Infrastructure Technologies and Risk: From National Security Problem to the Management of Electricity Supply

Extended abstract
The new politics of risk: the performing of regulation in a comparative perspective
EASST Conference 2010,
Practicing Science and Technology, Performing the Social
University of Trento,
Italy, 2-4 September 2010.

Antti Silvast
Doctoral candidate
Department of Social Research, University of Helsinki, Finland
phone: +31-6-84906416
email: antti.silvast@helsinki.fi
homepage: http://www.valt.helsinki.fi/blogs/silvast/inenglish.htm

Introduction

Two main approaches may be identified in the currently popular sociological discussions about risk. First, many sociologists claim the current practices of risk result from late 20 th century and early 21st century societal developments. Accordingly all societies everywhere have entered a new epoch which results into new form of societal relationship to risks (e.g. Beck, 1992; Giddens, 1990; Furedi, 2006). Second, in another popular discussion, it has been argued that risks are always the result of cultural interpretations, not merely of `objective´ technical calculations of probabilities and impacts of unwanted events. Sociologists should also thus not study the tools and techniques of risk, but instead, the ways that people perceive risk inside their cultural groups (Douglas & Wildavsky, 1982).

These are relevant and important considerations for guiding research. Yet, at the same time, often they tend not to be sensitive to the diversity of the ways that technical experts and safety specialists are already managing insecurity. In the research project *Managing Insecurity: Risk and*

Technologies of Welfare, based at the University of Helsinki, Faculty of Social Sciences, we concentrate thus on the techniques that translate concerns over welfare and security into risks and the ways how these risks are implemented in the daily practices of people. By being empirically sensitive to the different expert ways of dealing with risks, we strive to avoid the presumption that all contemporary risks result from one general societal development, or that every risk is either completely cultural or completely `objective´ to start with.

The empirical subprojects of the Managing Insecurity project analyze different topics related to the technologies of welfare in Finland: private insurance, social insurance, health care and electricity supply. The research question of my dissertation project is: *How does risk figure in the managing electricity supply in Finland?* The research is grounded on two separate cases. The first of these is based at the level of national security and defence policy. According to earlier research regarding the US, the construction of critical infrastructures as a national security problem in the 20 th and 21st century has happened through a number of steps, from "concern with critical systems upon which modern society, economy and polity depend" to "the identification of vulnerabilities of these systems and of threats that might exploit these vulnerabilities as matters of national security" and finally the "effort to develop techniques to mitigate system vulnerabilities" (Collier & Lakoff, 2008, 24).

Adapting these and other related research approaches (Kristensen, 2008; Collier, 2006; Edwards, 2003), I want to study the emergence of infrastructures as a national security problem in Finland. Semiotic analysis methods (Silvast, 2006, 2009; Greimas, 1980/1966; Sulkunen & Törrönen 1997a, 1997b) are employed, and focus is placed on the capabilities, obligations and agency associated with *infrastructures*, the notion of *dependence* on them, the notion of *vulnerability* because of this dependence and the figurations of the concept *risk* and the related *preparedness* and *prevention.* As for empirical material, the case uses Finnish security documents from the 2000s. To lesser extent, background information from security expert interviews and participation in infrastructure-security themed seminars is also employed.

National policy is an increasingly powerful way of constructing infrastructures as a security problem (Collier & Lakoff, 2008; Kristensen, 2008). Yet, at the same time, it is not the only topic domain where infrastructure risk may figure. To illustrate this, the second case of the dissertation inverts the research design from the previous case: instead of concentrating on the `high´ level of national security and defence policy, the case analyzes the `low´ basis of normally invisible layers of infrastructure operation (see Bowker & Star, 1999). Building on research results from earlier

studies and analyses, it will concentrate on the local and situated skills that are needed for the operating a large technological system (Steenhuisen, 2009; Roe & Schulman, 2008; De Bruijne, 2006) and the effects of automation, ownership of organizations, weather conditions, customer welfare and competitive market logics to infrastructure provision (Kumpulainen et al, 2006; Graham & Marvin, 2002). To this end the case asks the following research question: what are the key meanings and daily practices related to infrastructure risks for technicians who work in the two control rooms of an electricity distribution company in a Finnish town? The duties of these rooms, on-going 24 hours a day seven days a week, are trading electric power at the common Nordic electric power exchange Nord Pool in the so-called *energy market control room* and maintaining the town's electricity distribution networks in the so-called *electricity distribution control room*. The research of the rooms relied on interviews and participant observations which were carried out during six days of the technicians' work in 2008. For learning more about control room practices and terminology, I have also spent a number of days in different infrastructure control rooms in Netherlands together with a research group from the Delft University of Technology, Faculty of Technology Policy and Management.

For the remainder of this extended abstract, I summarize preliminary research results from the two cases and then briefly discuss them in the concluding section.

Constructing a national security problem

The first case of the dissertation studied how electricity supply has been constructed as a Finnish national security problem. The analysis starts by noting that there exists two normative rationalities of technology security in Finland: *the security of supply thinking*, which goes back to the defence economic planning of the 1950s and was later articulated in the Security of Supply Act and the founding of the National Emergency Supply Agency in 1992, and *the vital functions thinking*, which stems from Finnish security and defence policy concerns for internationalization and new security risks from the early 2000s and was not originally concerned with securing technological systems, but with defining the heterogeneous `functions´ – for example the economy, state affairs and military defence – that are needed for the maintaining of the Finnish `society´. I have chosen to study this latter thinking, because it articulates an important aspect of infrastructure risk: namely, if infrastructures are understood as "those systems without which contemporary societies cannot function" as sociologist Paul Edwards (2003, 187) has written, then it is fruitful to look at what is understood as this `society´ and its `functioning´ in the context of national policy. As far as I know, this kind of focus on society's vital functions is also rather original instance in the international

policies of critical infrastructure protection – though not always acknowledged to be so by security experts (see the national review of infrastructure protection policies by Finnish security experts in Abele-Wigert & Dunn, 2006). Moreover it has seen three official strategies in 2003, 2006 and forthcoming in 2010 respectively thus facilitating comparisons for changes within security discourses.

The case documents that the vital function strategies have indeed seen abrupt changes with style of writing and vocabularies between 2003 and 2006. Towards the 2006 strategy, the vital functions thinking becomes increasingly preoccupied with technological malfunctions, and for this end the official strategy starts to employ technocratic security concepts `vulnerability´ and `dependence´. Accordingly it is actors such as the `whole society´ or all `services in the society´ that have become `dependent´ on `technology´ such as information and communication technologies and energy supply, and hence `vulnerable´ to technological breakdowns. Conversely, in the 2003 strategy, the concept `dependence´ still mostly points to `threats´ that are the result of action states or other political and societal actors: for example, energy import dependency is presented first of all a geopolitical problem not a technological dependency problem. Also the concept `infrastructure´ changes markedly between the 2003 and 2006 strategy: instead of being the capacity for provision of vital functions as in 2003, in 2006 infrastructures become themselves defined as one of the society's vital functions that we are dependent on and that need to be protected.

As for the figurations of tools and techniques, where as protection of critical infrastructure in the US (Kristensen, 2008) and the EU (European Council, 2008) promotes the calculation of the probabilities and impacts of unwanted events through the technique of risk, calculation seems not to be the only or even the main technique that figures in the Finnish reasoning about society's vital functions. Instead, the techniques of *prevention* and *preparedness* are prescribed to ministries and in 2006 increasingly also to private businesses, and these techniques supplement planning for risk with regular crisis exercises and the creative imagining of disaster scenarios. This I would claim represents a precautionary approach to risk: the exercises and scenarios, like the precautionary principle, do not rely on systematically measured formalized data – for the respective complex threats, this data does not nearly always exist – but instead on `worst-case hypotheses´ imagined by security experts. This marks also, perhaps an unexpected, analogy from the Finnish infrastructure security considerations to currently topical European political discussions on precaution with respects environmental risks, consumer protection and medical accidents (Callon et al, 2009).

Control room risk

Inverting the research design from the first case, the second case of the dissertation analyzes infrastructure risk at the `low´ basic level of control rooms where electricity supply systems and energy markets are being operated. This control room work, in first appearance, is highly routine and standardized. The routine character is most of all reflected on the workers' opinions about what they do. Several energy market room technicians reported that their work is almost wholly subsumed under the economic demands of making profitable stock exchanges on the energy markets. For the distribution room's workers, they told me that their work strives for maintaining the physical well-being, health and safety of customers and line workers and avoiding material losses that result from technical breakdowns, in this order of priority. Towards these ends the work was reported to follow strict laws, standards and practical protocols. Risks that went beyond these practices seemed to be superfluous for the workers, leading one of them even to conclude that there is no security risk in the work.

However, the ethnographic analysis of the data showed a rather different side of the daily practices. Its main result is that risks are not only managed and prevented, but also made and taken in action (see also Roe & Schulman, 2008, 114). What appears as rather planned and economic on the level of worker discourse is on closer ethnographic analysis constantly marked by the using of practical rules of thumb, skill, tacit knowledge, habits, team work and adapting to changing situational contexts. Rain, for example, increases heat consumption, and the setting of street lights increases electricity consumption, and the always unpredictable happening of these events requires improvisations from the technicians. Firing up an electricity generator, as another example, requires cautionary and skillful coordinations between the control room and the power plant before the economic decision of selling the energy can be made. Also the distribution control room has analogical tension between anticipation of uncertainties and improvisation in their respect: the work is highly standardized and follows law and protocols, but each fault situation is reportedly also different and requires creative adaptations by the technicians. This is perhaps also impacted by the control room being at the junction of several interconnected technical systems. Electricity blackouts may have repercussions in many other systems and provisions such as district heating and customers' household equipment. On the other hand, the risks of electricity supply and energy markets can be sparked by risks of other technologies such as telecommunications, district heating, building sites, maintenance and computers, in some cases also by household electricity supply. It is easy to assume that this places exceptional demands on the workers' abilities to act with respects the turbulent behaviors of diverse technological systems.

Conclusions

Assuming that contemporary risk stems from one common societal development, or that risk is always interpreted through the glens of fixed cultural interpretation models, is often relevant and provides important insights. But at the same time, arguably there is some attention to detail these perspectives may be omitting. This paper has documented that for experts and professionals, infrastructure risk is a construction that finds rather different local and situated figurations. The first case results that when national security, economic security, public health or public safety is at stake, infrastructure security experts withdraw at least partly from risk calculations and fall back on imagining the `worst hypothesis´ in a precautionary manner. The second case illustrates that in maintaining a large technological system, routine plans and calculations sometimes have to be abandoned for the active tinkering with risks. Based on these results, perhaps it is best to summarize infrastructure risk a contingent set of responses to larger problematizations (see Collier, Lakoff & Rabinow, 2004; see also Langumier, 2010). When problematizations change for example at the national policy level or at the working environment of electricity technicians, so must the risk responses, and even though it has not been documented by this research, perhaps one can assume that also the opposite effect is possible: that sometimes the routine deployment of risk responses can itself create new problems or even disasters (Langumier, 2010). This dynamic interrelationship between risk responses and larger problems I would argue merits further attention both with the research of infrastructures and broader debates about risks and anticipating the future.

References

Abele-Wigert, Isabelle & Dunn, Myriam (2006). International CIIP Handbook 2006: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies. Center for Security Studies, ETH Zurich.

Beck, Ulrich (1992). *Risk Society: Towards a New Modernity*. London: Sage.

Bowker, Georg & Star, Susan-Leigh (1999). *Sorting Things Out: Classification and its Consequences* . London: Polity.

De Bruijne, Mark (2006). Networked Reliability: Institutional Fragmentation and the Reliability of Service Provision in Critical Infrastructures. Dissertation for TUD Technische Universiteit Delft.

Callon, Michel; Lascoumes, Pierre & Barthe, Yannick (2009). *Acting in an Uncertain World: An Essay on Technical Democracy.* Cambridge: MIT Press.

Collier, Stephen (2006). Infrastructures and Reflexive Modernization. Presentation given at the Research Collegium of University of Helsinki.

Collier, Stephen & Lakoff, Andrew (2008). The Vulnerability of Vital Systems: How Critical Infrastructures Became a Security Problem. In Dunn Cavelty, Myriam & Kristensen, Kristian Søby (eds.) *Securing `the Homeland´: Critical Infrastructure, Risk and (In)security*. London: Routledge, 17-39.

Collier, Stephen; Lakoff, Andrew & Rabinow, Paul (2004). Biosecurity: Proposal for an Anthropology of the Contemporary. *Anthropology Today* 20 (5): 3-7.

Douglas, Mary & Wildavsky, Aaron (1982). *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers*. Berkeley—Los Angeles: University of California Press.

Edwards, Paul (2003). Infrastructure and Modernity: Force, Time and Social Organization in the History of Sociotechnical systems. In Misa, Thomas; Brey, Philip & Freeberg, Andrew (eds) *Modernity and Technology*. Cambridge: MIT Press, 185-225.

European Council (2008). On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection Directive 2008/114/EC.

Furedi, Frank (2006). *Culture of Fear Revisited*. Polity Books.

Giddens, Anthony (1990). *Consequences of Modernity*. Polity Books.

Graham, Stephen & Marvin, Simon (2002). *Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition.* London: Routledge.

Greimas, A. J. (1966/1980). *Strukturaalista semantiikkaa* . Tampere: Gaudeamus. Translated from French to Finnish by Eero Tarasti. French Original Sémantique structurale.

Kristensen, Kristian Søby (2008). `The Absolute Protection of our Citizens´: Critical Infrastructure Protection and the Practice of Security. In Dunn Cavelty, Myriam & Kristensen, Kristian Søby (eds.) *Securing `the Homeland´: Critical Infrastructure, Risk and (In)security*. London: Routledge, 63-83.

Kumpulainen, Lauri; Laaksonen, Hannu; Komulainen, Risto; Martikainen, Antti; Lehtonen, Matti; Heine, Pirjo; Silvast, Antti; Imris, Peter; Partanen, Jarmo; Lassila, Jukka; Kaipia, Tero; Viljainen, Satu; Verho, Pekka; Järventausta, Pertti; Kivikko, Kimmo; Kauhaniemi, Kimmo; Lågland, Henry & Saaristo, Hannu (2006). Visionary Network 2030: Technology Vision for Future Distribution Network. VTT Research Notes 2361.

Langumier, Julian (2010). Conclusion speech at Disasters and risks: from empiricism to criticism, a two-day international symposium at the CERI-Sciences Po & EHESS, 17th and 18th of June, Paris. France.

Roe, Emery & Schulman, Paul (2008). *High Reliability Management: Operating on the Edge* . Stanford: Stanford Business Books.

Silvast, Antti (2006). Keskeytyksestä kritiikkeihin: sähkönjakelun häiriöiden kokemuksia ja kohtaamisia. (“From Breakdown to Criticisms: Experiencing and Facing Electricity Supply Disturbances.”) Master's Thesis, University of Helsinki, Faculty of Social Sciences, Helsinki.

Silvast, Antti (2009). Riskiyhteiskunta ja merkityksenanto: sähkönjakelun häiriöiden semioottista tarkastelua. (“The Risk Society and Meaning Giving: Semiotic Investigation of Electricity Supply Disturbances.”) In Hannula, Erja & Oksanen, Ulla (eds.) *Murtuvat merkit: semiotiikan teoreettisen ja soveltavan tutkimuksen näkökulmia.* (“Breaking Signs: Perspectives for Theoretical and Applied Research in Semiotics.”) Helsinki: Palmenia, 187-198.

Sulkunen, Pekka & Törrönen, Jukka (1997a). *Semioottisen sosiologian näkökulmia. Sosiaalisen todellisuuden rakentuminen ja ymmärrettävyys*. (“Perspectives for Semiotic Sociology: The Construction and Meaning of Social Reality.”) Tampere: Gaudeamus.

Sulkunen, Pekka & Törrönen, Jukka (1997b). The Production of Values: The Concept of Modality in Textual Discourse Analysis. *Semiotica* 113 (1-2): 43–70.

Steenhuisen, Bauke (2009). Competing Public values: Coping Strategies in Heavily Regulated Utility Industries. Dis - sertation for TUD Technische Universiteit Delft.