Governance of Critical Infrastructures, Systemic Risks, and Dependable Software

Carsten Orwat[a], Christian Büscher[a], Oliver Raabe[b]

[a] Institute for Technology Assessment and Systems Analysis (ITAS) and
[b] Institute for Information and Economic Law (IIWR) at the
Karlsruhe Institute of Technology (KIT)

Technical Report
Karlsruhe, 2010

1 Introduction

Over the last two hundred years, researchers have observed a correlation between the evolution of large technical systems and functional systems in modern society. The provision of water and energy, the transportation of goods, the fast travel of persons or the communication with spatially distant persons have become basic features of modern society. Large technical systems are shaped by social processes and, vice versa, are shaping social processes. They are basic building blocks for industrial production, economic trade, communication or health care treatment, and many other fields or issues. Enabling the differentiation of functional systems like economics, science, law, politics, education, etc. and including the majority of the population with outputs and services, large technological systems are usually considered *infrastructure systems* (Mayntz 1993) and will be referred to in the following as *large technical infrastructure systems* (Mayntz 2009a).

Since the 1970s, one has also observed unintended and undesired consequences of large technical systems. The systems' underlying principles, for example those valid for power plants or large chemical plants, often demand large-scale and complex facilities whose technical operations and interactions are strictly separated from the remaining environment (human organisms, ecological systems). System reliability and safety become an increasing challenge for society. An intense discussion about the reliability of organizations running complex and dangerous technologies led to a 'High-Reliability-Organizational Theory' (La Porte 1981, 1982). Intelligent organisational design and management are considered to achieve safety in the context of large-scale high technology. The corresponding approach of 'Nearly-Error-Free Control Systems' emphasises the need for safety measures, prevention, anticipation, and extraordinary analytical methods to avoid failures when operating high-tech systems (La Porte 1982: 189). One approach of researchers is to favour intensive regulation in order to reduce risk and achieve safety. Other authors do not share this somehow 'optimistic' view and describe inherent limits of safety where non-linear interactions of system elements and a tight coupling of technical facilities lead to operation failures and loss of control. Additionally, the overall complexity of the system is increased by the implementation of technical, organizational or regulatory safety features (Perrow 1984; Sagan 1993).

Organization-oriented risk research has recently started to extend towards the interconnections and interdependencies among the technical and social elements of infrastructure systems, leading to approaches of *systemic risk* and *governance*. Today's discussions about systemic risks are concerned with the issue of dependability of outputs and services, the expectation of high efficiency and reliability in the development, implementation, and operation of large socio-technical systems, and the institutional settings in form of the interplay of government regulation and research funding, market coordination and deliberate decision-making.

With the widespread introduction and intensified use of information and communication technologies (ICT) as measures of operation and coordination in large technological infrastructure systems, a new quality of reliability issues arises. The extended—or even ubiquitous—use of software systems in future critical infrastructures provides many opportunities, especially to realise decentralisation and virtualization and to automate the plethora of transactions. On the other hand, software systems are never used in absolute safety so that additional risks can be added to critical infrastructures. With this in mind, software development and implementation become an issue for critical infrastructure protection (CIP) and critical information infrastructure protection (CIIP).

The use of software systems in critical infrastructures also causes changes in the governance structures and institutional arrangements of infrastructure systems. Vice versa, changes in institutional arrangements demand adaptations on the technology side. It is the task of technology assessment to analyse these technical and institutional structures with regard to the question whether they enable or endanger the relevant functions. The assessment of risks and dangers refers to the maintenance of a reliable operation of socio-technical systems or to the externalisation of negative consequences for other areas of the society.

In this paper, we depict the functions and impacts of the ubiquitous use of software systems in (future) critical infrastructure systems, emphasising that software could be seen as an institution and, thus, be part of institutional arrangements that govern critical infrastructures. This requires to set software institutions into relation with the given governance structures of critical infrastructures (Section 2). One proposition is that besides technical, organisational, and human sources also governance structures of the entire infrastructure system can be a source of risks. Governance structures provide the incentives and constraints for dealing with risks in the normal operation of a system or in case of failures. Thus, the dependability of software systems in critical infrastructures is also determined by the design of the governance structures (Section 3). Lastly, we sketch out research approaches, especially the role of technology assessment for analysing systemic risks and governance structures in future critical infrastructures, and highlight four particular research fields, i.e. the complexity in future critical infrastructures, the interconnectedness of future infrastructures, the coherence of technological and institutional practices, and the options of governance (Section 4).

2 Underlying Concepts: Software and Governance of Critical Infrastructures

2.1 ICT in Critical Infrastructures

Although there is no commonly used definition of '*critical infrastructure*' in the literature, most authors have used the term to refer to large-scale, networked socio-technical systems of energy, water, communication, and transportation (de Bruijne & van Eeten 2007; Kröger 2008; IRGC 2006). In this context, '*criticality*' of infrastructures could be understood as the manner of connectedness so that society's total vulnerability is focused to a few particular 'critical points' in the system (Hellström 2007: 427). With the extended use of ICT in critical infrastructures, also software systems became one of the critical points in infrastructure protection which is revealed by several examples of software failures and resulting significant losses in infrastructure systems (Jackson et al. 2007; Jackson 2009; Zhivich & Cunningham

2009). Software systems became a *key systemic element*, i.e. the dependability of entire infrastructure systems relies on the dependability of the embedded software systems. In this context, the many facets of software dependability—including functionality, performance, adaptivity, availability, fault tolerance, correctness, safety, security, privacy, and trustworthiness—set the scope of the multiple types of risks to be considered (cf. Avižienis et al. 2004).

We assume that, besides technical factors, the dependability of software in critical infrastructures is also a matter of market constellations, regulative frameworks, organisational structures, and human behaviour that influence the development and actual use of dependable software by operators who provide the critical infrastructure.[1] We understand the development and implementation of dependable software also as a matter of the governance structures and the design of incentives or constraints for developing, implementing, and running software in critical infrastructures.

While governance structures are necessary and decisive to obtain dependability of implemented software systems, they can also be sources of additional risks related to the use of software systems in critical infrastructures. Research has to consider that a large portion of institutional elements of the governance structures is programmed into software systems in order to realise the *'real-time' paradigm* of the *'virtualized' critical infrastructures*. In other words, institutional arrangements for enabling, steering, and controlling of the millions of transactions in future virtualized infrastructures have to be automated by software systems in order to be successfully handled. This means that institutions have to be transferred into software systems.

2.2 Software as an Institution

In general, *'institutions'* can be understood as established and prevalent social rules that structure social interaction (Hodgson 2006: 2). Institutions encompass legal rules, contracts, social norms, and conventions and their means of enforcement (North 1991, 1992, 2005; Ostrom 2005; Ménard & Shirley 2005; Hodgson 2006; Richter & Furubotn 1996). If institutions are applied, controlled and enforced, they create order in social interactions and reduce uncertainty, which can result from arbitrary or opportunistic behaviour. They create stable expectations of the behaviour of others. Besides constraining, they also enable behaviour and interactions among actors: Traffic rules, for example, enable (safe) traffic (Hodgson 2006: 2). Less uncertainty reduces the costs of transacting among each other, e.g. the costs of searching for, conducting, controlling or enforcing trading acts. Such transaction costs are determined by the level of certainty of transacting that depends on the existence and functioning of institutions preventing or reducing opportunistic behaviour (Williamson 1987). The shape of institutions determines the efficiency of trading, the degree of the division of labour, specialisation

[1] This assumption is partly based on previous research on risks of large technical systems emphasizing that organizational and societal errors within complex social processes have to be taken into account (e.g., Grabowski & Roberts 1996; Tervo & Wiander 2010).

and productivity. Therefore, existence and effectiveness of institutions are crucial factors of economic performance, societal wealth, and social development (North 1991, 1992).

Software systems increasingly regulate actions of individuals and interactions among them, with striking examples of Digital Rights Management (DRM) systems, e-commerce systems, or online cooperation tools. In critical infrastructures of the future, software systems will regulate transactions to an unprecedented level, especially if the paradigms of virtualisation and decentralisation will be fully realised.

Firstly, software systems technically enforce conventional institutions. DRM systems, for instance, convert contract terms into technically enforced usage restrictions. Secondly, with software systems, even new rules can be defined and enforced (Grimmelmann 2005; Lutterbeck 2008: 4). From this perspective, software systems include systems of formal rules that are either implemented by the software developer or imposed through system settings on users. With reference to the discussions of 'lex informatica' (Reidenberg 1998), 'code as law' (Lessig 1999), 'regulation by software' (Grimmelmann 2005) or 'regulation by machine' (Radin 2004), we can also speak of 'software as institution' (Orwat et al. 2010). Software systems normally interact with legal provisions, standards, contracts, conventions, and social norms (Wagner 2005). Together, such institutional elements provide the *institutional arrangements* and *governance structures* of critical infrastructures.

In contrast to conventional institutions like social norms, conventions, contracts, and legal provisions, software institutions have some specific characteristics (Grimmelmann 2005; Reidenberg 1998; Lessig 1999; Shah & Kesan 2003; Brousseau 2006; Zittrain 2008):

(1) Software systems enforce rules automatically. While this feature is the necessary precondition of efficient transactions in virtualized and decentralised infrastructures, it is also a potential source of failure propagation without a chance of human intervention.

(2) Software acts immediately and directly and without ex post interpretation e.g. by courts. Which options users have is defined ex ante, and forbidden behaviour is technically made impossible.

(3) Software is plastic and precisely malleable. This allows establishing rule systems in a high level of detail and in complex settings for which conventional institution types could be too onerous.

(4) Increasingly, software regulates in a 'context-aware' way, for example, depending on changeable surroundings or situations of users. Therefore, there may be more differentiated and sophisticated types of rules that adapt to the specific contexts.

(5) Software institutions are dynamic. By updating software systems, the embedded rules can be changed. The development of software follows a software-specific logic including economic and technical objectives, and is not the result of societal processes as is the case with the most conventional institutions.

(6) Software acts partly unnoticed. Secondary functions of software systems, such as data mining, can be run unnoticed by the end user.

On the one hand, automation, immediacy and plasticity are the advantageous features of software for transferring transactions in critical infrastructures to software systems. Economic and social transactions that would otherwise be impeded by the difficulties encountered when erecting an institutional framework, become possible, efficient, and effective.

On the other hand, there is a flipside to the embedding of institutions in software. If software development, implementation, and the software-technical realisation of rules are not coherent with the expectations of users or affected actors as well as with the existent institutional framework, the individual acceptance and the societal acceptability of the software systems are endangered. Here, DRM systems with the software-based definition and enforcement of usage rights of digital products (e.g., digital music, videos, or eBooks) give a controversial example. Concerns exist that with such a technical definition and enforcement a new (quasi) 'law' is set up by private actors, which might collide with statutory law or with the usage expectations of consumers (Lessig 1999; Samuelson 2003; Helberger 2006; Mulligan et al. 2003).

2.3 Governance in General

While there are different origins and understandings of '*governance*' in theory and practice, governance, for the purpose of our research, can be understood as collective decision-making and coordination in situations with different degrees of involving a variety of public, semi-public or private actors (Chhotray & Stoker 2009). The chosen governance mode determines the choices of policy goals, instruments, and modes of implementation (Howlett 2009). Through the realisation of governance modes, governing actors make use of, shape or abolish institutional arrangements or establish new ones.

The modes of governance may range from self-regulation by private actors to diverse forms of cooperation among public and private actors (e.g., public-private partnerships) to regulatory activities by governments as main actors (e.g. Mayntz 2008; Schuppert 2008). Some authors emphasise that governance expresses a polycentric, network-like decision-making of actors, including governmental actors, with heterogeneous interests (Rhodes 1996; Stoker 1998; Chhotray & Stoker 2009). Furthermore, governance often takes place concurrently at multiple levels such as local, regional, national, supranational or global levels (e.g., Bache & Flinders 2004). However, the multitude of actors involved in governance and, especially, the inclusion of non-governmental actors in public decision-making causes several problems such as a higher degree of complex interdependence among governing actors, blurring of responsibilities, or difficulties about accountabilities (Stoker 1998; Howlett 2009).

In general, governance structures are needed in order to prevent or correct coordination and provision failures of pure market approaches ('market failures') such as social costs, public goods, natural monopolies, ruinous competition, problems of common pool resources, or information asymmetries (e.g., Ewers & Fritsch 1987). A further need for governance can result from the necessity to stimulate the generation of scientific and technological knowledge and the provision of technological innovations, if private actors have no sufficient incentives to do so. Governmental intervention is the 'classical' response to market failures but the notion of 'governance' refers to situations in which civil parties, private firms, private associations or semi-public actors such as standardization organizations, supplement or substitute governmental actors in self-regulating or cooperative approaches.

Although the outcome of political processes—as the resulting governance structure—is no longer calculated and shaped by a single actor alone, intervention of governments is in some cases required and has (sometimes limited) options to influence the outcomes. There are rationales for the governmental measures of technology policy, in particular, because governments cannot be substituted in their function of making legitimate collectively binding decisions (Grunwald 2000: Chap. 3, 2008: 357ff.). Furthermore, governments are often seen as actors of 'last responsibility' (Leibfried 2008).

On the other hand, if weaknesses of direct regulation by governments can be assumed, governments can delegate responsibility to self-regulating governing actors. This may be relevant in cases where there is rapid technological development (Heil 2001: 129) like it is expected for future infrastructure systems. In such cases, governments may have a lack of information and expertise which would be required for an effective direct regulation. Such information and expertise can often be found only at the level of the sub-system (Grimm 2001). In particular, governments normally have a deficit to forecast dynamic technological developments and implementations, which would be required to shape *ex ante* the regulation of technologies (Ladeur 2000). Self-regulation, thus, would be better able to flexibly react to new technical developments (Büllesbach 2005: 14ff.) and would be more 'open' to innovation (*Innovationsoffenheit*).

Although the spectrum of actual realisations of self-regulation may be considerably broad, ranging from full self-regulation to governmental steering (Hoffmann-Riem & Schneider 1998: 406), governments, according to the concept of 'regulated self-regulation', can have roles in setting up a regulative framework for self-regulation and providing a kind of 'safety net responsibility' (*Auffangverantwortung*) if self-regulation fails (Hoffmann-Riem 1998: 537). In such cases, governments can allocate responsibilities for coordination to private or semi-private actors, keep oversight, and intervene if considerable wrong turns of self-regulation become evident (Vesting 2003).

2.4 Governance of Infrastructure Systems

Historically, the importance of infrastructure systems like telecommunication, rail transport, or electricity has been justifying that the state owned, funded research and development and investments in the infrastructures. Especially the security of supply for the society (*Daseinsvorsorge*) has to be guaranteed by the state on the basis of legal obligations. In addition, also economic arguments, such as the infrastructures' features of natural monopolies, network effects, vertical exclusion, or ruinous competition provide rationales for governmental intervention and supply (e.g., Assaf 2007; Finger & Varone 2009; for network industries see, Spulber & Yoo 2009). The dominant organizational model was the "... publicly owned or regulated, integrated national monopoly ..." (Mayntz 2009a: 126).

Since 'liberalisation' and privatisation came up in the 1980s and 1990s, infrastructure systems have no longer been governed by a single actor alone but by structures of multiple actors. Thus, current policies for critical infrastructures resemble more the situation of *'governance'* rather than hierarchical authority structures (Mayntz 2009b). Internet governance can be seen as an example of governance of a large infrastructure system in which governmental interventions are marginal by setting the legal framework. Instead, self-regulation by private organisation is prevalent (Bygrave & Bing 2009; Brousseau 2006).[2]

Some of today's critical infrastructures are characterised by *institutional fragmentation* by the unbundling of functions that were previously integrated into a single organisation, such as the institutional separation of production from network operation in the electricity industry (e.g., Finger et al. 2005; Kiesling 2009). Institutional fragmentation brings in new actors and enhances the overall complexity, which has implications for the reliability and security of their networks and services (Personick & Patterson 2003; Abele-Wigert 2006; de Bruijne & van Eeten 2007). With regard to infrastructures, analyses of the British railway accidents and power outages in the USA and Europe revealed governance failures accompanied by technical failures (van der Vleuten & Lagendijk 2010; Künneke & Finger 2007). The Y2K problem was also an example of a global technical problem with no means of central authoritative governance to push for adequate response (Büscher 2004; Quigley 2008).

Correspondingly, in these infrastructures, *public-private partnership* (PPP) now is the dominant organisation model that has implications for the treatment of risks (Dunn-Cavelty & Suter 2009; Mills et al. 2008) because different from the primary public concern of "safety first" (at any cost), private actors have to calculate an economically reasonable risk optimum that may deviate from the safety optimum. Additionally, governmental actors that are involved in public-private partnerships are dependent on the expertise of developers and operators (Dunn-Cavelty & Suter 2009). This dependence is increasing ever more with the extended use of software in critical infrastructures. Therefore, governance structures with a changed role of governments must be adapted to changed structures of expertise and knowledge (see Section 2.3).

Motivations and structures of governance of the electricity, transport and cloud computing infrastructures differ widely: Sectors with regulation, de-regulated sectors, self-regulated sectors, and in most cases a mixture of these can be observed. In any case, governments are no longer the only actors. While the future Smart Grid is increasingly being decentralised through the political motivations of liberalisation and privatisation as well as of energy-saving ('top-down'), the governance of cloud computing is mainly one of self-governance by market actors in a 'bottom-up' approach. However, private self-governance can be supplemented or substituted by governmental interventions if required on account of societal defects (see Section 2.3).

[2] The main Internet governance actors are the Internet Society (ISOC), Internet Architecture Board (IAB), Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), Internet Assigned Numbers Authority (IANA), and the Internet Corporation for Assigned Names and Numbers (ICANN), see for an overview and discussion (Bygrave & Michaelsen 2009).

3 State of the Art: Risks in Software-Based Critical Infrastructures

3.1 Systemic Risks and Governance Failures

One of the tasks of technology assessment is to identify risks of technology developments and develop options to cope with them (e.g., Grunwald 2009). Currently, analyses of technology assessment are also extended to systemic risks (Hellström 2009; Klinke & Renn 2006; Renn & Keil 2008; Keil et al. 2008). In general, analyses of systemic risks are given impetus by the recent financial crises, and thus the majority of studies can be found in the field of financing and banking (e.g. Goldin & Vogel 2010; Allen & Saunders 2004; overviews by Dow 2000; De Bandt & Hartmann 2000). Only a few studies focus on systemic risks in critical infrastructures, often outlining future research needs, approaches, and concepts (Hellström 2007; Bartle & Laperrouza 2008; Laperrouza 2009; Mellstrand & Ståhl 2009).

For our research purpose, *systemic risks* can be understood as a phenomenon in which, through contagion and cascading, failure of a system component leads to the dysfunction of the entire system or large parts of it (e.g., OECD 2003; Kaufman & Scott 2003; Kambhu et al. 2007). In order to better understand systemic risks, it seems useful to refer to a heuristic developed by Charles Perrow (Perrow 1984, 2008). It helps to explain that systemic risks can emerge in situations with complex (non-linear) interactions and tight coupling of system components, even when the technical system is designed with linearity in causal relations and with de-coupling or loose coupling of its elements. Tight coupling means a close arrangement in space and time of dependent elements of systems. These elements are arranged without slack or buffer. Failures happening to one unit immediately affect other units. This is typical of all facilities working in a closed 'containment'.

Furthermore, instead of the expected linear interactions, technical systems have shown unexpected complex interactions. One of many examples is the interaction between the o-ring seals of the Challenger Space Shuttle and the cold temperatures on launch day that lead to the disastrous chain reaction now known as the 'Challenger launch decision' (Vaughan 1996). A situation of complex interactions hinders a description, planning, and controlling of technical processes in the form of causal schematics and decreases the possibilities of an anticipation of negative consequences.

This understanding of systemic risks is in contrast to occasional damages by defects or inappropriate behaviour of individuals. It is a feature of systemic risks that systems *inherently within their normal functioning and reproduction* concurrently cause conditions that may endanger the entire system. We assume that single events can propagate into systemic events if the system structures are shaped to enable this.

With the continuous differentiation of society, complex structures with autonomous acting agents—but with interdependent impacts—become ubiquitous. In particular, the analyses of the financial crisis have revealed that systemic risks are a *multi-causal and mutual-causal phenomenon* determined by self-enforcing processes as virtuous and vicious circles (e.g., Krugman 2008). Systemic risks stem from many simultaneously occurring, mutually influencing events. In the financial sector, systemic risks result from mechanisms inherent to the economic rationale: A highly symbolic exchange medium in the form of money leading to 'innovative' financial transactions, encouragement of risk taking and risk hiding in the financial system, and automated IT-supported trading, combined with recent trends of deregulation of financial innovations and misaligning of incentives for actors involved in risk sharing and risk shifting. Since some of the causes are determined by the institutional structure of the financial sector, systemic risks can also be seen as the result of *governance failures* or failures of the structure of institutional arrangements, respectively (Dow 2000; Kaufman & Scott 2003; Goldin & Vogel 2010).

However, insights about systemic risks in the banking and finance sector cannot easily be transferred to infrastructure sectors. As for a comparison between the financial system and energy systems, Bartle and Laperrouza (2008) see differences and similarities in the extent of damage, the time of error propagation, and in the degree of uncertainties concerning systemic risks. While the extent of possible damages in the financial systems could reach a global magnitude, the possible damage in socio-technical energy supply systems supposedly reaches a regional, sometimes a national and in rare cases a continental magnitude. A possible spreading of failures or damaging events through the respective networks could occur rapidly in both cases. For the financial systems, it is conceivable, that a crisis situation leads to an endangerment of the whole economic system itself and, therefore, of the whole society. Such a catastrophe in the sense of an irreversible change in the state of affairs of the financial sector could lead to a reorganization of the coordination mechanisms of financial transactions and of governance structures. For the existing energy supply systems, the consequences of a system-wide damaging event are potentially high but normally bounded and constrained having rather the effect of a 'repair' than a reorganisation.

3.2 Software and Governance Risks in Critical Infrastructures

Governance structures of critical infrastructures can be sources of risks if inadequate incentives for risk prevention or risk distribution are given or if cooperative risk governance solutions do not exist or function sub-optimally. This is relevant for infrastructure provision as well as for software development and implementation.

The dominant model in today's infrastructure provision is the *public-private partnership* model. This model is characterised by different incentives of public and private actors affecting the dependability of critical infrastructures. Initial negative experiences with the public-private partnerships (de Bruijne & van Eeten 2007) and with 'liberalisation' in infrastructure provision (Laperrouza 2009) suggest that an extended governance model for critical infrastructure protection is needed involving manifold actors owing and being responsible for the operation of critical infrastructures (Dunn-Cavelty & Suter 2009; Sajeva & Masera 2006).

Most IT systems in critical infrastructures are maintained and operated by private actors. Insights from risk research indicate that risks of information systems in critical infrastructures can stem from low incentives for investments in IT security by for-profit entities (Haimes et al. 2008; Tervo & Wiander 2010). In general, *behavioural research and economics of software security* reveal that (especially private) software users do not install absolute software security, but implement an optimisation strategy taking into account security investments and operation costs on the one side as well as security improvements and possible competitive advantages due to high security reputation on the other side (e.g., Gordon & Loeb 2004; Dynes et al. 2008). Also at the stage of software development, there is a balancing of costs and benefits of investing in software security (Arora et al. 2008). Software engineering processes include a trading off among system quality characteristics, meaning that external governance requirements (e.g., laws, regulations, and contractually obligated requirements) are not directly transposed into internal policies, procedures, and standards for software assurance but are compared with other aspects such as profitability or capacities (e.g., Croll 2010).

In systems made up by many actors, system reliability may also have the characteristics of a public good with the tendency that individuals 'free-ride' on the contributions by others and the overall result is inefficient (Varian 2004). Related to this, system security can also be regarded as an externality: A lack of security of one IT unit may have negative effects on other units (Camp & Wolfram 2004). If institutional frameworks do not demand other behaviour, security externalities result as a decision of individual actors by endangering the entire system with a suboptimal security level of one system component (Anderson & Moore 2006, 2009; van Eeten & Bauer 2008). To counteract the problems of public goods and externalities characteristics, several institutional mechanisms are discussed in theory and applied in practice, including information provisions, standard setting, or research and development funding (e.g., Camp & Wolfram 2004).

To conclude so far, we assume that systemic risks can result—besides from the technical design—from the institutional structures of socio-technical systems leading to inappropriate risk sharing or risk shifting. We assume that systemic risk may result from a mismatch of institutions and their incentives and controls in security and co-operation decisions of individual (rational) actors against the background of increasing complexity of critical infrastructure systems. However, an assessment of systemic risks becomes problematic. Due to the seldom occurrence of damages, the analysis of systemic risk is hampered by the lack of historic data (Kambhu et al. 2007: 38). In addition, there is a lack of experience of governance in areas with converging governance structures such as the emerging Smart Grid infrastructure, which is subject to regulatory provisions from the electricity, telecommunication, and ICT industries.

4 Research Agenda

4.1 Research Approach: Technology Assessment and Risk Analysis

Technology assessment provides the systematic procedures of scientific analyses of conditions and consequences of new technologies. It also provides procedures of policy analysis to derive coherent governing options (Grunwald 2002, 2009). The analysis of the chances and risks of new technologies is an elementary part of technology assessment. In contrast to market research conducted by enterprises, public technology assessment focuses on societal issues of new technologies which cannot be adequately solved by technology developers or market actors alone. In many cases, technology assessment, thus, explores the intended effects and unintended consequences of new technologies. It also explores the necessities and options of political interventions and of necessary adjustments of governance structures either to lower barriers for innovation and for societal acceptability or to influence the shaping of new technologies.

4.2 Research Focus: Complexity in Future Critical Infrastructures

Although ICT is already widely used in large technical systems for fine-tuned and enhanced operation of installed capacity (e.g., Nightingale et al. 2003), the proposed next generations of 'intelligent systems' should provide the functionalities to enable automated cooperation and coordination in order to further improve the utilisation of installed capacity resting in different stages of fragmented value chains. In future *virtualized* infrastructures, decentralised software-intensive control systems should enable the anticipative and real-time calculation, simulation, and planning of cooperative capacity utilisation and the temporal and seamlessly coordinated supply of products and services from different sources. Software systems should ensure dynamic adaptation to volatile supply and demand.

Virtualization can also be understood as the 'perfect realisation' of the 'just-in-time' paradigm, which means, per se, that there is a large number of couplings of functions and information flows that is itself prone to risks (Longstaff et al. 2000). Especially through *'real-time'* provision of functionality, the critical infrastructures will have a large number of couplings. Decentralisation with automated coordination and cooperation of software systems necessitates tight interconnections and interdependencies of subsystems. With the extended coordination layer of software systems above the functional levels of infrastructures, the complexity of critical infrastructures has been increasing and the interconnections and interdependencies among the elements have been developing into potential sources of risks. Due to the resulting complexity, the infrastructure systems may interact in unforeseen ways.

The technical control of these systems is a critical technical function of infrastructure systems. Future critical infrastructures are characterised by a high degree of *software-based automation of interactions and transactions* with large portions of rules written in software systems. This results not only in a considerable reliance on dependable software but also leaves less room for human interpretation and intervention. On the one hand, automation helps to exclude occasional human error, on the other hand it decreases the understanding of the complex processes and interconnections 'beneath the surface' during operation. A release from decisions goes hand in hand with a fade-out of possible consequences during operation, which have to be considered in advance at the stage or programming. As illustrated by computer trading of securities without human control, a potential of uncontrolled chain-reactions and non-linear processes emerges from automated decision-making (e.g., Goldin & Vogel 2010). In the field of organic computing (e.g., Müller-Schloer & Schmeck 2010), similar phenomena have been discussed recently and been analysed under the term of '*emergent phenomena*' or '*emergent behaviour*' that may show up as unanticipated and undesired behaviours in self-organising interactive IT systems.

The manner of development and implementation of software systems and the design of their interconnections become the crucial factors that determine the coordination structures that govern interactions in critical infrastructures but may also be the causes of systemic risks. The substitution of human decisions by software-based mechanisms means a redistribution of risks and responsibility into software development and application.

4.3 Research Focus: Interdependencies between Future Critical Infrastructures

Future critical infrastructures distinguish themselves from past ones by the fact that they converge with one another. Especially the layer of the critical information infrastructures is more and more implemented in a 'mega-infrastructure' (Amin 2005) of converging telecommunication, electricity, transport and computation infrastructures. The future infrastructures can be understood as a 'network of systems' or 'system of systems' with a plethora of interconnected heterogeneous systems run by a multitude of public or private actors with heterogeneous interests in security. In particular, future critical infrastructures are based no longer on proprietary networks, but on the Internet. For example, the realisation of the Smart Grid is based on the 'Internet of Things' and the 'Internet of Services'. Cloud Computing is largely based on Internet technologies. Among other things, this means that the dependability of critical infrastructures is also determined by risks of the Internet and the coordinating software.

We assume that *systemic risks* may, in particular, result from the coupling of different infrastructures. While risks within one infrastructure are subject to a long tradition of risk analysis and risk management, interdependencies between different critical infrastructures are rarely observed, with some exceptions (Rinaldi et al. 2001; IRGC 2006; Laprie et al. 2007; Haimes et al. 2008; Rosato et al. 2008; Panzieri & Setola 2008). Most research focus on single, non-interacting networks. However, a theoretical analysis with reference to the electrical blackout in Italy in 2003 reveals that especially the couplings of interdependent networks are prone to iterative cascading of failures (Buldyrev et al. 2010). In that case, the shutdown of power stations led to failures of nodes in the Internet communication network, which in turn led to further breakdowns in power stations (Buldyrev et al. 2010; Rosato et al. 2008; further examples given by: Bologna & Setola 2005).

Normally, engineering and optimisation of critical infrastructures are subject to local design. However, over the past two decades, infrastructures "... evolved globally through unplanned aggregation of isolated parts, adaptation to anticipated and unanticipated demands, and the transformation of services according to evolving social needs." (Vespignani 2009: 984) Therefore, critical infrastructures can be understood as *complex systems* "... for which it is generally impossible to abstract the global behaviour from the analysis of single components, especially under conditions such as failures and disasters." (ibid.) The application of network theory and theory of complex (adaptive) systems (e.g., Setola & De Porcellinis 2009; Eusgeld et al. 2009; Longstaff et al. 2000) helps to understand critical infrastructures as complex systems that are typically characterised by nonlinear relationships, multiple stable states, hysteresis, contagion, and synchrony (Kambhu et al. 2007: 30ff.).

The interdependencies between infrastructures are the factors allowing failures to propagate between infrastructures and to cause widespread disruption (Bologna & Setola 2005; Vespignani 2010). The many interdependencies of infrastructures can be roughly classified by (1) physical couplings of electricity, water or gas, or material flows, (2) logical and information couplings, (3) inter-regional economic couplings, and (4) inter-sector economic couplings (Haimes et al. 2008). It is worth noting that risk analysis explicitly goes beyond a pure engineering perspective taking into account financial dependencies, political coordination or governance structures.

First instances lead to the assumption that risk-relevant couplings in and between infrastructures are also influenced by economic interests such as cost savings, which might deviate from an engineering logic: Risks can stem from relying energy control systems on Internet connections and services (e.g., Nartmann et al. 2009). Also risk can result from the interest of software vendors to couple software products to gain market shares (Perrow 2008). Problems for the overall infrastructure security can also stem from the connection of SCADA systems[3] to the Internet or the use with insecure computer operation systems (Gold 2009). The increased openness of the SCADA architecture and the increased connectivity provide more functionality and potentials of cost reductions, but also considerably more vulnerability (Christiansson & Luiijf 2008; Anderson & Fuloria 2009b).

Another example for potential risks is that software systems will also be used for the collaborative stabilisation of the European ultrahigh voltage network. By this, software failures may cause cascading failures in the network, rendering the network operator also liable for software system failures besides the liability for, e.g., failures of the physical infrastructure.[4] This will pose serious challenges for the software quality, certification of software quality or options of insurance. This is particular relevant for the use of autonomous self-organising systems.

In future highly interconnected critical infrastructures, networks of actors are responsible for the dependability of data protection and security of ICT systems. For instance, involved actors are responsible for securing the data of other actors. However, the information technology risk is *inherently transitive*. Damage caused by lax information security or vulnerable products of one actor also causes damage to other actors that share the data or system. Negative externalities are exposed to other companies or individuals not responsible for the security of the system (Matwyshyn et al. 2010). Previous research suggests that most dependability problems of IT systems in critical infrastructures do not consist in hostile attacks or system-internal problems, but rather stem from surroundings with socio-economic and technical issues in complex system-of-systems developments that lack, for example, large-scale, holistic risk analysis and collaboration (Tervo & Wiander 2010).

[3] Supervisory Control and Data Acquisition (SCADA) systems are used in critical technical systems, such as nuclear power plants, electricity transmission and distribution systems or industrial production plants.

[4] See for Germany the changes in liability rules for infrastructure operators with the shift in the burden of proof.

From a dynamic perspective, future critical infrastructures can even resemble *complex adaptive systems*, in which the robustness "... has to emerge from the collective properties of individual units that make up the systems; there is no planner or manager whose decisions completely control the system" (Kambhu et al. 2007: 33 quoting statements by Simon Levin). These systems are 'adaptive' in the sense that not the entire system is adapting and adjusting itself in a coordinated way, but only some components of the system are adapting and changing (Kambhu et al. 2007: 32). Especially the lack of a 'central planner' challenges the engineering, optimisation and risk management of infrastructures and requires adequate types of governance. For instance, it is unclear whether systemic risks could emerge during the introduction of new software systems or the update of existing ones in a setting of a multitude of interconnected components of the infrastructure system. Systems of critical information infrastructures contain a large portion of legacy systems and a large number of third-party components also with many legacy systems (Mellstrand & Ståhl 2009).

4.4 Research Focus: Incoherence of Technical and Institutional Practices

Large technical infrastructure systems consist of multi-layered networks of physical and non-physical processes. We have to distinguish between the physical aspects of the production of outputs (e.g., energy provision) as well as the coordination of operations mainly by ICT on the one hand and the social processes of developing, implementing, operating, and regulating on the other hand. Institutional arrangements on how a technical system is governed and the technological settings are strongly interrelated.

From the dynamic perspective of a co-evolution of technologies and institutions, in particular the *coherence* between technological and institutional practices is needed to safeguard the critical technical functions like capacity management, system management, interconnection, and interoperability (Finger et al. 2005; Künneke & Finger 2007; Künneke 2008; Finger & Varone 2009; Künneke et al. 2010). For instance, while large parts of the institutional arrangement of the electricity sector underwent fundamental changes through 'liberalisation', deregulation, and privatisation, the characteristics of the technological structure of electricity networks have nearly remained the same.

On the one side, institutional reforms led to the unbundling of major parts of the value chain from a former vertically integrated entity into many independent organisations. Electricity production, trade, metering, and sales are now mainly organised under market conditions. However, private actors have less incentive to invest in large-scale energy production facilities so that the resulting relative low reserve margin causes risks (Künneke 2008: 234f.; Künneke & Finger 2007).

On the other side, the network-related activities of transmission and distribution are still under sector-specific regulation due to their natural monopoly characteristics. The network governance structure—driven by technology characteristics—is mostly still organised as a centralised integrated system with centralised planning, control and operation. However, the envisaged decentralised and more small-scale power production including renewable energy facilities, gas turbines, or combined heat and power plants (CHP) require a two-way structure of network governance with decentralised control systems that can manage multiple in- and outflows (Künneke 2008). The above-mentioned intelligent software-intensive control systems are developed to allow such a decentralised structure. They would enable the further technical disintegration of the electricity system, a decentralised coordination, and a reduction of the costs of transactions enabling also dynamic pricing (Amin & Wollenberg 2005; Kiesling 2009; Ilic & Jelinek 2009). It becomes possible that the future electricity infrastructure follow the 'Internet paradigm' as interconnected systems of semi-independent networks (Künneke 2008: 260; Nightingale et al. 2003). Therefore, in order to facilitate the envisioned technological changes in future critical infrastructures, i.e. the decentralised energy production as well as the decentralised and self-organising coordination, adequate adjustments and revisions of institutional governance structures are necessary (Künneke 2008; Künneke et al. 2010; Kiesling 2009; Rohracher 2007).

Additionally, all parts of the energy system from production to supply have to be technically balanced at any time to make electricity continuously available. However, such a technical system management is a pure collective good that is, normally, not provided by market solutions (Künneke 2008: 239). Thus, also with the use of decentralised intelligent control systems, adequate governance structures have to be found that ensure the provision of this collective good.

To sum up, research is necessary to continuously analyse the co-evolution of technological and institutional practices and make suggestions to enhance the coherence between both. With the conceptualisation of software as an institution, software systems become an analytical element in the striving for coherence between technological and institutional practices. From a dynamic perspective of institutional change (e.g., Streeck & Thelen 2005), research focus is on the substituting, complementing or reinforcing relationships between software-institution and conventional institutions.

4.5 Research Focus: Options of Governance

Governance structures provide the institutional incentives and constraints for the way of actual adoption and use of software systems, and, therefore, determine indirectly through the behaviour of the infrastructure operator the dependability of the software system and of the critical infrastructure. For instance, incentives are necessary for the operator to adequately disclose and share data on system failures (Matwyshyn et al. 2010; Assaf 2007) or to cooperate in inter-firm risk governance to prevent systemic risks (Dynes et al. 2008). Thus, research should investigate the existing governance structures, decision processes, actors involved in developing and implementing software, and their underlying behavioural motivations and constraints, in order to derive insights on adequate governance structures, procedures, and instruments.

Especially, research has to consider the different levels of information and expertise spread among the actors involved. Although necessary for standardisation purposes or to shape ex ante appropriate regulation, the possibilities to forecast technological developments are limited due to knowledge deficits. Participation with the utilisation of decentralised prognosis knowledge is suggested to mitigate such deficits. Governance structures are required that stimulate the adequate revelation and exchange of information and expertise, taking into account that public and private actors have different motivations, procedures, options and limitations to acquire, process, and utilise such information and expertise.

As mentioned above, software systems increasingly regulate transactions within organisations and, in particular, between them as well as the possibilities of access and usage of data and information. Normally, only a single actor or a small group made decisions in software development and implementation. They are usually not subject to democratic control. The more software regulates aspects of our life—especially when collectively binding decisions are embedded in software that cannot be easily circumvented or negotiated by affected parties[5]—the more issues of public legitimacy of the emerging software institutions result and the more could one ask whether more societal actors should be able to participate in and influence the development and implementation of software. In addition to criteria of technical system integrity (i.e. resilience and robustness) and economic performance (i.e. static or price efficiency, dynamic efficiency or 'innovation openness', and systemic efficiency), also public values have to be considered. It should be questioned how *public values* could be embedded in software systems. The coherence of the technical and institutional governance determines the functioning of infrastructure systems with regard to the economic and technical criteria as well as the public values (Finger et al. 2005).

Public values concerning infrastructures encompass (a) from the consumers' perspective the 'Universal Service' criteria, including quality, accessibility, affordability, and reliability and (b) from the collective perspective the criteria of security of supply, national security, social and environmental protection (Finger et al. 2005). With the extended and intensified use of ICT, the inclusion of public values concerning ICT in analyses gets more important. These may include values of privacy and data protection, integrity of personal systems and components, adequate intellectual property rights, prevention of misuse and computer crime, societal acceptable changes in working conditions, adequate user interfaces and feedbacks, etc. It seems intuitive that public values need to be embedded at the stage of software development and application. If infrastructures and software have to be regulated—which seems not to be necessary in any case—, regulation has to be shifted towards the software development and application stages. This is exemplified by Smart Grid developments, where 'smart' electricity metering considerably utilises personal data and researchers suggest adaptations of privacy protection regulations (Anderson & Fuloria 2010; Raabe et al. 2010).

Several technology studies point to limitations of societal steering or shaping of technological developments and institutional evolution due to path dependence, resistance to change, or complexities of decision situations (e.g., Mayntz 2008; Grunwald 2000). Furthermore, in future infrastructure systems, the interactions are among a large and unpredictable number of more or less autonomous actors—some in a self-organised manner—and, thus, the behaviour of the entire infrastructure system is less predictable since coordination is not provided and guaranteed by a single actor. Instead, a multitude of actors with heterogeneous

[5] A similar and relevant discussion has been started for ubiquitous computing (e.g., Spiekermann & Pallas 2006).

interests and including many institutional arrangements at sub-levels of coordination provide and maintain diverse governance schemes (see Section 2.3).

However, although limited there remain certain societal options to steer technological developments and to adjust governance structures. In particular, in many infrastructure sectors—but also to a certain extent within the software sector (Shah & Kesan 2003; Kesan & Shah 2005)—policy instruments including funding of research and development as well as education, governmental procurement, standardisation, certification and information provision, liability rules, intellectual property rights or direct regulation have relevance. Furthermore, several security regulations apply to companies in general and infrastructure operators in particular (e.g., Dynes et al. 2008).

For future critical infrastructures, such policy instruments have to be reconsidered in view of ongoing technological and governance changes as well as the converging technological and governance spheres. Difficulties of policy measures in the software sector can be transferred to infrastructure sectors. For instance, the (further) *standardisation* of software and infrastructure elements is of basic importance to obtain and secure software quality and software interoperability. However, standardisation—especially in the software industry—is plagued with problems of the dominance of proprietary standards and 'standard wars' (e.g., Shapiro & Varian 1999), the importance of early phases of standardisation due to strong path dependence and 'lock-ins' due to the high switching costs (e.g., David & Greenstein 1990), hurdles for participation in standardisation procedures (Werle & Iversen 2006; Orwat et al. 2010), tensions between interoperability and product diversity, or tensions with goals of competition policy (e.g., Calderini & Giannaccari 2006).

As another example, also *certification of software dependability*, as one often favoured policy instrument for software security[6], is controversially discussed (Anderson & Fuloria 2009a, 2009b). Many certification schemes for software dependability examine the existence of standard proof procedures and not the evidence of the actual fulfilment of dependability goals (Jackson et al. 2007; Jackson 2009: 80). In order to become credible, certification schemes have to fulfil several requirements with regard to the independence of auditors, fee structures, audit and sanction mechanisms, and means to exclude moral hazard (e.g., Jahn et al. 2005). For future infrastructures it is also problematic that the focus of certification schemes is mainly local and does not include systemic risks that stem from the interconnections within and between infrastructures.

5 Conclusions

We assume that risks and systemic risks in future critical infrastructures are a multi-causal and mutual-causal phenomenon, resulting from risks of non-dependable software, risks of

[6] See, for instance, the ISO/IEC 27002 Information Security Standard, including Certification, the 'Common Criteria' Certification scheme, or the BSI-Standards zum Informationssicherheitsmanagement, IT-Grundschutz-Katalog.

inappropriate governance structures of critical infrastructures, and especially their interconnections. Research should analyse—especially by focussing on the interrelations between technical, institutional and human system components—whether technical and governance structures are sources of systemic risks. It should contribute insights to the optimisation of governance structures to reduce risks, to enhance the societal acceptability and to provide recommendations for the development and implementation of software systems. We assume that systemic risks in critical infrastructure systems have their origins in both the technical and their organisational and governance design. Governance structures provide the incentives and social constraints for the treatment of risks.

The proposed research emphasises four features of future critical infrastructures: (1) Rules of governance structures are increasingly technically realised by software systems, i.e. rules regulating transactions in and between critical infrastructures are embedded in and enforced by software systems. The appropriate design of relationships between 'software-institutions' and conventional institutions can be decisive for the societal acceptability of the emerging infrastructure system. (2) Critical infrastructure systems increasingly converge, in particular, by their reliance on the critical information infrastructure including the Internet. This may create new chances but also new risks that are beyond the focus of usual risk analyses. (3) The coherence of technological and institutional practices determines the fulfilling of technical criteria like reliability, economic performance criteria like dynamic efficiency and public values like privacy protection. Software systems with their technical and institutional characteristics are central in the search for coherence. (4) With the embedding of governance rules into software systems, the governance structures and policy instruments of the software industry play a crucial role for the already converging governance structures of critical infrastructures. All in all, however, both the analysis of systemic risks in future critical infrastructures and the analysis of the converging governance structures are still in their infancy.

References

Abele-Wigert, I. (2006): Challenges Governments Face in the Field of Critical Information Infrastructure Protection (CIIP): Stakeholders and Perspectives, in: Dunn, M.; Mauer, V. (eds.): International CIIP Handbook 2006, Vol. II - Analyzing, Issues, Challenges, and Prospects, Zürich: ETH Zürich, Center for Security Studies.

Allen, L.; Saunders, A. (2004): Incorporating Systemic Influences Into Risk Measurements: A Survey of the Literature, in: Journal of Financial Services Research, Vol. 26, No. 2, pp. 161-191.

Amin, M. (2005): Infrastructure security: Reliability and dependability of critical systems, in: IEEE Security and Privacy, Vol. 3, No. 3, pp. 15-17.

Amin, S.M.; Wollenberg, B.F. (2005): Toward a smart grid, in: IEEE Power and Energy Magazine, Vol. 3, No. 5, pp. 34-41.

Anderson, R.; Fuloria, S. (2009a): Certification and evaluation: A security economics perspective, ETFA 2009 - 2009 IEEE Conference on Emerging Technologies and Factory Automation, available online at: http://www.cl.cam.ac.uk/~rja14/Papers/certi_eval.pdf, last access at 2010-09-29.

Anderson, R.; Fuloria, S. (2009b): Security Economics and Critical National Infrastructure, The Eighth Workshop on the Economics of Information Security (WEIS 2009), University College London, England, 24-25 June 2009, available online at: http://www.cl.cam.ac.uk/~sf392/publications/WEIS-2009.pdf, last access at 2010-09-29.

Anderson, R.; Fuloria, S. (2010): On the security economics of electricity metering, Cambridge: Cambridge University, available online at: http://www.cl.cam.ac.uk/~rja14/Papers/meters-weis.pdf, last access at 2010-09-26.

Anderson, R.; Moore, T. (2006): The Economics of Information Security, in: Science, Vol. 314, No. 5799, pp. 610-613.

Anderson, R.; Moore, T. (2009): Information security: where computer science, economics and psychology meet, in: Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, Vol. 367, No. 1898, pp. 2717-2727.

Arora, A.; Frank, S.; Telang, R. (2008): Estimating Benefits from Investing in Secure Software Development, webpage published by "Build Security In" initiative of the U.S. Department of Homeland Security, available at: https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/business/267-BSI.html, webpage version of 2008-11-12, last access at 2010-09-29.

Assaf, D. (2007): Government Intervention in Information Infrastructure Protection, in: Goetz, E.; Shenoi, S. (eds.): Critical Infrastructure Protection, Heidelberg et al.: Springer, pp. 29-39.

Avižienis, A.; Laprie, J.C.; Randell, B.; Landwehr, C. (2004): Basic concepts and taxonomy of dependable and secure computing, in: IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 1, pp. 11-33.

Bache, I.; Flinders, M.V. (2004): Multi-Level Governance, Oxford, New York: Oxford University Press.

Bartle, I.; Laperrouza, M. (2008): Systemic risk in the network industries: is there a governance gap?, 5th ECPR general conference, Potsdam University, September 10th -12th, 2009, Potsdam; published by Centre for the Study of Regulated Industries, School of Management, University of Bath, available online at: http://infoscience.epfl.ch/record/142565/files/Bartle%20Laperrouza%20ECPR%20Sept09%20systemic%20risk.pdf, last access at 2010-09-29.

Bologna, S.; Setola, R. (2005): The need to improve local self-awareness in CIP/CIIP, First IEEE International Workshop on Critical Infrastructure Protection; published by IEEE.

Brousseau, E. (2006): Multi-level governance of the digital space: does a "second rank" institutional framework exist?, in: Brousseau, E.; Curien, N. (eds.): Internet and Digital Economics, Cambridge: Cambridge University Press, pp. 617-648.

Buldyrev, S.V.; Parshani, R.; Paul, G.; Stanley, H.E.; Havlin, S. (2010): Catastrophic cascade of failures in interdependent networks, in: Nature, Vol. 464, No. 7291, pp. 1025-1028.

Büllesbach, A. (2005): Selbstregulierung im Datenschutz, in: Recht der Datenverarbeitung, Vol. 1, No. Sonderbeilage, pp. 13-17.

Büscher, C. (2004): Handeln oder abwarten? Der organisatorische Umgang mit Unsicherheit im Fall der Jahr-2000-Problematik in der IT, Wiesbaden: Deutscher Universitäts-Verlag.

Bygrave, L.A.; Bing, J. (Eds.) (2009): Internet Governance. Infrastructure and Institutions, Oxford: Oxford University Press.

Bygrave, L.A.; Michaelsen, T. (2009): Governors of Internet, in: Bygrave, L.A.; Bing, J. (eds.): Internet Governance. Infrastructure and Institutions, Oxford: Oxford University Press, pp. 92-125.

Calderini, M.; Giannaccari, A. (2006): Standardisation in the ICT sector: The (complex) interface between antitrust and intellectual property, in: Economics of Innovation and New Technology, Vol. 15, No. 6, pp. 543-567.

Camp, L.J.; Wolfram, C. (2004): Pricing Security, in: Camp, L.J.; Lewis, S. (eds.): Economics of Information Security, Dordrecht: Kluwer, pp. 17-34.

Chhotray, V.; Stoker, G. (2009): Governance Theory and Practice: A Cross-Disciplinary Approach, Basingstoke, New York: Palgrave Macmillan.

Christiansson, H.; Luiijf, E. (2008): Creating a European SCADA Security Testbed, in: Goetz, E.; Shenoi, S. (eds.): Critical Infrastructure Protection, IFIP International Federation of Information Processing, Vol. 253, New York: Springer, pp. 237-247.

Croll, P.R. (2010): System and software assurance - Rationalizing governance, engineering practice, and engineering economics, 2010 IEEE International Systems Conference Proceedings, SysCon 2010.

David, P.A.; Greenstein, S. (1990): The Economics Of Compatibility Standards: An Introduction To Recent Research, in: Economics of Innovation and New Technology, Vol. 1, No. 1, pp. 3-41.

De Bandt, O.; Hartmann, P. (2000): Systemic risk: A survey, European Central Bank, Working Paper Series, Working Paper No. 35, Frankfurt am Main: European Central Bank, available online at: https://www.ecb.int/pub/pdf/scpwps/ecbwp035.pdf, last access at 2010-09-29.

de Bruijne, M.; van Eeten, M. (2007): Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment, in: Journal of Contingencies and Crisis Management, Vol. 15, No. 1, pp. 18-29.

Dow, J. (2000): What is systemic risk? Moral hazard, initial shocks, and propagation, in: Monetary and Economic Studies, Vol. 18, No. 2, pp. 1-24.

Dunn-Cavelty, M.; Suter, M. (2009): Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection, in: International Journal of Critical Infrastructure Protection, Vol. 2, No. 4, pp. 179-187.

Dynes, S.; Goetz, E.; Freeman, M. (2008): Cyber Security: Are Economic Incentives Adequate?, in: Goetz, E.; Shenoi, S. (eds.): Critical Infrastructure Protection, IFIP International Federation of Information Processing, Vol. 253, New York: Springer, pp. 15-27.

Eusgeld, I.; Kröger, W.; Sansavini, G.; Schläpfer, M.; Zio, E. (2009): The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures, in: Reliability Engineering and System Safety, Vol. 94, No. 5, pp. 954-963.

Ewers, H.-J.; Fritsch, M. (1987): Zu den Gründen staatlicher Forschungs- und Technologiepolitik, in: Herder-Dornreich, P. (ed.): Jahrbuch für neue politische Ökonomie, Tübingen: Mohr (Siebeck), pp. 108-135.

Finger, M.; Groenewegen, J.; Künneke, R. (2005): The Quest for Coherence Between Institutions and Technologies in Infrastructures, in: Journal of Network Industries, Vol. 6, No. 4, pp. 227-261.

Finger, M.; Varone, F. (2009): Regulatory Practices and the Role of Technology in the Network Industries: The Case of Europe, in: Künneke, R.W.; Groenewegen, J.; Auger, J.-F. (eds.): The Governance of Network Industries: Institutions, Technology and Policy in Reregulated Infrastructures, Cheltenham and Northampton: Edward Elgar, pp. 87-101.

Gold, S. (2009): The SCADA challenge: securing critical infrastructure, in: Network Security, Vol. 2009, No. 8, pp. 18-20.

Goldin, I.; Vogel, T. (2010): Global Governance and Systemic Risk in the 21st Century: Lessons from the Financial Crisis, in: Global Policy, Vol. 1, No. 1, pp. 4-15.

Gordon, L.A.; Loeb, M.P. (2004): The Economics of Information Security Investment, in: Camp, L.J.; Lewis, S. (eds.): Economics of Information Security, Dordrecht: Kluwer, pp. 105-127.

Grabowski, M.; Roberts, K.H. (1996): Human and organizational error in large scale systems, in: IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, Vol. 26, No. 1, pp. 2-16.

Grimm, D. (2001): Selbstregulierung in der Tradition des Verfassungsstaates, in: Hoffmann-Riem, W. (ed.): Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates. Ergebnisse des Symposiums aus Anlaß des 60. Geburtstages von Wolfgang Hoffmann-Riem, Berlin: Duncker & Humblot, pp. 9-20.

Grimmelmann, J. (2005): Regulation by Software, in: Yale Law Journal, Vol. 114, pp. 1721-1758.

Grunwald, A. (2000): Technik für die Gesellschaft von morgen. Möglichkeiten und Grenzen gesellschaftlicher Techniksteuerung, Frankfurt, New York: Campus.

Grunwald, A. (2002): Technikfolgenabschätzung - eine Einführung, Berlin: Sigma.

Grunwald, A. (2008): Technik und Politikberatung. Philosophische Perspektiven, Frankfurt am Main: Suhrkamp.

Grunwald, A. (2009): Technology Assessment: Concepts and Methods, in: Meijers, A. (ed.): Handbook of the Philosophy of Science, Volume 9: Philosophy of Technology and Engineering Sciences, Amsterdam et al.: Elsevier/North Holland, pp. 1103-1146.

Haimes, Y.; Santos, J.; Crowther, K.; Henry, M.; Lian, C.; Yan, Z. (2008): Risk Analysis in Interdependent Infrastructures, in: Goetz, E.; Shenoi, S. (eds.): Critical Infrastructure Protection, IFIP International Federation of Information Processing, Vol. 253, New York: Springer, pp. 297-310.

Heil, H. (2001): Datenschutz durch Selbstregulierung – Der europäische Ansatz, in: DuD - Datenschutz und Datensicherheit, Vol. 25, No. 3, pp. 129–134.

Helberger, N. (2006): Code and (intellectual) property, in: Dommering, E.; Asscher, L.F. (eds.): Coding Regulation. Essays on the Normative Role of Information Technology, Information Technology and Law Series, No. 12, The Hague: T.M.C. Asser Press, pp. 205-248.

Hellström, T. (2007): Critical infrastructure and systemic vulnerability: Towards a planning framework, in: Safety Science, Vol. 45, No. 3, pp. 415-430.

Hellström, T. (2009): New vistas for technology and risk assessment? The OECD Programme on Emerging Systemic Risks and beyond, in: Technology in Society, Vol. 31, No. 3, pp. 325-331.

Hodgson, G. (2006): What Are Institutions?, in: Journal of Economic Issues, Vol. 40, No. 1, pp. 1-25.

Hoffmann-Riem, W. (1998): Informationelle Selbstbestimmung in der Informationsgesellschaft. Auf dem Wege zu einem neuen Konzept des Datenschutzes, in: Archiv des öffentlichen Rechts, Vol. 123, No. 4, pp. 513-540.

Hoffmann-Riem, W.; Schneider, J.-P. (1998): Zur Eigenständigkeit rechtswissenschaftlicher Innovationsforschung, in: Hoffmann-Riem, W.; Schneider, J.-P. (eds.): Rechtswissenschaftliche Innovationsforschung: Grundlagen, Forschungsansätze, Gegenstandsbereiche, Schriften zur rechtswissenschaftlichen Innovationsforschung, Bd. 1, Baden-Baden: Nomos.

Howlett, M. (2009): Governance modes, policy regimes and operational plans: A multi-level nested model of policy instrument choice and policy design, in: Policy Sciences, Vol. 42, No. 1, pp. 73-89.

Ilic, M.; Jelinek, M. (2009): Changing Paradigms in Electric Energy Systems, in: Künneke, R.W.; Groenewegen, J.; Auger, J.-F. (eds.): The Governance of Network Industries: Institutions, Technology and Policy in Reregulated Infrastructures, Cheltenham and Northampton: Edward Elgar.

IRGC (2006): Managing and Reducing Social Vulnerability from Coupled Critical Infrastructures, Geneva: International Risk Governance Council (IRGC), available online at: http://www.irgc.org/IMG/pdf/IRGC_WP_No_3_Critical_Infrastructures.pdf, last access at 2010-09-29.

Jackson, D. (2009): A Direct Path to Dependable Software, in: Communications of the ACM, Vol. 52, No. 4, pp. 78-88.

Jackson, D.; Thomas, M.; Millett, L.I. (Eds.) (2007): Software for Dependable Systems: Sufficient Evidence?, National Research Council - Committee on Certifiably Dependable Software Systems, Washington, D.C.: National Academies Press.

Jahn, G.; Schramm, M.; Spiller, A. (2005): The Reliability of Certification: Quality Labels as a Consumer Policy Tool, in: Journal of Consumer Policy, Vol. 28, No. 1, pp. 53-73.

Kambhu, J.; Weidman, S.; Krishnan, N. (Eds.) (2007): New Directions for Understanding Systemic Risk. A Report on a Conference Cosponsored by the Federal Reserve Bank of New York and the National Academy of Sciences, Federal Reserve Bank of New York; National Research Council, Washington: National Academies Press.

Kaufman, G.G.; Scott, K.E. (2003): What is systemic risk, and do bank regulators retard or contribute to it?, in: Independent Review, Vol. 7, No. 3, pp. 371-391.

Keil, F.; Bechmann, G.; Kümmerer, K.; Schramm, E. (2008): Systemic Risk Governance for Pharmaceutical Residues in Drinking Water, in: GAIA, Vol. 17, No. 4, pp. 355-361.

Kesan, J.P.; Shah, R.C. (2005): Shaping Code, in: Harvard Journal of Law & Technology, Vol. 18, No. 2, pp. 319-399.

Kiesling, L.L. (2009): Deregulation, innovation and market liberalization: electricity regulation in a continually evolving environment, New York: Routledge.

Klinke, A.; Renn, O. (2006): Systemic Risks as Challenge for Policy Making in Risk Governance, in: Forum Qualitative Sozialforschung, Vol. 7, No. 1, p. Art. 33.

Kröger, W. (2008): Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools, in: Reliability Engineering and System Safety, Vol. 93, No. 12, pp. 1781-1787.

Krugman, P. (2008): The International Finance Multiplier, available online at: http://www.princeton.edu/~pkrugman/finmult.pdf, last access at 2010-09-29.

Künneke, R.; Finger, M. (2007): Technology Matters: The Cases of the Liberalization of Electricity and Railways, in: Competition and Regulation in Network Industries (CRNI), Vol. 8, No. 3, pp. 303-336.

Künneke, R.; Groenewegen, J.; Ménard, C. (2010): Aligning modes of organization with technology: Critical transactions in the reform of infrastructures, in: Journal of Economic Behavior & Organization, Vol. 75, No. 3, pp. 494-505.

Künneke, R.W. (2008): Institutional reform and technological practice: the case of electricity, in: Industrial and Corporate Change, Vol. 17, No. 2, pp. 233-265.

La Porte, T.R. (1981): Managing Nuclear Waste, in: Society, Vol. 18, No. 5, pp. 57-65.

La Porte, T.R. (1982): On the Design and Management of Nearly Error-Free Organizational Control Systems, in: Sills, D.L.; Wolf, C.P.; Shelanski, V.B. (eds.): Accident at Three Mile Island: The Human Dimension, Boulder: Westview Press, pp. 185-202.

Ladeur, K.H. (2000): Datenschutz - vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken: Zur "objektiv-rechtlichen Dimension" des Datenschutzes, in: DuD - Datenschutz und Datensicherheit, Vol. 24, No. 11, pp. 12-19.

Laperrouza, M. (2009): Does the Liberalization of the European Railway Sector Increase Systemic Risk?, in: Palmer, C.; Shenoi, S. (eds.): Critical Infrastructure Protection III. Third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Hanover, New Hampshire, USA, March 23-25, 2009, Revised Selected Papers, Berlin, Heidelberg: Springer, pp. 19-33.

Laprie, J.C.; Kanoun, K.; Kaâniche, M. (2007): Modelling interdependencies between the electricity and information infrastructures, in: Saglietti, F.; Oster, N. (eds.): Computer Safety, Reliability, and Security. 26th International Conference, SAFECOMP 2007, Nuremberg, Germany, September 18-21, 2007. Proceedings, Lecture

Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Heidelberg et al.: Springer, pp. 54-67.

Leibfried, S. (2008): Rückkehr des Staates?, in: Blätter für deutsche und internationale Politik, Vol. 53, No. 3, pp. 79-85.

Lessig, L. (1999): Code and other laws of cyberspace, New York: Basic Books.

Longstaff, T.A.; Chittister, C.; Pethia, R.; Haimes, Y.Y. (2000): Are we forgetting the risks of information technology?, in: Computer, Vol. 33, No. 12, pp. 43-51.

Lutterbeck, B. (2008): Vom "empirischen" zum "generischen" Recht - der Beitrag der Institutionenökonomik. Beitrag für den Workshop «Software als Institution», veranstaltet vom Karlsruhe Institute of Technology (KIT), Karlsruhe 12. Dezember 2008, Berlin: Technische Universität Berlin, available online at: http://ig.cs.tu-berlin.de/ma/bl/ap/2008/BL-VomempirischenZumgenerischenRechtDerBeitragDerInstitutionenoekonomik-2008-12-30.pdf, last access at 2010-09-29.

Matwyshyn, A.M.; Cui, A.; Keromytis, A.D.; Stolfo, S.J. (2010): Ethics in Security Vulnerability Research, in: IEEE Security & Privacy, pp. 67-72.

Mayntz, R. (1993): Grosse technische Systeme und ihre gesellschaftstheoretische Bedeutung, in: Kölner Zeitschrift für Soziologie und Sozialpsychologie, Vol. 45, No. 1, pp. 97-108.

Mayntz, R. (2008): Von der Steuerungstheorie zu Global Governance, in: Schuppert, G.F.; Zürn, M. (eds.): Governance in einer sich wandelnden Welt, Wiesbaden: VS Verlag für Sozialwissenschaften, pp. 43-60.

Mayntz, R. (2009a): The Changing Governance of Large Technical Infrastructure Systems (Vortrag auf der Tagung "Complexity and Large Technical Systems", Meersburg, Mai 2008), in: Mayntz, R. (ed.): Über Governance. Institutionen und Prozesse politischer Regelung, Schriften aus dem Max-Planck-Institut für Gesellschaftsforschung, Band 62, Frankfurt am Main, New York: Campus, pp. 121-150.

Mayntz, R. (2009b): Von politischer Steuerung zur Governance? Überlegungen zur Architektur von Innovationspolitik (Ausarbeitung eines Vortrags auf der Tagung "Innovation und gesellschaftlicher Wandel", Dortmund, Oktober 2007), in: Mayntz, R. (ed.): Über Governance. Institutionen und Prozesse politischer Regelung, Schriften aus dem Max-Planck-Institut für Gesellschaftsforschung, Band 62, Frankfurt am Main, New York: Campus, pp. 105-120.

Mellstrand, P.; Ståhl, B. (2009): Analyzing systemic information infrastructure malfunction, 2009 4th International Conference on Critical Infrastructures, CRIS 2009; published by IEEE.

Ménard, C.; Shirley, M.M. (2005): Introduction, in: Ménard, C.; Shirley, M.M. (eds.): Handbook of New Institutional Economics, Berlin, Heidelberg: Springer, pp. 1-18.

Mills, D.E.; Brown, K.; Waterhouse, J. (2008): Asset management stewardship: The effectiveness of public-private mix governance structures, 2008 1st International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future, INFRA 2008; published by IEEE.

Müller-Schloer, C.; Schmeck, H. (2010): Organic Computing: A Grand Challenge for Mastering Complex Systems, in: it - Information Technology, Vol. 52, No. 3, pp. 135-141.

Mulligan, D.K.; Han, J.; Burstein, A.J. (2003): How DRM-based content delivery systems disrupt expectations of personal use, Proceedings of the 2003 ACM Workshop on Digital Rights Management, Washington, DC, available online at: http://www.law.berkeley.edu/files/DRM_personal_use.pdf, last access at 2010-09-29.

Nartmann, B.; Brandstetter, T.; Knorr, K. (2009): Cyber security for energy automation systems - new challenges for vendors, 20th International Conference on Electricity Distribution, Prague, 8-11 June 2009, Paper 0247, available online at: http://www.cired.be/CIRED09/pdfs/CIRED2009_0247_Paper.pdf, last access at 2010-09-29.

Nightingale, P.; Brady, T.; Davies, A.; Hall, J. (2003): Capacity utilization revisited: Software, control and the growth of large technical systems, in: Industrial and Corporate Change, Vol. 12, No. 3, pp. 477-517.

North, D.C. (1991): Institutions, in: Journal of Economic Perspectives, Vol. 5, No. 1, pp. 97-112.

North, D.C. (1992): Institutionen, institutioneller Wandel und Wirtschaftsleistung, Tübingen: Mohr.

North, D.C. (2005): Institutions and the Performance of Economies Over Time, in: Ménard, C.; Shirley, M.M. (eds.): Handbook of New Institutional Economics, Berlin, Heidelberg: Springer, pp. 21-30.

OECD (2003): Emerging Risks in the 21st Century - An Agenda for Action, Paris: Organisation for Economic Cooperation and Development.

Orwat, C.; Raabe, O.; Buchmann, E.; Anandasivam, A.; Freytag, J.-C.; Helberger, N.; Ishii, K.; Lutterbeck, B.; Neumann, D.; Otter, T.; Pallas, F.; Reussner, R.; Sester, P.; Weber, K.; Werle, R. (2010): Software als Institution und ihre Gestaltbarkeit, in: Informatik-Spektrum (Online First Version).

Ostrom, E. (2005): Doing Institutional Analysis: Digging Deeper than Markets and Hierarchies, in: Ménard, C.; Shirley, M.M. (eds.): Handbook of New Institutional Economics, Berlin, Heidelberg: Springer, pp. 819-848.

Panzieri, S.; Setola, R. (2008): Failures propagation in critical interdependent infrastructures, in: International Journal of Modelling, Identification and Control, Vol. 3, No. 1, pp. 69-78.

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

Perrow, C.B. (2008): Complexity, catastrophe, and modularity, in: Sociological Inquiry, Vol. 78, No. 2, pp. 162-173.

Personick, S.D.; Patterson, C.A. (2003): Critical Information Infrastructure Protection and the Law. An Overview of Key Issues, Washington, D.C.: National Academies Press.

Quigley, K.F. (2008): Responding to Crises in the Modern Infrastructure. Policy Lessons from Y2K, Basingstoke: Palgrave Macmillan.

Raabe, O.; Lorenz, M.; Schmelzer, K. (2010): Generic Legal Aspects of E-Energy, in: it - Information Technology, Vol. 52, No. 2, pp. 107-113.

Radin, M.J. (2004): Regulation by Contract, Regulation by Machine, in: Journal of Institutional and Theoretical Economics - Zeitschrift für die gesamte Staatswissenschaft, Vol. 160, No. 1, pp. 142-156.

Reidenberg, J.R. (1998): Lex Informatica: The Formulation of Information Policy Rules Through Technology, in: Texas Law Review, Vol. 76, No. 3, pp. 553-584.

Renn, O.; Keil, F. (2008): Systemische Risiken: Versuch einer Charakterisierung in: GAIA, Vol. 17, No. 4, pp. 349-354.

Rhodes, R.A.W. (1996): The New Governance: Governing without Government, in: Political Studies, Vol. 44, No. 4, pp. 652-667.

Richter, R.; Furubotn, E. (1996): Neue Institutionenökonomik: eine Einführung und kritische Würdigung, Tübingen: Mohr.

Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. (2001): Identifying, understanding, and analyzing critical infrastructure interdependencies, in: IEEE Control Systems Magazine, Vol. 21, No. 6, pp. 11-25.

Rohracher, H. (2007): Die Wechselwirkung technischen und institutionellen Wandels in der Transformation von Energiesystemen, in: Dolata, U.; Werle, R. (eds.): Gesellschaft und die Macht der Technik. Sozioökonomischer und institutioneller Wandel durch Technisierung, Schriften aus dem Max-Planck-Institut für Gesellschaftsforschung, Frankfurt am Main: Campus, pp. 133-151.

Rosato, V.; Issacharoff, L.; Tiriticco, F.; Meloni, S.; De Porcellinis, S.; Setola, R. (2008): Modelling interdependent infrastructures using interacting dynamical models, in: International Journal of Critical Infrastructures, Vol. 4, No. 1-2, pp. 63-79.

Sagan, S.D. (1993): The Limits of Safety: Organizations, Accidents, and Nuclear Weapons, Princeton, N.J.: Princeton University Press.

Sajeva, M.; Masera, M. (2006): A strategic approach to risk governance of critical infrastructures, in: International Journal of Critical Infrastructures, Vol. 2, No. 4, pp. 379-395.

Samuelson, P. (2003): DRM {and, or, vs.} the law, in: Communications of the ACM, Vol. 46, No. 4, pp. 41-45.

Schuppert, G.F. (2008): Governance – auf der Suche nach Konturen eines „anerkannt uneindeutigen Begriffs“, in: Schuppert, G.F.; Zürn, M. (eds.): Governance in einer sich wandelnden Welt, Wiesbaden: VS Verlag für Sozialwissenschaften, pp. 13-40.

Setola, R.; De Porcellinis, S. (2009): Complex Networks and Critical Infrastructures, in: Chiuso, A. et al. (eds.): Modelling, Estimation and Control of Networked Complex Systems, Berlin, Heidelberg: Springer, pp. 91-106.

Shah, R.C.; Kesan, J.P. (2003): Manipulating the governance characteristics of code, in: Info, Vol. 5, No. 4, pp. 3-9.

Shapiro, C.; Varian, H.R. (1999): The Art of Standard Wars, in: California Management Review, Vol. 41, No. 2, pp. 8–32.

Spiekermann, S.; Pallas, F. (2006): Technology paternalism – wider implications of ubiquitous computing, in: Poiesis & Praxis: International Journal of Technology Assessment and Ethics of Science, Vol. 4, No. 1, pp. 6-18.

Spulber, D.F.; Yoo, C.S. (2009): Networks in Telecommunications: Economics and Law, Cambridge: Cambridge University Press.

Stoker, G. (1998): Governance as theory: five propositions, in: International Social Science Journal, Vol. 50, No. 155, pp. 17-28.

Streeck, W.; Thelen, K. (2005): Introduction: Institutional Change in Advanced Political Economies, in: Streeck, W.; Thelen, K. (eds.): Beyond Continuity - Institutional Change in Advanced Political Economies, Oxford: Oxford University Press, pp. 208-240.

Tervo, H.; Wiander, T. (2010): Sweet dreams and rude awakening - Critical infrastructure's focal IT-related incidents, Proceedings of the 43rd Hawaii International Conference on System Sciences - 2010, HICSS-43, Koloa, Kauai, Hawaii; published by IEEE.

van der Vleuten, E.; Lagendijk, V. (2010): Interpreting transnational infrastructure vulnerability: European blackout and the historical dynamics of transnational electricity governance, in: Energy Policy, Vol. 38, No. 4, pp. 2053-2062.

van Eeten, M.J.G.; Bauer, J.M. (2008): Economics of Malware: Security Decisions, Incentives and Externalities, STI Working Paper 2008/1, Information and Communication Technologies, DSTI/DOC(2008)1, Paris: Organisation for Economic Co-operation and Development (OECD), available online at: http://www.oecd.org/dataoecd/53/17/40722462.pdf, last access at 2010-09-29.

Varian, H.R. (2004): System Reliability and Free Riding, in: Camp, L.J.; Lewis, S. (eds.): Economics of Information Security, Dordrecht: Kluwer, pp. 1-15.

Vaughan, D. (1996): The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA, Chicago: University of Chicago Press.

Vespignani, A. (2009): Predicting the Behavior of Techno-Social Systems, in: Science, Vol. 325, No. 5939, pp. 425-428.

Vespignani, A. (2010): Complex networks: The fragility of interdependency, in: Nature, Vol. 464, No. 7291, pp. 984-985.

Vesting, T. (2003): Das Internet und die Notwendigkit der Transformation des Datenschutzes, in: Ladeur, K.-H. (ed.): Innovationsoffene Regulierung des Internet: neues Recht für Kommunikationsnetzwerke, Schriften zur rechtswissenschaftlichen Innovationsforschung, Bd. 7, Baden-Baden: Nomos.

Wagner, R.P. (2005): On Software Regulation, in: Southern California Law Review, Vol. 78, pp. 457-520.

Werle, R.; Iversen, E.J. (2006): Promoting Legitimacy in Technical Standardization, in: Science, Technology & Innovation Studies, Vol. 2, No. 2, pp. 19-39.

Williamson, O.E. (1987): The Economic Institutions of Capitalism, New York: Free Press.

Zhivich, M.; Cunningham, R.K. (2009): The Real Cost of Software Errors, in: IEEE Security and Privacy, Vol. 7, No. 2, pp. 87-90.

Zittrain, J. (2008): Perfect Enforcement on Tommorow's Internet, in: Brownsword, R.; Yeung, K. (eds.): Regulating Technologies. Legal Futures, Regulatory Frames and Technological Fixes, Oxford and Portland: Hart, pp. 125-156.