

losses from natural disasters were at least 50% higher than UN estimates, a figure currently thought to be around US $2.5 trillion (UNISDR 2013).

My own concern as a sociologist is that our discipline, which charges itself with making sense of the modern world, has tended to ignore these brute facts. There is a small specialism in the sociology of disasters but leaders within this field criticise it for being piecemeal, isolated from mainstream sociology, lacking in theoretical innovation and blind to differential suffering (Tierney 2007; Vaughan 1999). For a time during the 1990s the discipline's mainstream showed interest in something called "risk society" (Beck 1992; Giddens 1990; Luhmann 1993), but it has fallen from the radar since, while curiously, life has gotten riskier for so many around the world.

In the paper that follows I offer a sociological contribution to the study of disasters by asking the questions: can we identify specifically modern forms of risk and disaster, and, if we can, what can be done to mitigate them? In so doing the discussion will also speak directly to the conference theme: "From Opportunity to Action: Bridging the Gap between Disaster Reduction and Development through Science(s), Technology and People Centred Actions". It will note both the risks and opportunities that science and technology promise before making suggestions – drawn from Science and Technology Studies (STS) – on potentially fruitful people-centred actions. The paper, then, is a meditation on technical, organizational and networked causes of disaster and political and democratic solutions to them.

Science and Technology as Sources of Risk

Science and technology are often offered as the source of society's salvation, yet a generation of sociological work on risk seems to reverse this stance. Science and its technological application are positioned as today's greatest sources of ruination. Put differently, our biggest threats and gravest disasters seem to be *internal* to society itself. Ulrich Beck (1992), Anthony Giddens (1990) and others suggest that they are nothing less than the side effects of industrial modernity. For risk society theorists, we now dwell in an era of "manufactured uncertainty" in which various risks keep accumulating and threatening (Giddens 1995: 78; see also Beck 2009).

To make sense of contemporary reality Anthony Giddens (1990) sketched out the differences between traditional times and our own times thus:

Table 1. Risk in Traditional and Modern Societies

Traditional Society	Modern Society
Reference to the past	Constant scrutiny of the present: reflexivity
Slow pace, limited scope	Rapid pace, global scope
Social activity localised	Activity disembedded from social environment
Unity of time and space	Separation of time and space
Expert knowledge peripheral	Expert knowledge central
Threats from nature	Threats from reflexive modernity
Emphasis on *fortuna* (fate)	Emphasis on risk
External risks	Manufactured risks

Such statements beg for empirical elaboration, something which the grand theorists of the risk society have been loath to engage in (they are, after all, theorists). Fortunately there is an abundance of material available to us from Science and Technology Studies (STS). This can be brought in to supplement the rather abstract risk society material.

The risk society literature's emphasis on "uncertainty" is a useful one to retain. A generation of work

within STS sounds the following warnings to those who seek easy techno-science solutions:

- Experts are not always expert (Stehr and Grundmann 2011: 104-8, Vaughan 1997, Wynne 1996)
- No one is in charge of our complex technologies (Perrow 1984; Wynne 1996)
- Modern socio-technical systems are open and vulnerable (Winner 2004 and 2006)
- Scientific knowledge is socially produced and subject to change (Kuhn 1970)
- Technologies are not good, bad or neutral (Kranzberg 1986)
- Disaster looms: all technologies and technological systems are accidents waiting to happen (Perrow 1984; Virilio 2003; Wynne 1988)

Brian Wynne (1988) and Diane Vaughan (1997) offer ways into thinking about technical and organisational forms of disaster and the role of expert control therein. They also offset the technologically and organisationally determinist accounts of accidents and disasters offered by Perrow in the following section. Wynne and Vaughan both studied the Space Shuttle *Challenger* explosion of January 28, 1986. As Wynne (1988: 150-1) noted, in the case of the *Challenger* NASA was fully aware that some components and subsystems were not in proper working order. This had been the case with previous missions, none of which came to a catastrophic end. The *Challenger* explosion was caused by leaking O-ring seals on the solid rocket boosters. Earlier launches demonstrated thermal stressing of the O-rings and leak paths in the surrounding insulation. It was widely agreed that the O-rings had never performed as they should. They were frequently burned or broken, and they were liable to leak. They were acceptable as opposed to optimal. This was but one component not working to script. The result was that notions of safety shifted. What was taken to be safe was negotiated informally in-house. Observable failures were a matter of ongoing debate, but it was agreed (wrongly in retrospect) that all failures were within acceptable limits. Vaughan identifies such practices as the 'normalization of deviance'. Like Wynne, her empirical investigations led to an emphasis on the routinisation of risk. In particular she draws attention to the flow of information and what she identifies as 'structural secrecy' associated with the activities, interactions and decision making of specialised work groups that give an organisation its form (Vaughan 1997: 238). All of this took place within an organisation that ignored industry safety rules, as well as its own, that was riven by competition and a scarcity of resources, the lacked internal transparency or meaningful external regulation (Vaughan 1997: 33-4).

Novel Risks and Vulnerabilities?

Is there anything to the risk society literature or the insights drawn from STS? Can we identify specifically *modern* forms of risk and disaster, of *manufactured uncertainty*? I think that we can. There do appear to be historically novel forms of risk related to the power, complexity, connectivity, openness and vulnerability of the socio-technical systems that now sustain us.

Indeed, accidents and disasters are to be expected in complex hi-tech assemblages. This is because the potential exists for failures within the system to interact with each other in unanticipated and often incomprehensible ways (recall the bullet points in the previous section). These will be particularly devastating in "tightly coupled" systems where processes are rapid, intimately linked and hard to stop. In these systems accidents will be "normal" (Perrow 1984). Such accidents are the outcome of several failures in processes, planning, personnel, procurement, technologies, materials and environment. Indeed, these normal accidents may even be more normal than Perrow presumes. In New Zealand almost a third of public hospital expenditure goes to treating medical – read accidental – injuries (adverse events), most of which are deemed preventable (Brown *et al.* 2002). Similarly, global estimates of Information Technology projects' failure rates run anywhere between 33 and 80% (Sessions 2009: 3, Thompson

2005).

Complex networks are particularly risky. The global spread of digital technologies, for example, signals an increase in interactive complexity: systems are designed to connect to and synchronize with yet more systems. Indeed, modern systems are coupled together, they form *interdependent* networks. Not that they are typically studied as such (Buldyrev *et al.* 2010: 1025). A fundamental property of interdependent networks is that failure of nodes in one network may lead to failure of dependent nodes in other networks. This can happen recursively and lead to cascading failures.

Let us discuss these points with reference to electrical power generation and distribution. This rests on a complex and vulnerable assemblage in which power does not consistently flow along the same predetermined path. When a supplier sends power to another it increases the power supply, while the receiver either reduces production or has increased demand. Power goes from "source" to "sink" along connecting paths. Shifts in generation and transmission anywhere within the system alter loads on generators and transmission lines at all other points, the consequences of which may not be fully anticipated or managed. Delivery systems become more complex as distances and interconnectivity increase.

The normal way to guard against system failure is to ensure that power flows remain below the transmission line's capacity. When the capacity limit is transgressed the lines overheat. This may cause them to sag, generate unstable power supply or even fail. Longer power lines result in greater losses. Further vulnerabilities arise because AC power grids need the frequency and phase of all power generation to synchronise within tightly defined limits. Circuit breakers are used to remove generators from the system if their frequency fluctuates too greatly. However, when 'certain parts of the grid are carrying electricity at near capacity, a small shift of power flows can trip circuit breakers, which sends larger flows onto neighbouring lines to start a chain reaction failure' (Lerner 2003: 10).

Electrical power is not merely infrastructure; it meets the International Risk Governance Council's (IRGC) definition of *critical* infrastructure. Critical infrastructures are large-scale human-built systems that supply continual services central to society's functioning. They are the subject and source of numerous threats. These systems typically have no single owner, manager or controller meaning interests and operating procedures can diverge and conflict (Kröger , 2005).

The vulnerability of the electricity system is demonstrated by a blackout which took place on September 28, 2003. This rapidly escalated into grid collapse. The event began when a falling tree broke an electrical power line in Switzerland's Lukmanier Pass. The nearby San Bernadino line subsequently overloaded. Twenty four minutes after the first tree flashover, a second tree came down in the San Bernadino Pass. Two important lines failing were too much for the system to bear. Moments later the overloads tripped the other interconnectors towards Italy, separating it from Europe's electricity network (UCTE 2004: 4-5). The low voltage level in the north of the country caused several Italian power plants to trip. All of Italy was left without power. It says something about the fragility, complexity and interconnectivity of the modern world when a nation is brought to a halt by two trees falling outside its territory. During what time period could this happen but our own?

The IRGC measures criticality by space, size and time: the geographical spread of failure, the severity of its effect and the speed with which it is felt. Failure in the electric power network is potentially international in scale; it can profoundly affect those within the afflicted area and do so immediately (Kröger 2007: 10). Network failures of this type are as critical as it gets. Disruptions to critical infrastructures have rippling effects as they are dynamic and interdependent arrangements. Electricity powers, connects to and synchronises with other systems. Stephen Graham (2010: 5) argues that it is more apt to think of separate infrastructures as a complex single whole. Blackouts affect pumps, refrigeration, traffic lights, trains and cell phone towers. This has serious consequences for water, waste, food, transportation and communication systems. Modern social life is impossible to imagine without it.

In addition to thinking about novel forms of risk we might also want to devote some time to considering the novel consequences of risks in terms of their temporality and spatial distribution. These novel features can be summarised in brief as:

- A new temporality: dangers can exist across longer periods of time – industrial toxins, for example, can have intergenerational impacts. Kai Erikson (1995) referred to them as a 'new species of trouble', in part because they have no obvious beginning, middle or end.
- A new spatiality: in a globalised world risks are also globalised. Anthropogenic climate change is a good example here. Though human-made it does not respect any political boundary. Modern risks, Ulrich Beck says, are "de-bounded".
- A new potency: we have created risks which exceed our ability to communicate them. Nuclear waste remains dangerous for hundreds of thousands of years. No symbol system, no language, has lasted more than a few millennia.
- Taken together these new risks may also indicate a new victimology. Beck (1996: 31) famously said that not all of the victims of Chernobyl have yet been born.

A new role for the media: again, ionizing radiation is the perfect exemplar. We cannot detect it. It evades the dominion of the senses. We need the media to alert us to such dangers. But there are other reasons for including the media here. For Susan Sontag (2003: 18): 'Being a spectator of calamities taking place in another country is a quintessential modern experience, the cumulative offering by more than a century and a half's worth of those professional, specialized tourists known as journalists'. It is only in our own epoch that we witness the world's suffering.

The Next Catastrophe

Thus far we have discussed modern risks, focussing on a specific event. But the sociology of disasters and the sociology of complex organisations both suggest that we think beyond the 'event': the disaster itself and its immediate aftermath. They urge that consideration also be given to those undergirding structural factors that contribute to disasters (a point which resonates with the conference theme given its signalled intent of 'disaster reduction'). In order to do this scholars suggest seeking to reduce vulnerabilities.

For Perrow we do this by avoiding the three great risk factors, which are concentrations of: energy, population, and political and economic power. Concentration of energy refers to such things as water stored behind dams, and the storage of toxic and explosive materials. Concentrations of population are to be avoided in risky areas like flood plains, in high density areas (which will also add additional infrastructural stresses) and near concentrations of energy. Perrow also warns against the tendency to monopoly, which he calls "monoculture". Typically the third risk factor permits the first via deregulation and privatisation.

This final point has been powerfully reinforced upon us in New Zealand of late. In our country the key question pertaining to our identity is: are we a farm or a film set? By economic returns the answer is unequivocally the former. And our fortunes are made by peddling a wholly fictitious "clean green" brand. But with intensive agriculture comes extensive pollution. And with the concentration of economic power – a single company pushing a single commodity – comes significant risk and vulnerability. This was demonstrated in August this year when Fonterra, the country's largest dairy manufacturer, announced that a pipe at its whey-processing plant had not been properly cleaned. Later inspections erroneously identified revealed traces of botulism-causing bacteria. The *Listener* magazine editorialised:

New Zealand is now facing the terrifying truth of how vulnerable its economy is to even a small error… [O]vernight the country's priceless reputation as a supplier of safe, quality food is in international

question – and with it, potentially, a ruinous chunk of our economy.

New Zealand is always just one unfortunate accident away from penury. Overwhelmingly dependent as we are on our reputation as a reliable source of processed agricultural products, a safety scare about any product, let alone baby food is catastrophic (Stirling 2013: 3).

The financial media reinforced the point. At *Bloomberg* Matthew Brockett and Tracy Withers (2013) wrote of the contamination, in a piece titled 'New Zealand's World Dairy Dominance Becomes Achilles Heel', quoting bank of New Zealand economist Doug Steel: 'The events of the past few days are a stark reminder of New Zealand's increasing vulnerability to a single product and to a single export destination'. The scare led to product recalls in China and bans in Belarus, Kazakhstan, Russia and Sri Lanka, with issues reported in Vietnam, the Middle East and elsewhere. The true cost to the economy is yet to be calculated, but it is projected to run into the millions.

Perrow offers a persuasive schema to understand the production of disasters in our world, but it seems to be the case that he misses something out here. Surely in the modern networked world another contemporary risk factor is the concentration of information.

Marc Goodman (2012) draws attention to this in an article called 'Dark Data'. This piece signals the downside of the Big Data digital revolution. He notes that no technology has ever been produced that has not been hacked. The Sony Playstation hack is a worrying precedent: 'more than 100 million people had their accounts compromised and their passwords stolen. Never before in human history has it been possible for one person to rob 100 million people – but our interconnectedness and mass data storage now make this possible' (Goodman 2012: 76). Ominously, Goodman suggests that we are really only seeing the beginnings of cybercrime. The explosion of medical monitoring technologies – smart bracelets, smart phone apps that measure such things as blood sugar levels or brain activity – are particularly concerning. What happens when these technologies get hacked? What also of the swathe of medical implants that transmit digital data: cochlear implants, diabetic pumps, pacemakers and defibrillators. Over 60 000 Americans have pacemakers connected to the internet. How would you feel about someone illegally accessing that data? How would you like your pacemaker turned off? Writes Goodman (2012: 77): 'Criminals, terrorists, and hackers understand the power of our interconnectivity: if you control the code you control the world'.

We know, in fact, that these technologies have been hacked. Insulin pumps were hacked by the New Zealander Barnaby Jack in 2012 (Robertson 2012), and this year he was to demonstrate the hacking of pacemakers and defibrillators at a Las Vegas conference (Holpuch 2013).

Goodman has noted the downside of the Big Data revolution, but STS teaches us that technologies are not simply good or bad, that their impact and significance are to be found in cultures of use. It seems to me that we will continue to live with the downside of connectivity and Big Data: fraud, and increasing state and corporate surveillance. But equally it seems to me that Big Data and connectivity can be harnessed for collective welfare, to assist with disaster reduction and to enable people-centred actions. Google's Crisis Response, for example, is well established (http://www.google.org/crisisresponse/). It includes public alerts, partnering opportunities and tools for first responders. Indeed, there is now an established literature on "crisis informatics" (see the database assembled by Leysia Palen 2013).

Mitigating the Next Catastrophe

What is to be done about today's risks? Ulrich Beck (2005: 7-8, 182-183) suggests other potential solutions via the development of a cosmopolitan orientation which recognizes the global connections of people, their nations, economies and environments. Risky practices can be further reduced by acts of political consumption (boycotts), nationalization and re-regulation. While the lesson that Charles Perrow (1984: 64) draws from all of this is that we should modify our management of systems where the risks

might be acceptable (where possible looking to forge "loose couplings") and abandon systems where the consequences of accidents are too great (for example, nuclear power).

Indeed, we can mitigate risks by moving from concentrations to "deconcentrations" and from dependencies to interdependencies (for example the internet looks like an interdependent system yet most of us are dependent upon Microsoft products). In preference one should seek to make relationships based on commonalities and reciprocity. The mechanisms for doing all of this are largely regulatory: good governance in the public sector (including high levels of citizenship participation and transparency), and robust regulation of the private sector (including anti-trust legislation). Perrow also alerts us to two other types of failure in addition to regulatory failure: organisational failure and executive failure.

These transformations are a major but necessary challenge. They involve us making adjustments to our risk assessments and to our vision. Perrow suggests that risk assessment could usefully shift from probabilistic to "possibilistic" estimations: what happens when the worst-case scenario results? Are some economic, political or technological arrangements simply too risky to permit? Accidents and disasters do not just typically happen: there are lead-ups, concerns and warnings, certain "red flag" moments. These warnings should be heeded. Additionally, decisions which are made for short-term benefit (in business and in politics) should be shifted to the longer term. Therein lies the path to sustainable solutions. Finally, Perrow suggests build resilience wherever possible. Stem growth in high vulnerability areas (he mentions California and Florida), compel catastrophic loss insurance, and distribute relief on a need basis rather than in accordance with the dictates of political patronage.

These suggestions all make good sense. Leaving it to experts and politicians seems to be a risky strategy. Besides, who is expert? Now we are not simply enquiring in relation to the complexity of today's socio-technical systems (empirical studies by Perrow himself, Wynne and others within STS show us that there is no such thing as an all-knowing authority) but something much broader: surely experts are not simply those who study issues or potentially profit from them but are also those that live and breathe the issues and that potentially suffer from them. Do they have nothing to contribute? Most of Perrow's solutions are technocratic. They rely on politicians and official authorities. Here we offer some final thoughts on what is to be done, making specific reference to the people-centred actions of the conference theme.

The Democratic Disaster: Bringing the People Back In

There is now a burgeoning sociological literature devoted to the problems with our democracies. The basic point being that government these days appears to be of the people rather than by and for them. Sociologists note rising levels of atomisation and individualisation (Putnam 2000), and a corresponding erosion of community and civil society. Colin Crouch (2004) has argued that we are moving into a post-democratic paradigm, while Manuel Castells (2005) has suggested that we are witnessing a 'crisis in democracy'. Some work has also been done in this area by practitioners of STS. Here I pick up on the work of Michel Callon and colleagues (Callon *et al.* 2009).

One of the problems Callon sees with standard democratic processes and market practices – which he refers to as "delegative" democracy – is that they create overflows. Economists understand these as externalities. Callon draws attention to two sociologically interesting types of overflows – where overflows are unforeseen effects and unexpected problems. He calls these orphans and hurt groups. Orphan groups are too small to count politically or economically – there is no viable market for them. Hurt groups are those that suffer from overflows, as in pollution. To Callon's way of thinking the hurt and the orphaned should be included in the very decisions which affect their lives. Callon's work with Pierre Lascomes and Yannick Barthe focuses on scientific and technological advances and controversies, but given that the large body of disaster literature returns some fairly consistent findings around the necessity of successful community engagement to ensure meaningful community rebuilding and on-going

resilience – could we not apply their insights into this area? It is an open question, although my personal view is that we can. I think that the democratization of democracy, the development of a "dialogic" democracy in Callon *et al.*'s terminology can only be healthy. Surely decisions are more robust when they are not made for us but with us. What is required is a technical upgrade of our political systems. Callon et al suggest developing "hybrid forums" of citizens, experts and politicians. Earlier, Wynne and Vaughan gave us some insights into what can happen when we leave things solely to the experts.

As Callon *et al.* recognise, it is the configuring of experts in hybrid forums that mix them with citizens and politicians that will hopefully produce new forms of distributed intelligence able to engage with and promote more informed and less disastrous futures. In their opinion there are several problems with standard "delegative" democracy. To begin with it sets up two divides: between experts and laypersons and between elected representatives and ordinary citizens. If democracy is reduced to merely dropping a paper into a ballot box every few years it is not all that democratic. Some people participate in this process but some will be excluded (as in those under the legal voting age or perhaps those to infirm to make it to a polling station). A related problem is that groups are reduced to voting individuals, when they may live and identify as functioning members of a collective. Typically when voting or participating in some form of referendum the number of options are limited, perhaps only to "yes" or "no" responses. Once votes have been tallied representatives are appointed. This means that populations are reduced to their representatives, which also means that the represented are effectively silenced.

The solution to this democratic malaise is the creation of hybrid forums to highlight externalities and exclusions. These hybrid forums can take various forms: focus groups, public inquiries, consensus conferences, citizen's panels and juries. These deliberative bodies contain citizens, experts and politicians. How do they come about? Callon et al suggest that every controversy or disaster creates new actors. This could be communities that suddenly find themselves living next to proposed nuclear storage waste sites or those populations displaced by an earthquake. Emergent groups will then form. It is the task of the authorities to learn their composition, their preoccupations and their expectations. So, we can refer to this initial phase as relating to issues of identity: *the quest to be heard.* Progress comes when there is recognition of other concerned and interested groups. This second phase is marked by the willingness to *listen*. When these groups merge into a collective – which involves compromise and adjustment, we have a successful outcome – 'collective experimentation and learning' (Callon et al. 2009: 9), the creation of a new common world.

In their opinion, having assessed several western European ventures of this kind, various associations, media and public authorities need to be involved if it is to work out and to be meaningful. They also observe varying levels of success. They measure these according to three criteria which they call: intensity, openness and quality. Firstly, any dialogic fora must include lay groups early on in the disaster or controversy, and they must show a strong concern for the composition of the collective. Secondly, there must be a diverse range of groups included, and ideally they should be independent of well-established interest groups that pre-date the current issue. Official spokespersons should also be truly representative of their groups. Thirdly, the issues raised should be serious and worthwhile, and the continuity with which they are raised should be observed. Finally, we get to the implementation phase. Three questions are worth keeping in mind: i) Are the various interested parties able to access the debates and participate in them? ii) Transparency: are debates open and are they easily accessed? iii) Clarity: are the rules that frame debates clear?

My closing comment is actually a question. Such practices have worked in western countries concerning scientific and technological controversies: could they work in non-western societies and in relation to disasters? Stated more provocatively, would a hybrid forum engaged in Haitian rebuilding have made the US military the largest aid beneficiary (Katz 2013)?

REFERENCES

Beck, U. (2009) World Risk Society and Manufactured Uncertainties. *Iris*, 1(2): 291-299.

Beck, U. (2005) *Power in the Global Age*. (K. Cross, trans.). Polity, Cambridge.

Beck, U. (1996) World Risk Society as Cosmopolitan Society? Ecological Questions in a Framework of Manufactured Uncertainties. *Theory, Culture & Society*, 13(4): 1-32.

Beck, U. (1992) *Risk Society: Towards a New Modernity*. (M. Ritter, trans.). Sage, Los Angeles.

Bevere, L., Rogers, B., and Grollimund, B. (2011) *Sigma, No. 1: Natural Catastrophes and Man-made Disasters in 2010: A Year of Devastating and Costly Events*. Swiss Reinsurance Company, Zurich.

Brockett, M., and Withers, T. (2013) New Zealand's World Dairy Dominance Becomes Achilles Heel. *Bloomberg*, 7 August. Available: http://www.bloomberg.com/news/2013-08-06/new-zealand-s-world-dairy-dominance-becomes-its-achilles-heel.html [28 August 2013].

Brown, P., MacArthur, C., Newby, L., Lay-Yee, R., Davis, P., and Bryant, R. (2002) Cost of Medical Injury in New Zealand: A Retrospective Cohort Study. *Journal of Health Services Research & Policy*, 7(Suppl. 1): 29-34.

Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H. Eugene, and Havlin, S. (2010) Catastrophic Cascade of Failures in Interdependent Networks. *Nature*, 464, 15 April: 1025-8.

Castells, M. (2005) *The Power of Identity*. Blackwell, Malden.

Callon, M., Lascoumes, P., and Barthe, Y. (2009) *Acting in an Uncertain World: An Essay on Technical Democracy*. MIT, Cambridge, Mass.

Crouch, C. (2004) *Post-Democracy*. Polity, Cambridge.

Erikson, K. (1995) *A New Species of Trouble: The Human Experience of Modern Disasters.* W.W. Norton, New York.

Giddens, A. (1995) *Beyond Left and Right*. Polity, Cambridge.

Giddens, A. (1990) *The Consequences of Modernity*. Stanford University Press, Stanford.

Goodman, M. (2012) Dark Data. In R. Smolan and J. Erwitt (eds) *The Human Face of Big Data.* Against All Odds Productions, Sausalito, California: 74-77.

Graham, S. (ed.) (2010) *Disrupted Cities: When Infrastructure Fails*. Routledge, New York.

Holpuch, A. (2013) Hacker Barnaby Jack's Cause of Death Could Remain Unknown for Months. *The Guardian*. July 29. Available: http://www.theguardian.com/technology/2013/jul/29/barnaby-jack-hacker-cause-of-death [28 August 2013].

Katz, J. (2013) *The Big Truck That Went By: How the World Came to Save Haiti and Left Behind a Disaster*. Palgrave Macmillan, New York.

Klein, N. (2007) *The Shock Doctrine: The Rise of Disaster Capitalism*. Allen Lane, Camberwell.

Kranzberg, M. (1986) Technology and History: "Kranzberg's Laws". *Technology and Culture*, 27(3): 544-560.

Kröger, W. (2007) *Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures*. International Risk Governance Council, Geneva.

Kröger, W. (2005) ‚Der Umgang mit systemischen Risiken – Das Angebot des International Risk Governance Council', Präsentation in der Vortragsreihe „Umgang mit gesellschaftrelevanten Risiken", ETH Zürich, 13 April, available: http://www.lsa.ethz.ch/news/050413-Vortragsreihe-ETH-Handout.pdf

Kuhn, T.W. (1970) The Structure of Scientific Revolutions. The University of Chicago Press, Chicago.

Lerner, E.J. (2003) What's Wrong with the Electric Grid? The Industrial Physicist, October/November: 8-13.

Luhmann, N. (1993) Risk: A Sociological Theory. A. de Gruyter, New York.

Palen, L. (2013) *Crisis Informatics Articles*. University of Colorado Boulder. Available: https://www.cs.colorado.edu/~palen/Home/Crisis_Informatics.html [21 August 2013].

Perrow, C. (2007) *The Next Catastrophe*. Yale, New Haven.

Perrow, C. (1984) *Normal Accidents: Living with High-Risk Technologies*. Basic Books, New York.

Putnam, R. D. (2000) *Bowling Alone: The Collapse and Revival of American Community*. Simon & Schuster, New York.

Robertson, J. (2012) McAfee Hacker Says Medtronic Insulin Pumps Vulnerable to Attack. *Bloomberg*. March 1. Available: http://www.bloomberg.com/news/2012-02-29/mcafee-hacker-says-medtronic-insulin-pumps-vulnerable-to-attack.html [28 August 2013].

Sessions, R. (2009) *The IT Complexity Crisis: Danger and Opportunity*. Available: http://www.objectwatch.com/whitepapers/ITComplexityWhitePaper.pdf. [3 November 2009].

Sontag, S. (2003) *Regarding the Pain of Others*. Picador, New York.

Stehr, N., and Grundmann, R. (2011) *Experts: The Knowledge and Power of Expertise*. Routledge, New York.

Stirling, P. (2013) 'A Terrifying Truth', *Listener*. 17 August, p. 3.

Southeastern Louisiana University (2010) Twitter Used to Predict Flu Outbreaks. *ScienceDaily*. 29 September 29. Available: http://www.sciencedaily.com/releases/2010/09/100928153809.htm [17 September 2013].

Thompson, C. (2005) *Improving IT Professionalism and Performance*. Available: http://www.bcs.org/server.php?show=ConWebDoc.3047 [3 November 2006].

Tierney, K. J. (2007) From the Margins to the Mainstream? Disaster Research at the Crossroads. *Annual Review of Sociology*, 33: 503-525.

Union for the Coordination of the Transmission of Electricity (UCTE) (2004) *Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy*. Available at: http://www.rae.gr/old/cases/C13/italy/UCTE_rept.pdf [19 October 2012].

UNISDR. (2013) *From Shared Risk to Shared Value –The Business Case for Disaster Risk Reduction: Global Assessment Report on Disaster Risk Reduction*. UNISDR, Geneva, Switzerland.

Vaughan, D. (1997) The Challenger launch Decision: Risky Technology, Culture and Deviance at NASA. The University of Chicago Press, Chicago.

Vaughan, D. (1999) The Dark Side of Organizations: Mistake, Misconduct, and Disaster. *Annual Review of Sociology*. 25: 271-305.

Virilio, P. (2003) Foreword. *Fondation Cartier*. Translated by C. Turner. Available: http://www.onoci.net/virilio/pages_uk/virilio/all_avertissement.php. [13 May 2013].

Winner, L. (2006) Technology Studies for Terrorists: A Short Course. In T. Monahan (ed.) *Surveillance and Society: Technological Politics and Power in Everyday Life*. Routledge, New York: 275-291.

Winner, L. (2004) Trust and Terror: The Vulnerability of Complex Socio-Technical Systems. *Science as Culture*. 13(2): 155-172.

Wynne, B. (1996) May the Sheep Safely Graze? A Reflexive View of the Expert-lay Knowledge Divide. In S. Lash, B. Szerszynski and B. Wynne (eds) *Risk, Environment and Modernity: Towards a New Ecology*. Sage, Thousand Oaks, California: 44-83.

Wynne, B. (1988) Unruly Technology. Practical Rules, Impractical Discourses and Public Understanding. *Social Studies of Science*. 18(1): 147-167.