INTERCONNECTED NETWORKS AND THE GOVERNANCE OF RISK

Paper to be presented at the meeting of the permanent study group
on 'Informatization in public administration'
of the EGPA Meeting in Oeiras (Portugal)
3-6 September 2003

Victor Bekkers & Marcel Thaens

Prof. dr. V.J.J.M. Bekkers
Department of Public Administration
Erasmus University Rotterdam
P.O. Box 1738
NL-3000 DR Rotterdam
Tel. + 31 10 4082636
Fax + 31 10 4089199
E-mail Bekkers@fsw.eur.nl

Dr. M. Thaens
Ordina Public Management Consultants
P.O. Box 3069
NL-3502 GB Utrecht
Tel. +31 6 55362169
E-mail Marcel.Thaens@Ordina.nl

1. Introduction

The dominant image of the 21ste century is that of the network society in which information and communication networks and infrastructures play an important role. Looking at the functioning of these networks we see that ICT networks and infrastructures are interconnected with at least two other types of networks and infrastructures. First, there are socio-organizational networks of groups of people and organizations. They use ICT-networks to exchange and share information as well as to communicate which one another. Secondly, there are physical and logistical networks and infrastructures that are used to transport commodities like gas, electricity, water, goods and people. ICT-networks are very often embedded in these logistical networks, for instance to provide the necessary energy or to monitor the movements of these commodities during its transportation. These three kinds of networks and infrastructures are increasingly interconnected and they can be seen as the backbone of our daily life and our daily practices. The result is a multiplying vulnerability for disturbances. These disturbances can bring our daily activities to a standstill. For instance, a major disturbance in the computer network (ICT-network) of the railways leads to a standstill of the rail traffic (physical network); while in large metropolitan areas thousands of people are not able to reach their working places (socio-organizational network).

In this paper we want to address the question what the increasing interconnectedness of ICT, physical and socio-organizational networks implies for the development of governance models regarding the management of vulnerability and risk. We will show that the standard reaction of governments to address the vulnerabilities related to the interconnectedness of networks is highly underestimated. And when it is addressed, it is organized from an internal, task-oriented perspective. The structure of our paper is organized around the following sections. First we will focus – in section two - on a number of characteristics of the network society and we will try to understand the vulnerabilities and risks, which are related to the emergence and functioning of network society. In section three we will follow a random person and show how his daily activities are supported by and embedded in the interconnection of ICT, socio-organizational and physical networks. In section four we show how Dutch governments react to the possible risks that are at stake. In the last section we will broaden our scope and address the fundamental question what kind of governance models governments can use to deal with the vulnerabilities of the network society and what these models imply for the relationship between government and citizens. A strategic agenda for discussion will be proposed. (1)

2. Interconnected risks in the network society

In this section we look at a number of theoretical notions, which can be used to get a better understanding of the network society, its interconnectedness and its vulnerabilities.

2.1 The concept of the network society

In the eyes of Castells (1996, 1997, 1998) the network society can be seen as the result of a paradigm shift, in which the predominantly locally organized industrial society of the 19th century has been transformed into the global network society of the 21st century. This shift is the result of fundamental change in the dominant production technology of capitalist economies and modern (western) societies: " a technology based primarily on cheap inputs of

energy to one predominantly based on cheap inputs of information derived from the advances of microelectronic and telecommunication technology " (Castells, 1996:61). The first characteristic of this 'technological paradigm' is that information is its raw material: all these new technologies are to act on information, not just information to act on technology, as was the case in the industrial revolution. The second feature is the pervasiveness of effects of new technologies. Because information is an integral part of all human activity, all processes of our individual and collective existence are directly shaped by ICT. The third characteristic refers to the networking logic of these new technologies. The morphology of the network seems to be well adapted to the increasing complexity of interaction and to the unpredictable patterns that emerge from this interaction. Network technology and the digitalization of commodities and processes (Negroponte, 1995) makes it possible to create rather flexible connections between, for instance people and organizations, that cross traditional geographical, temporal and functional boundaries (Bekkers, 1998). Flexibility is the fourth feature that can be mentioned, while the convergence of specific technologies into a highly integrated system is the last characteristic of this new technological paradigm. Microelectronics, telecommunications, bio- and opt electronics and computers are now all integrated into comprehensive systems.

The persistence of this new technological paradigm leads to social and economic conditions in which the nature of the production is focused on the production of information processing itself, the production of information processing devices and on the management of information processing (Castells, 1996:67). Moreover, the economy of the information society is a global economy: it is a economy with the capacity to work as a unit in real-time on a planetary scale, which uses ICT-networks to create new production and competition conditions that are based on the creation of information spaces (Castells, 1996: 92). Castells (1996:412) uses two notions to describe the creation of informational spaces on a planetary scale. The first notion is that of 'a space of flows' which can be described as the "material organization of time sharing practices that works through flows" (of capital, words, images, sounds, interactions etcetera). This space of flows can be described as a combination of at least three layers of material that support the constitution of it. The first layer is the circuit of electronic impulses, the network of interconnected technological systems themselves like for instance microelectronics, telecommunications, computer processing and broadcasting system (Castells, 1996:412). Its nodes and hubs constitute the second layer of the space of flows. An electronic network is always linked to specific places, with well-defined social, cultural, physical and functional characteristics (Castells, 1996:413). Some places are exchangers and function as a communication and coordination hub to facilitate the smooth interaction of all the elements integrated into the network. Other places are nodes of the network that are the location of strategically important functions that built a series of locality-based activities and organizations around a key function in the network. The location in the node links up the locality with the whole network. Wall Street can be seen as a node in the global financial market system, which is highly computerized. The third layer refers to the spatial organization of the dominant, technical, financial and managerial elites (Castells, 1996:415), who through hubs and nodes have access to the space of flows. The second notion Castells uses to describe this new informational space is that of 'timeless time', which is formulated as "the systematic perturbation in the sequential order of phenomena performed (..) Perturbation may take the form of compressing the occurrence of phenomena, aiming at instantaneity, or else by introducing random discontinuity in the sequence eternity" (Castells, 1996:464). An example is the Black Monday crash in the late eighties in Wall Street which had at the same time enormous local and global effects, due to the connection of electronic bidding systems by network technology. At the same time this examples illustrates that the network society is an enormous vulnerable society.

2.2 The concept of the risk society

Another author who is relevant for our research goal and which cannot be missed to understand the nature of interconnected networks is Beck. Disasters, like fire, war, famine and floods, are of all times. However, the modernization process that started with the process of industrialization in the 18th century has produced new risks. Before the industrial revolution the confrontation with risks was a confrontation with the will of God (Beck, 1999:50). In the 19th and 20th century our assessment of risks and dangers has changed. Risk full behavior is seen as source of danger, which can be traced by looking at the decisions and consideration of utilities that have been made. These decisions may have intended and unintended consequences that produce specific risks and dangers. As a result of this changing perspective on risk assessment, the so-called 'calculus of risk' has been introduced, which connects the physical, the engineering and the social sciences'. Risks can be calculated and can be (statistically) described as events, which make them to a certain degree understandable and manageable. Moreover, the calculation of risks makes it possible to buy off such a risk by taking out an insurance policy and/or by taking counter measures, like technical adjustments. In the calculus of risk, the governance of risk is seen as a process of social engineering that permits a type of 'technological moralization' (Beck, 1994:51-52). Technological moralization refers to a process in which paying an insurance premium can pay off risk full behavior or it can be neutralized in terms of a minimum percentage of occurrences. The result is a monopolization of the way modern societies define and deal with risks, of the way knowledge about the causes and effects of potential risks is presented, and actions are or will be taken (Beck, 1999:59). The assessment of risk and risk full behavior is no longer the subject of moral, ethical and individual considerations; it de-individualizes and is not the subject of political debate.

The dominance of the 'calculus of risk' obscures the perspective on a process which Beck (1999:73) has called 'reflexive modernization': the transition from the industrial to the risk epoch of modernity occurs unintentionally, unseen, compulsively, in the course of a dynamic of modernization which has made itself autonomous, on the pattern of unintended consequences. The risk society is not an option that can be chosen or rejected in the course of political debate. It arises through the automatic operation of autonomous modernization processes that are blind and deaf to the consequences and dangers. In total, and latently, these produce hazards, which call into question the basis of the industrial society. In contrast to earlier industrial risks, these new biological (the rise of the BSE disease), chemical (the explosion of a dioxin plant in Seweso, Italy), nuclear (the explosion of a nuclear plant in Chernobyl), environmental (the Ozone-layer) an genetic engineering (DNA manipulation and food production) risks can a) be limited in terms of neither time or place, b) are not accountable according to established rules of causality, blame and liability, because of its complexity, dynamics and overwhelming number of involved actors and c) cannot be compensated for or insured against (Beck, 1999:77; 54). They become an event with a beginning and no end; an open ended festival of creeping, galloping and overlapping waves of destruction, according to Beck (1999:54). The only way out is to create a process of self-confrontation with the consequences of the risk society by increasing the reflexive capacity of the modernization process itself (Beck, 1999:73). A necessary condition for establishing this reflexive capacity is to break up the monopoly of how risks are being defined and perceived. In a risk society that identifies itself as such, the critique should be democratized (Beck, 1999:79). Social self-critique is needed, which can overcome an industrialized society with a 'truncated' democracy, in which questions of the technological change of society remain

beyond the reach of political-parliamentary decision-making (Beck, 1999:70). This can be established by a further separation of powers between the political and economic-technological powers, and by the creation of a free public sphere, in which an open and public debate can be organized (Beck, 1999:70-71).

2.3 The cultural and institutional bias of risk

Can we know the risks we face? This is the title of the first chapter of Douglas & Wildavsky's book 'Risk and Culture'. Risk and uncertainty are two sides of the same coin. Knowledge about risks is surrounded by uncertainty, but the ultimate question is, how should we assess this uncertainty? The assessment of risk is a highly subjective matter. The assessment of risks is a process that not only takes place on the individual and micro-level, but also on meso, group level and a macro, societal level. How do groups or communities assess events as risky? The assessment of an event as a risk full event is a joint product of knowledge about the future and consent about the most desired prospects. In Douglas and Wildavsky's (1983:4) perspective the ultimate challenge in the process of risk assessment is to create a common perception, understanding a definition of – and thus agreement on – risk. In most cases knowledge is uncertain and/or the criteria and norms people use to assess these risks also differ. The process of the selection and definition of events as risky events is about acceptability, which is always a political issue. There is no single correct conception of risk; there is no way to get everyone else to accept 'it'. Risk assessment should be seen from a cultural perspective, looking at cultural bias, which is embedded in each social arrangement, for instance a group, an organization or a society. The choice of risks and the choice how to live are taken together. Each social arrangement has its own risk portfolio, in which common values lead to common fears and vice versa. As Douglas and Wildavsky (1983:8) put it "risk taking and risk aversion, shared confidence and shared fears, are part of the dialogue on how to organize social relations. For to organize, means to organize some things in and other things out". This notion implies that a cultural analysis of risk assessment, risk taking and risk avoiding is a meaningful way of looking at risks. How do actors or social institutions define risks, which norms and values lay behind this definition, which interests are at stake and how do actors communicate about their definition of risk in order to create a shared understanding about the nature of certain events? It is the social environment that defines which dangers are worth attention (Douglas & Wildavsky, 1983:9).

Hood et al. (2001:6) focuses on the question how governments try to regulate societal risks. The result is a policy and intellectual archipelago or risk domains isolated from one another, with different policy stance across various domains. Each domain has its own risk regulation regime. By using the concept of a regime Hood et al. try to analyze the definition of risks and the measures which are taken to control the emerge of these risks, from an institutional perspective. In this perspective it is interesting to look for the 'rules' that influence the definition of risk and risk policies. Rules are "the routines, procedures, conventions, roles, strategies, organizational forms and technologies around which (...) activity is constructed. We also mean the beliefs, paradigms, codes, cultures and knowledge that surround, support, elaborate and contradict these roles and routines" (March & Olsen, 1989; 22; see also DiMaggio & Powell, 1991).
The result is a broad variety of risks and risk regimes. This variety shows that the notion of the risk society is too broad and too abstract. The variety of the regime content, particularly the size of the regulatory effort, can largely be explained by features of the regime context,

which is rather dynamic. Moreover, Hood et al (2001:174) draw the conclusion that within many regimes a coherent control system is lacking.

2.4 Bringing the ideas together

We have looked at a number of relevant theoretical ideas, which can be used to understand the risks that are emerging from the interconnection of ICT, physical and socio-organizational networks as well as to understand how societies and governments assess these risks. At the end of this section we will bring some of these ideas together.

Understanding the origin of interconnected risks
The following notions are important to understand the origin of the risks that emerge from the interconnection of networks:

- Castells shows how ICT has penetrated in all the domains of human activity, not as an exogenous source of impact, but as a fabric in which such activity is woven (Castells, 1996:31). This observation justifies the central question in our paper: what does the interconnectedness of ICT, physical and socio-organizational networks imply for the interdependencies and vulnerabilities which are embedded in their interconnectedness;
- The vulnerabilities of Castells' network society become manifest in the location of certain 'hubs' and 'nodes' in the space of flows. It are these 'hubs' and 'nodes' in which the interconnectedness of ICT, physical and socio-organizational networks is organized. Moreover, disturbances in the global space of flows of timesharing activities and interactions lead to local and global risks;
- The network society can be seen as the result of a process of modernization, which autonomous logic produces unintended consequences, which manifest themselves as events with a beginning but and no end, with local and global effects;
- The perception and definition of risks, emerging from the interconnectedness of networks, is highly subjective and biased from a cultural perspective, in which it is important to look for a common values and norms; and
- The perception and definition of risks, emerging from the interconnectedness of networks is influenced by the 'rules' that are embedded in government organizations and in risk regulation regimes.

The changing nature of the risks in the network society
If we look at the work of the authors we have studied, we see that the risks in the evolving network society are changing if we compare them with the risks in the industrial society. Some talk about 'new' risks in relation to 'old' risks (Douglas & Wildavsky, 1983:16). New risks are hidden (we shall not know we are encountering them), the dangers are involuntary (we would not willingly accept them) and they are irreversible (there is no turning back). If we try to bring this characterization of the so-called 'new' risks a step further, which dimensions can be seen?

- The broadening of risks. The interconnection of networks and the existence of interconnected risks can lead to spill-over and snowball-effects, which will penetrate other domains and activities;
- The deepening of risks. Events can hit a node in the networks, which can be seen as hitting the hart of the network, leading to a severe crisis. An example is the crash of the Twin Towers in Manhattan that also hit the heart of the financial system;

- The acceleration of risks. The real-time or timeless nature of the network society can generate harmful effects in seconds. Computer viruses demonstrate this each time again.
- The glocalization of risks. Disturbances in interconnected networks, which support worldwide economic, financial, military and other operations and activities, do not only have global effects, but also have local effects that can vary in intensity. At the same time local distortions can spread themselves, using these networks, and generate worldwide effects. The SARS virus is an example of a local disease which has spread by using global (air traffic) infrastructures;
- The subjectivity of risks. The risks in the network society are culturally and institutionally biased, which can lead to different perceptions of risks and different risk avoiding or risk taking activities by the nodes in the network or the different parties that are gathered around a node.

Dealing with risks

How can we deal with the vulnerabilities that emerge from the interconnection of networks, and what does this imply for the role of government? Analyzing the literature that is used in this paper, the following observation can be made:

- The global interconnectedness of ICT, socio-organizational and physical networks limits the capacity to take effective risk avoiding measures or to handle crisis. The interconnectedness of networks fundamentally challenges one of the core tasks of government: preserving safety, and thus challenges the legitimacy of the sovereign state (Castells, 1997:243);
- Question marks can be put at the capacity of governments or the capacity of the state to influence the shaping and functioning of the network society and spaces of flows that constitute this new society. Castells (1998:347) sees a crisis of the nation-state as a sovereign entity as well as a related crises of representative democracy as a result a blurring boundaries of sovereignty. The existing geometry power, which is based on the idea of the hierarchical state, will be replaced by a new geometry of power, that of the horizontal, multilateral, decentralized and fragmentized network state;
- According to Castells (1998:347) icons, symbols and symbolism in politics play an important role in the network society (‘the medium is the message’, to quote McLuhan), which implies that risk management policies in the network society will also be highly symbolic;
- It is important to look how government (and societies) defines and select events as harm full events, which ask for government intervention. What is the cultural and institutional bias of relevant stakeholders that lay behind the definition and selection of these risks? In relation to our research goal, it is important to look how governments define the interconnection of networks as a risk full development. In this definition it is important to look at the frames of references which are used, and how these frames of references are influenced by the institutional setting in which they are developed, used and reproduced (Douglas & Wildavksy, 1983; Hood et al., 2001)
- Beck (1998) points at the one-dimensional, techno-economic definition of risks and risk avoidance. Risk management is predominantly seen as ‘social engineering’. Defining risk management as the management of the safety chain, in which effective management is seen as establishing a smooth coordination of separate activities, which together constitute the chain, is an example of a social engineering approach of risk avoidance. In order to break up the one-dimensionality of risk management policies, Beck (1998) pleads for the democratization of the discussion about risks, which

emerge from the modernization of society, in which alternative risk definitions can compete with the existing ones; and

- According to Hood et al. (2001) the governance of risk can be facilitated, if we are able to increase the learning capacities in policy networks by enhancing the variety and overlap of perspectives and risk regulation regimes. However, the control systems within a risk regulation regime are so badly organized and maintained, that it is important to improve these control systems first before we can ask the question, how to improve these learning capacities.

3. Traveling through the network society

In this section we reconstruct the life of a random person by following him during one day. In this reconstruction of some events during this day we will show, how his activities are embedded in (interconnected) networks and which possible risks he faces. We reconstruct the risk from the perspective of an ordinary citizen.

Events	Involved networks	Examples of connected risks
Wake up and Get up	Electricity network (alarm and shower) Gas-infrastructure (shower) Water-infrastructure (shower) Telephone network Food safety (breakfast) Computer networks (laptop) Rail-infrastructure (train) Waste-disposal Traffic-infrastructure (street)	No warm water No telephone use No use of the computer Short circuit on electricity (fire) No use of domestic appliances Train accident Collision on the street (Indirect) Health damage by food poisoning/waste disposal
Go to work	Rail-infrastructure Communications-infrastructure (newspaper) Traffic-infrastructure Security network (office; entrance-gate and receptionist) Transport-infrastructure (elevator)	Train accident Incomplete or inaccurate information (manipulation) (newspaper) Accident on the street No entrance to the office Getting stuck in the elevator
At the office	Communication networks (laptop, telephone, GroupWise, mail, post) Electricity network (light, coffee machine, computer) Water-infrastructure (coffee, toilet) Security networks (password on computer) Personal networks (talking with colleagues)	No post, email of manipulated email Viruses on computer No electricity No water or polluted water No entrance to the computer systems
Meeting outside the office	Communications network (intranet) Electricity network (reserving a bike by intranet) Traffic-infrastructure (bike) Social networks (meeting) Security network (entrance-badge, checking in)	Collision on the street No reservation for a bike No entrance Computer network down Manipulation of information Identity-fraud (internet)
Riding home by car	Traffic-infrastructure (car and parking badge) Traffic circulation system (traffic lights) Communication-infrastructure (car-stereo) Fuel-provision (LP Gas)	Traffic accident Disordered Traffic (Traffic lights not working) No radio-transmission No Fuel for car

If we look at the risks as described above, it is interesting to change the perspective from a citizen-oriented perspective towards a government-oriented perspective. We have selected a number of government organizations that are responsible for the development and implementation of risk policies in the geographical and functional area in which our random person works and travels. How do these organizations define these risks? Do they relate these risks to the increasing interconnection of ICT, physical and socio-organizational networks? What actions do they take?
We have analyzed the official policy documents of the following public authorities:

- The policy document on integral safety of the Ministry of Internal Affairs (Integraal Veiligheids Programma), which address the problem of the safety of citizens in the public domain;
- The policy document on external safety of the Ministry of Spatial Planning, Housing and the Environment;
- The integral safety policy document of the Province of South-Holland, which addresses all the events and situations which are potentially harmful in the region and for which this regional authority is responsible (Integrale Veiligheidsnota Provincie Zuid-Holland);
- Several documents regarding the safety of citizens for which the municipality of The Hague is responsible, which were available at the website www.denhaag.nl;
- The policy document on railway safety of the Ministry of Traffic (Nota Railveiligheid);
- The Action program on Terrorism and Safety of the Ministries of Internal Affairs and Defence (Actieprogramma Terrorismebestrijding en Veiligheid);
- The policy document on vulnerabilities on the Internet of the Ministry of Internal Affairs (Nota Kwetsbaarheden op het internet-Kwint).

We will not discuss the individual documents, but we will draw some conclusions, using the format of section 2.4

Understanding the origin of interconnected risks
A great number of policy documents point out the vulnerabilities that result from the increasing interconnectedness of social, organizational and ICT-infrastructures. Especially, in those places where the infrastructures meet. At the same time there is more attention for the independent meaning of ICT-infrastructures. The Risk-society is a well-known notion that mainly is used as a concept to position risks in the present era. This is especially so for the policy documents on the national level. They mainly deal with the general safety policy at the macro-level. This is different at the middle- and micro level of provinces and the local communities. At these levels risks are usually not associated with the interconnectedness of infrastructures, but with risky behavior of persons, groups and organizations. Therefore, the policy is aimed at reducing this behavior. This accounts for the fact that a lot of attention is given to measures that aim at eliminating the source or minimizing the effect of this kind of behavior.

The changing nature of the risks
In the different policy documents no analysis is made of the changing nature of the risks in the network society by linking them to an interwoven infrastructures. An almost immediate

reduction of complexity is often at hand. This is the case in the policy document on integral safety, in the Action program on Terrorism and Safety and in the policy document on vulnerabilities on the Internet. The policy document on railway safety mainly addresses physical risks and emphasizes the development of personal injury and material damage. Risks within the ICT-infrastructure are at the center in the policy document on vulnerabilities on the Internet. The Action program on Terrorism and Safety focuses on 'classical' forms of criminal behavior that is carried out by using modern means and by making use of the vulnerabilities of our modern society. Also the policy document on integral safety reduces the complexity of reality. It focuses on fighting the trouble that is caused by crime within the public space. We conclude that in the policy document on external safety from the Ministry of Spatial Planning, Housing and the Environment and the integral safety policy document of the Province of South-Holland, an important role is played by the spatial embedded ness of risks which makes it possible to localize these risks and to know them. In these documents it is not fully recognized that new risks with a different character are emerging.

Dealing with risks

Different documents bring up the role of government in dealing with risks and the consequences of this role for the legitimacy of government. Protection against these risks is seen as an assignment for government. However, this does not relieve citizens, companies other government organizations or societal organizations from there own responsibility in this domain. Yet another conclusion that can be drawn relates to the thought that risks, at least to a certain limit, can be controlled and that they are amendable by forms of 'social engineering'. This controllability rests upon two assumptions. The first is the assumption that risks can be known and can be localized. Risk analysis and inventories of risks are important for the control and reduction of risks (see for example the integral safety policy document of the Province of South-Holland). The idea that working with a safety chain results in a better control over risks is the second assumption. Then, important in controlling risks are:

- A better information supply that crosses organizational borders;
- A better coordination between the links in the safety chain;
- A further integration of tasks between the links in the chain; and
- More attention to the prevention of risks.

In addition to this, ICT's are more and more seen as a deus-ex-machine. Due to the exchange and sharing of information and knowledge and communication, the use of modern ICT's leads to a better information supply within the safety chain. Furthermore, the use of modern ICT's contributes to the fact that risks can be known, for example by supporting policy development and decision-making. ICT's also accounts for a further rationalization of the controllability of risks.

Earlier we have pointed out that in general in the policy documents risks are often recognized as a result of the interconnectedness of infrastructures. However in most of these documents a quick reduction of complexity takes place. This is due to the fact that the definition of risks and the way in which to deal with them takes place on the basis of the tasks, the responsibilities, the routines and the authority of a government organization. It could be stated that this leads to a demand-oriented approach of risks. With it goes that maintenance of laws and rules (especially permits) is accentuated.

4. The governance of risk: three models

The governance of risk can be seen as dealing with a 'wicked problem'. Our understanding of the nature of the variety of potential risks (which emerges from the interconnection of ICT

networks, socio-organizational networks and physical networks) is limited. Clear causal relations cannot be discerned. We also do not know if the measures which has been taken to avoid possible risks, are sufficient enough. Moreover, we do not how we should assess these risks in a political way. The normative framework to assess the measures to be taken is permanently in discussion, for instance in relation to privacy issues. At the same time we see that a broad variety of public, semi-public and private organizations are dealing with the problem, which leads to all kinds of multi layer and multifunctional communication and coordination problems.

In essence we discern three governance models that can be used as a perspective to address the problem of the governance of risk. In each model there is one dominant, but different coordination mechanism, which has different effects on the role and position of government and the citizens in dealing with the risk that emerge for the interconnection of ICT, socio-organizational and physical networks. After we have described each model, we will draw some conclusions and formulate a number of strategic question and dilemmas.

4.1 The state: the governance of risk as a problem of 'command and control'

Because of their impact on society, safety and vulnerability problems are in this model seen as assignments for government. Two variations can be seen within this model. In the first, safety is viewed as a managerial administrative problem in which maintenance and supervision on the execution of rules is a central issue. In the second, safety is seen as a technological question. ICT's should be used to narrowly monitor behavior and movements and to make them visible. Interventions can then take place earlier and easier.
The cybernetic model of steering (Van Gunsteren, 1976) lies at the basis of these two 'command and control' approaches of safety problems. Typical for this model is the idea that the government is situated at one central point above society and is capable to perform preventive as well as corrective interventions. Crucial for this is an information supply that is functioning optimally. For its interventions the government has a number of instruments to its disposal that can be used for supervision, inspection and monitoring. It concerns for example legal competences to exercise administrative pressure, such as the closing of dangerous objects, the withdrawal or suspension of permits, the enforcement of fines and the distribution of warnings.

From this model viewed safety risks are control issues. Central control is seen as the strengthening of the ability of a government organization to supervise. This can be realized in three different ways. The first is to integrate inspection agencies. The assumption behind this is that an integral approach is needed to deal with the complexity of most policy areas. The second way is to support supervision by improving the information supply for an organization, for example by developing monitoring systems based upon a 'will to know' (Bekkers, 1994). The third and last way is to extend and refine legal competences to intervene, especially from the viewpoint of administrative and criminal law.

Central in the technological variation of the cybernetic 'command and control' approach are the so-called 'safety enhancing technologies'. A lot of significance is attached to the detection ability of these technologies (Bullinga, 2002). The most well known example is the use of video-surveillance in buildings and public spaces, even in streets. The ability to detect is the result of technological developments. One of these is the fact that computer technology is becoming smaller and smaller. Therefore, people, buildings, goods, appliances and animals are more often provided with chip or mobile technology. As a result local intelligence is being

realized that can be detected at distance. The infrastructures needed are provided by a further integration between ICT and other networks (such as television and video). This development is sometimes referred to as 'embedded internet'. This detection model is also based upon a cybernetic steering model; from a central point it is possible to monitor the behavior and movements of people and for example vehicles and to intervene if this is necessary.

Usually this 'command and control' model evokes questions about people's privacy. This because detection technology calls upon the scenario of 'Big Brother is watching you'. At the same time however, the introduction of this sort of technology often involves the introduction of a new information technological network or infrastructure. This leads to an interesting paradox. To reduce the safety risks that result from the interaction and the interconnection of different kinds op networks and infrastructures, a new infrastructure is connected to the already existing infrastructures. As a result the complexity and with it the risks will increase….

4.2 The market: the governance of risk as a problem of self-regulation

In the second model it is recognized that that are considered as facts of the western 'open' society in the year 2003. This puts in perspective the role and the position of government as guardian of society's stability; government's space to move is limited. At the same time however, the prevention and fighting of safety risks is seen as an assignment for government. The steering model that is connected with the approach above is a form of steering at distance. Within certain judicial frameworks, the care for safety is seen as a derivative responsibility for citizens and companies. But because these frameworks contain standards for processes rather than standards regarding the content, citizens and companies have to develop own ways to take their responsibility. Examples are compulsory third-party liability insurance for citizens and motorists, but also internal environmental care programs for companies and forms of certification.

A variation of the model above is where markets are used to deal with risks. Here self-regulation is also used as steering mechanism. The idea that safety risks are inextricable linked with the complexity and the dynamics of western society is further radicalized. This radicalization leads to the opinion that corrective and preventive government interventions cannot succeed. It is up to individual citizens and companies to raise their own consciousness of risks and to take care of them. Safety risks then become liability problems that have to be solved by private law. The assumption behind this line of reasoning is that the possible financial consequences of such a liability works preventively. When accidents of incidents occur, there consequences are covered by (injury) compensations and insurances against damage.

Beck (1999) has pointed out that that 'new' risks can no longer be assured. Their effects are so massively, disastrous and radical that they would cause the bankrupt of the insurance branch. This is the reason why insurance companies have changed their insurance contracts after the attacks at the WTC in New York on the 11th of September 2001. Now, damages as a result of terrorist attacks are no longer covered.

Another instrument within this model is certification. By developing a quality assurance system, connected with a system of certification, private companies can prevent the occurrence of risks. For more then one reason this is interesting for them. It raises the quality-

level within the company, but more important, it can also lead to the prevention of various liability claims. A well-known example in the Netherlands is Albert Heijn, an international supermarket chain. They demand a certain level of quality of their fresh foods (such as meat) from their suppliers. These demands are imposed by certification. If a supplier cannot or can no longer meet the demands, they will lose their certificate and as a consequence their returns. So, safety risks are not covered by the government, but by private enterprises.

4.3 The civil society: the governance of risk as a problem of civic competence

In the third and also last model, safety is seen as a collective responsibility of the State, the private companies and society. An attempt is made to involve citizens and groups of citizens in the safety-issue. Therefore, this safety issues becomes a societal issue. This applies to the public debate about safety but also to the (mostly preventive) approach of vulnerabilities that are the results of the interaction and interconnectedness of social-organizational, physical and technological networks.

The importance of organizing a public debate about the nature and the effects of 'new risks' is pointed out by Beck (1999). He objects to an approach in which the nature and the effects of these risks are over rationalized in econometric models and in measures for prevention and correction based upon these models. This suggests an illusion of controllability. As a result, certain groups of scientists one-sidedly monopolize the diagnosis of risks. These groups also monopolize the way in which knowledge about the risks is presented and the way in which these risks are dealt with. Beck also blames politicians and administrators for following these groups of scientists. Sometimes, this leads to an 'iron coalition' between scientists, politicians and administrators that each have an interest in cherishing the earlier mentioned illusion of controllability. It is therefore that a plea is made for breaking the monopoly by bringing up some alternative perspectives and by setting up platforms for debate and dialogue. These platforms are aimed at influencing opinions held by the public and by politicians.

Another approach also tries to involve the citizen in the safety-issue. This by addressing the different citizen's roles played in society. For example citizens can act as private persons and as consumers of government services. They then have a direct interest in safety. They can also be involved in the issue because they are sincere involved in public affairs (the 'citoyen' role). An example of this involvement is interactive policymaking. However, it is also interesting to look at the information base of citizens, which enables them to actually play the role of co-supervisor to the government. Safety issues are then seen as a process of co-production of policy or supervision. Some instructive examples of this development can already be found in the actual practice of supervision.

By means of the Internet and web technology citizens can access government information. This enables them to judge for themselves if the quality of measures and actions taken by government live up to their own standards and interests. By making this kind of information available, the functioning of a policy area becomes more transparent for citizens. By introducing the citizen (and interest groups) as co-supervisor, this transparency leads to the integration of certain 'checks and balances' within the existing system of supervision.

In this case, two examples are interesting. The first is that on the website of the Inspection of Education in the Netherlands inspection reports can be found. These reports contain a judgment of the quality of elementary schools as well as suggestions for improvements. With

this kind of information, parents can make their own well-informed judgments about the quality of their child's school. Also on the basis of this information an appeal can be made towards the school governors about the delivered quality and the measures they have taken to raise the quality. So in fact this website functions as a stimulus to raise the quality of education. A second example has to do with a disaster that took place in the Dutch city of Enschede. In May 2000 a big firework plant exploded, taking many lives and devastating a complete residential area. As a result, many provinces are developing so called risk registers that can be consulted by citizens trough the Internet. In such a register it is possible to check which safety risks (following from certain objects or installations such as plants) occur in the environment where a citizen lives and works. It is also possible to see the (safety) requirements for these objects and installations and the measures taken by them to meet these requirements. With this kind of information, citizens can appeal to these measures to government as well as to the private companies. Also, such an information base facilitates a process of self-organization. Citizens organize themselves around the information as an interest group. As such, they can put pressure on government organizations responsible for granting permits and on private companies as holders of these permits.

5. A strategic agenda: conclusions and tensions

When the risks that follow from notions as interconnectedness and interwoven networks are confronted with the different steering models as described in the last paragraph, some dilemma's and tensions come forward. They constitute a political agenda for safety policy that is based on vulnerabilities of citizens.

An impossible task: an uncontrollable assignment for government
The first tension has to do with the degree in which risks can be considered controllable if they result from the interaction and interconnectedness between social-organizational, physical and technological networks. This is in fact the question if a government is still able to fulfill her assignment as guardian of safety in a society of interwoven networks and infrastructures. This question is especially relevant when we consider the complexity and the dynamics of the issues at stake, the organizational and administrative levels involved and the interwoven public and private responsibilities.

The safety chain as instrument: illusion or solution
In many policy documents on safety the so-called safety chain is put forward as an effective instrument for dealing with risks. The concept of a chain is seen as a means to put in order different kinds of activities and to improve the sequence of them. According to Beck (1999) this leads to cherishing the illusion of predictability and controllability. The question is whether the view in which activities are put in sequence of the safety chain is doing justice to the earlier mentioned complexity and the dynamics of the issues at stake, the organizational and administrative levels involved and the interwoven public and private responsibilities. Even from an administrative and organizational view alone, it can be seen that a network of organizations (each organization with a different position, interests, assignments, responsibilities and competences) is hiding behind each activity within the chain. It is interesting to see that also from a chain-oriented approach of safety, usually the preventive or repressive measures are molded and shaped on the basis of a specific assignment of a certain organization, resulting from legislation and rules. Furthermore, the dominant internal orientation of the safety chain approach often neglects the external interaction between different kinds of (interwoven) networks and infrastructures.

Reduction of complexity: centralization or more variety
From a steering point of view, the complexity and the dynamics that result from the interwoven social-organizational, physical and ICT-networks offer an interesting challenge. It's the question namely if centralizing some of the assignments and responsibilities in the field of supervision, can control this complexity. Often, this kind of centralizing also means that some kinds of merger of supervisors have to take place. Perhaps is the opposite of centralization a more appropriate reaction to the complexity. Some insights about steering, such as the concept of requisite variety (Conant and Ashby, 1970), point out that complexity can only be controlled by using complex and varied steering mechanisms. The network character of the earlier mentioned risks therefore asks for a network-like organizational reaction. This means by definition that many and varied supervisors continue to exist. It is important however, that these supervisors are able to maintain open relations with each other. It should be prevented that they become introverted.

Safety versus privacy
Another tension has to do with the trade off between guaranteeing the safety of society and respecting the individual privacy of citizens (see i.e. Thaens et. al 2002). For a matter of fact, the same tension applies to improving government service to citizens by using modern ICT's. In order to come to a safer society/improved level of service government increasingly uses modern information and communication technologies. One can think of the use of smart card and transaction technology, the attribution of unique characteristics (biometrics) and the observation of persons (using cameras and the tapping of telephone and internet traffic). For 'average' citizens the use of this kind of technologies has important consequences. More data are collected and citizens are being observed. Besides that, the information that is collected is more often stored, processed/used or exchanged/re-used. Regardless of the fact whether he is obtaining services or because he shows divergent behavior compared to 'average' citizens, these consequences become proportional more strongly when a citizen has more contacts with government organizations. For divergent behavior it can be seen that the combination of smart cards, unique characteristics and transaction technology creates a process that directly can be followed by government. Deviant behavior stands out in those processes and will lead to all kinds of additional actions and control. When deviant behavior shows, cumulative effects occur in policy measures. These measures then break in on each other. The consequences of modern ICT's further strengthen this process. For example, when the situation of someone diverges from an 'average' situation, extra control takes place. The information that is collected in this control can be used for additional analysis. Also the opportunity for additional exchange of information occurs. Of course, before the use of modern ICT's the government also investigated situations that diverged from average. However, the investigation was limited to the specific contact between the citizen and government. ICT's has especially consequences on the effects of such an extra control or investigation (Thaens et al, 2002). It stretches the context of control and investigation.
The dilemma therefore is the need for a permanent consideration of the ambitions of government (supported by ICT's) and the infringement these causes on the private life of citizens. Special attention is needed for the combination of technologies en policy measures, because these can have cumulative effects on the privacy of citizens.

Note
1. This paper is based on a study, which we have conducted for the Ministry of Spatial Planning, Housing and the Environment and the Ministry of Internal Affairs. The report is published as: Bekkers, V.J.J.M., M. Thaens, V.M.F. Homburg, J. Ragetlie and M. de Rooij, De keerzijde van verbonden netwerken. De relatie

overheid-burger in de risicosamenleving (The other side of interconnected networks. The relationship between government and citizen in the risk society), Eburon, Delft, 2002.

Literature

Adam, B., U. Beck, J. van Loon (2000), *The Risk Society and Beyond. Critical Issues for Social Theory*. Sage Publications, London/Thousand Oaks/New Delhi.

Beck, U. (1994), The reinvention of politics, Towards a theory of reflexive modernization, in: Beck, U, A. Giddens & S. Lash, *Reflexive modernization.* Polity Press, Cambridge, pp. 1-55.

Beck, U. (1998), *The politics of Risk Society*, in: Franklin (1998).

Beck, U. (1999), *Risk Society.* Sage Publications, London.

Beck, U. (1999), *World Risk Society*. Polity Press, Malden.

Bekkers, V.J.J.M. (1994), Nieuwe vormen van sturing en informatisering (New forms of steering and informatization), Eburon, Delft.

Bekkers, V.J.J.M. (1998), *De grenzeloze overheid (The boundless government),* Alphen aan den Rijn: Samsom.

Bekkers, V.J.J.M. (2000), *Voorbij de virtuele organisatie (Past the virtual organization)*, Elsevier, Den Haag.

Bullinga, M. (2002), *In Total Self/Control.* Den Haag, Ten Hagen Stam.

Castells, M. (1996), *The Rise of the Network Society, The Information Age: Economy, Society and Culture.* Blackwell, Cambridge.

Castells, M. (1997), *The Power of Identity, The Information Age: Economy, Society and Culture*. Blackwell, Cambridge.

Castells, M. (1998), *The End of the Millennium, The Information Age: Economy, Society and Culture*. Blackwell, Cambridge.

Castells, M. (2000), Materials for an exploratory theory of the network society. *British Journal of Sociology*. 51(1). Pp. 5-24.

Conant, R.C, R.W. Ashby (1970), Every good regulator of a system must be a model of that system, *International Journal of Systems Science*, Vol. 1, no. 2, 89-97.

DiMaggio P., W. Powell (1991), New Institutionalism in organizational analysus, Chicago, University Press, Chicago/London.

Douglas, M., A. Wildavsky (1983), *Risk and Culture, An essay on the Selection of Technological and Environmental Dangers.* University of California Press, Berkeley, Los Angeles, London.

Franklin, J. (1998, ed.), *The Politics of Risk Society*. Polity Press in association with the Institute for Public Policy research, London.

Gunsteren, H. (1976), *The quest for control*, Wiley, London.

Hood, C., H. Rothstein, R. Baldwin (2001), *The Government of Risk. Understanding Risk Regulation Regimes.* Oxford Press, Oxford.

March J.G. & J.P. Olsen (1989). Rediscovering Institutions, Free Press, New York

Negroponte, N. (1995), *Being Digital.* Knopf, New York.

Thaens, M, S. Zouridis en J. Kielema (2002), *ICT en privacy vanuit de burger gewaardeerd (ICT and privacy esteemed from the perspective of citizens),* research paper for the Ministry of Internal Affairs.