

# Knowledge of Society White Paper : 3

Risk Society and Risk Network

Heikki Mäkinen  
Risk Society and Risk Network  
Version 2.0  
10.9.2008

## Risk Society and Risk Network

### Table of Contents

Abstract .....	2
1.Communications Network and Sociality.....	3
2.Information society, Network Society, Risk Society.....	5
Origins .....	5
Network Society .....	5
Risk Society.....	6
3.Risk Network .....	7
Internet as Risk Network .....	7
Risk Network's Risk Profile .....	8
Risk Network and Technical Risks .....	9
Risk Network and Rationality .....	10
4.Network's Technical Information Security and Social Risks.....	12
5.Globalnet .....	15
6.After Risk Network .....	18
Literature .....	19
History of Modifications .....	22

## Abstract

Disinformation or misinformation in modern risk society, especially in network, is a substantial property in this society and depends on the quality of network where information exists. Information in global communications network has not necessarily any connection to social relations people live in.

The analysis of different kinds of social relationships, 'sociality', is based on analysis of interaction on foundation of knowledge relations. Forms of knowledge mediating this relation – knowledge and information - are realised in specific assets. In global communications network must be specified a third form of knowledge, Network Information. Its external carriers can be same as information's, but it is managed on basis of probability. Conceptual information may be, and usually is, 'true' by certain probability, but its meaning as information is definite in a social relationships. Network information is meaningful by a probability depending on risk management of a social relationship. It may be "misinformation, disinformation and out-of-control information", not according to its truth value but by its social consequences.

Security or sociality do not presuppose elimination of risks. Modern social system is never riskless. Security in social relationships presupposes that risks are specified and there are measures to manage them. This is in a very non-trivial sense connected with social in general and its forms in particular.

Risk society means that risk becomes an essential part of social interaction. It has always been present in interaction but in risk society its management becomes part of continuous social relationship which begin to be based on probability.

Communications network is a form of general interaction. Its special features, differentiating it from other forms of interaction, are that it is genuinely global and its rationality, predictability and reliability are determined only in global network.

Risk network is uncontrollable. This property is global. It is dependent on risk network as network build according to logic of social division of labour, as 'network Inter networks'. In risk network, between the levels of organizations and their local area networks, and global level, is build an area which is controllable only by mutual agreements of participants or public authority. Between organizations, in 'society', principles of hierarchy and rules are implemented in operations of state governed by law.

Development of transmission path means that communications is changing genuinely global. Internet's basic logic is not global. From the point of view of technology its structure is passed by, but it is supported by organizations as basic social elements of network, instead of networked formations. In the 'middle area' of organization and global network is an area of uncontrollable risk. It makes Internet a risk network and social formations based on it risk society formations.

## 1. Communications Network and Sociality

“... paradox of the information society ... how can such highly rational production result in the incredible irrationality of information overloads, misinformation, disinformation and out-of-control information. At stake is a disinformed information society” (Lash, 2002, 2).

The existence of disinformation or misinformation in modern risk society, especially in network, is not a paradox at all. It is rather a substantial property in this society and depends on the quality of network where information exists. Information in global communications network has not necessarily any connection to social relations people live in. If communications network is chaotic, has not a special structure or management, it is almost certain that it includes also disinformation and misinformation.

Ultimate conclusion about this may be: “The information society is not primarily a society in which the production of information displaces the production of goods. It is also not primarily a society in which knowledge or information becomes the most important factor of production. It is instead an order in which the principle of ‘society’ becomes displaced by the principle of ‘information’. An order in which sociality becomes displaced by a certain ‘informationality’. Sociality is long-lasting and proximal. Informationality is of short duration and at a distance” (Lash, 2002, 75).

In preference to assume a specific kind of ‘informationality’, it is reasonable to suppose that sociality itself has different forms and is changing. Social relations are based on communication in interaction between individuals (Mead, 1972, 1). Mediating factor in communication can be gestures, spoken language, written language, files, databases. These mediate knowledge in different forms. In general by communication and its mediating forms are build different kinds of Knowledge Relations (Mäkinen, 2008/12<sup>1</sup>, Mäkinen, 2008, 1, 54 – 80), which may develop into different forms of sociality.

Sociality is not to be understood as something that ‘exists in society’. This should presuppose an absolute specification of both social space and time (Mäkinen, 2007/8). Sociality is instead specified by social action; human behaviour where acting individual attaches a subjective meaning to it. Action is social when subjective meaning takes into account the behaviour of other individuals and is oriented according to this (Weber, 1976, 1, Mäkinen, 2008, 1 - 3).

Meaningful social action develops into rational action when acting individual takes an “objective, impersonal attitude toward himself” becomes “an object to himself” (Mead, 1972, 138). Rationality has degrees (Schutz, 1962, 33). In general case concepts ‘interaction’ and ‘rationality’ presuppose concept ‘risk’. When social relationships develop into large, ‘disembedding’ (Giddens, 1990) relationships, orientation to other individual’s behaviour and taking the objective attitude toward oneself, is not possible in immediate experience of individuals, but presupposes Knowledge Relation mediated by different kinds of knowledge. Then management of risk this relation includes, builds a meaning to social action (Mäkinen, 2008, 3 –

---

<sup>1</sup> Documents in yhteiskunnantieto.fi/White Papers series are referenced by year and number in series. These do not correspond to each other; the updated versions of documents keep their original number.

8, 25 – 28, Mäkinen, 2008/12). Orientation to behaviour of 'others' is specified by its probability and consequences and social relation is a 'probable course of meaningful social action' (Weber, 1976, 13).

The formations 'meaningful action', 'social action' and 'social relationship' are developed forms depending on knowledge relation, not elementary forms of sociality. They are based on selections (Bauman, 1990, 112) on foundation of risk management (Mäkinen, 2008, 25 – 26). These social formations are based on probability assessments. This becomes apparent when activity takes place in modern complex interaction environments, especially in communications network.

The analysis of different kinds of social relationships, 'sociality', is based on analysis of interaction on foundation of knowledge relations. Forms of knowledge mediating this relation – knowledge and information - are realised in specific assets. Information has an external carrier, such as document, file or database in which forms it is possible to deliver in communications network. Information is conceptual and explicit. Knowledge assets can be information, but knowledge is realized also as tacit knowledge (Polanyi, 1966) in "dynamic human process of justifying personal belief toward the truth" (Nonaka-Takeuchi, 1995, 58). Knowledge is meaningful for human action.

In global communications network must be specified a third form of knowledge, Network Information. Its external carriers can be same as information's, but it is managed on basis of probability. Conceptual information may be, and usually is, 'true' by certain probability, but its meaning as information is definite in a social relationships, as in continuity dominated social formations or scientific community. Network information is meaningful by a probability depending on risk management of a social relationship. It may be "misinformation, disinformation and out-of-control information", not according to its truth value but by its social consequences. Global information is represented in two forms: tacit knowledge in social action and network information. Conceptual information instead is always confirmed in certain continual social relationship (Mäkinen, 2008/12, Mäkinen, 2008, 56 - 62).

Concepts 'long lasting' and 'proximal' (sociality) or 'of short duration' and 'at a distance' (informationality) are problematic in the same way as concept 'society'. When social interaction is based on consideration of risk and continuity of its management, the social concepts of time and space are possible to specify by these concepts. Then socially global, 'extension', is specified as a social relation by a risk probability equal to 1 and social history, 'time', as probability of continuous social relationship. Sociality is continuum of global and history. It consists of coherent social action mediated by coherent social knowledge, having these dimensions (Mäkinen, 2007/8, Mäkinen, 2008/12, Mäkinen, 2008, 3 – 8).

Communications networks are in modern society environments where processes are situated and where knowledge is created, delivered and protected. Networks can be managed or not. The latter may be called Risk Networks. In them there can exist network information, also disinformation and misinformation, but confirmed conceptual knowledge presupposes continuous social relationships which are mediated into immediate activity by tacit knowledge.

Information and knowledge are both global. But environments where knowledge, conceptual or not, is concerned, must have a social structure. Network Information can exist without such a structure. In environments where knowledge is concerned, risks must be specified and managed by the ways services using knowledge require. In risk management environment dominated principally by social division of

labour, is build continual social relationships requiring respective forms of interaction and knowledge.

"We may define 'security' as a situation in which a specific set of dangers is counteracted or minimised. The experience of security usually rests upon a balance of trust and acceptable risk" (Giddens, 1990, 35 - 36). Actually the same content was given to concept 'sociality'. In network environment concept 'security', especially 'information security', has not any more its traditional meaning. In social formation where activities are dominated by organizations, it is apparent what has to be considered by information security: it requires protection of organization's information according to its objectives, for example business secrets or administrative organizations objectives against outer threats. This is risk management environment in social division of labour. It is also typical to sociality in social division of labour and organization's in competition with each other. When risk management environment develops into global network, risk management, and also security, cannot be based on information protection, but on its meaningful treatment in social action.

Security or sociality do not presuppose elimination of risks. Modern social system is never riskless and risks cannot be handled by faith or tradition (Beck, 1986, Giddens, 1990). Security in social relationships presupposes that risks are specified and there are measures to manage risks. This is in a very non-trivial sense connected with sociality in general and its forms in particular (Mäkinen, 2008, 6).

## 2. Information society, Network Society, Risk Society

### Origins

The concept 'Information society' was first proposed by Tadao Umesao at 1960's. Main sociological discussion started at 1970's from the theory of 'post-industrialised society' (Bell, 1973). According to it the social development had reached a phase where society and economy were governed by factors different than in industrial society. The change of occupational structure should direct towards service and later into information professions.

The change in professions is clear, and also the increasing use of knowledge and information in production and administration. But the remarkable social change in reference to them, change comparable to inception of capitalism and industrial society, has been an open question. Almost every information and communications technology change has begun before the breakthrough of ICT-technology (Castells, 2000a)<sup>2</sup>.

### Network Society

Activities and processes of society are increasingly formed around networks. This development has started long ago, if it is not generally a characteristic feature of society. Information technology however provides "the material basis for its (networks) pervasive expansion throughout the entire social structure" (Castells, 2000a, 500; Castells, 2004b).

---

<sup>2</sup> Webster states that Castells seems on the one hand emphasise the change depending on ICT-technology, but on the other hand continuity and states that the central features of capitalism remain (Webster, 2002, 100). Castells' theory is theory of 'informational capitalism' (Castells, 2000a, 18 - 21, Castells, 2000b) or 'informationalism' (Castells, 2004b, 8 - 13).

Network society is further capitalism – if it consists of organizations and enterprises working in social division of labour, according to profit seeking rationality. Typical, compared with former capitalism, is that network society is global and constituted about networks of capital movements (Castells, 2000a, 502). Global network society or economic activity are not new phenomenon but their modern technological infrastructure is (Castells, 2000b, 52; Castells, 2004b).

The concept 'Network Society' is problematic if its aim is to compensate the concept 'Information Society'. Concept 'network' may denote much more than communications network, but it is hardly discussed about essential matters, if analysis concerns only networks but not the importance of knowledge in social interaction and change. Significance of concept 'network society' is that it denotes that social system is not hierarchical but consists of equivalent partners. Non-hierarchy depends more on managed knowledge than on its management in network. The latter is however prerequisite of non-hierarchy. The social content of activities is depended on trust in network. It can in non-hierarchical system be constituted only between network's participants, organizations or persons.

Information society is global, and this considers all social phenomena, not only economics. Global in economics is property of capitalism. Global in all the other social phenomena is property of information society, network society, and – at the same time – risk society. Then social order does not consist of organizations, bureaucratic rationality, classes, or rationality based on profit seeking. It consists of global knowledge and social interaction mediated by it. There meaning of knowledge is based on risk management and probability.

Concerning risk management social division of labour and organizations in global network are a problem. All participants must manage their risks by themselves, but no-one manages risks in network; except economic relationships. But all the other social relationships should be managed globally too. Network's structure must support this.

Information society - or 'information age' (Castells) – may be capitalism, which uses ICT-technology. It is clear that technology society is using has changed in, but it is not clear that the functioning of society has changed. If the question is about social change to be compared with the inception of capitalism, the most indicators describing information society are senseless.

### **Risk Society**

The hypothesis of ICT-technology as a basis for deployment of networks into whole social structure becomes problematic by the dominant communications network paradigm – Internet. As a social description of it seems to suit, instead of 'Network Society' or 'Information Society', totally an other hypothesis: 'Risk Society'. It is anyhow questionable is it possible to form any kind of social relationships on basis of Internet.

Risk Society is build on that in post-industrial society exists a new type of risks, 'post industrial Grand threats' (Grossgefahren), which cannot be managed by means of risk management (Beck, 1986, also Beck 1988, 1997, 1999, 2000, Giddens, 1990, 1991, Beck – Giddens – Lash, 1994). Question is often about modernisation risks depending on knowledge (Beck, 1986, 35), which follow from application of knowledge into the nature, 'socialized nature' (Giddens, 2001, 65;

Giddens, 1990, 124). Modern society is always risk society but in the 'second modernity' (Beck) characteristics of risks change.

Risk society is not a society where exists risks. Instead there exists threats or dangers which are not possible to specify as risks and managed according to this. Threats are in sense of risk management managed, if it is possible to specify probability and consequences of threat. After this it is possible to plan the measures by which risk is managed in an acceptable way. Acceptable risk is specified, described and the measures to manage it are planned.

To a Grand Risk it is not possible to specify probability and its consequences are impossible to assess. Furthermore for consequences exists no socially regulated or reasonable means of management. The realisation of a threat does not mean the formation of risk society phenomenon but its realisation in an unforeseen and uncontrollable way does mean.

Grand risks are global (Beck, 1999, 2000, Giddens, 2001, 65 – 69). Environmental threats may concern anything and anybody, consequences of gene technology may be directed to anyone and whatever, virus attack can spread out in communications network anywhere. This uncontrollability and unpredictability is a central feature of Grand risks.

Risk society means that risk becomes an essential part of social interaction. It has always been present in interaction but in risk society its management becomes part of continuous social relationship which begin to be based on probability.

Actually risk society is developed when risks are genuinely uncontrollable, also on basis of probability. Things can genuinely go awry ... globally.

### 3. Risk Network

#### Internet as Risk Network

Internet can be analysed by the concepts 'Risk Society' and 'Risk Network'. Typical to it is 'openness', which crystallizes in three features:

- communication technology is based on dynamic routing which transfers network packet principally through any route, can use any router in the network,
- nodes can be connected to the network without regulation,
- at service level – as in web-services or email – whatever node, user or file in network is principally within reach by any other node or any other user.

Internet's success has been based on these properties. Its special advantage is dynamic routing by means of which network has challenged every increase in network loading. The other properties have created the glory of Internet's usability and 'freedom' – or illusion of them.

In basic Internet cannot be specified a totality, a social relationship, where it is possible to make a risk assessment. In this sense Internet has no information security or any other kind of service level<sup>3</sup>. This depends on the principal properties of Internet described earlier. These properties make it 'a common, undivided

---

<sup>3</sup> A minimum information security must exist also in Internet; otherwise it should not work at all. This may be called a zero-level information security (Mäkinen, 2005/2, Mäkinen, 2007/10). It includes cryptographic measures to protect the information flow, treatment of malicious software (f. ex. viruses), firewalls and communications services required to identification of network entities (IETF, RFC 3631).

media', where message can spread out unrestrictedly. At the same time these properties mean that network can be listened unrestrictedly – and so is done. The content of messages can be monitored for example by certain key words – and so is done. Messages coming to a router can be captured, stored and settled on keener investigation, even though after years – and so is done. When a message can spread out anyhow, viruses and spam can spread out unrestrictedly and uncontrollable. Carrying out a denial of service attack is simple.

Sun Tzu wrote: "The superior militarist strikes while schemes are being laid" (Sun Tzu, 2005, 35). One must attack against the strategy and plans of enemy.

In Internet it is impossible to act according to this advice, because the strategy of 'enemy' is based on the structure of network, its operation logic and ideology of 'freedom' and 'openness' of network.

### Risk Network's Risk Profile<sup>4</sup>

Risk network's risk profile may be specified by following features.

1. Risks are global. Every or several people are influenced by accidental events. For example virus protection should be arranged in every node which participates in communication with each other. Consequences spread out in network accidentally or optionally to every node which is not protected.
2. Risks are based on risk environments. It is developed institutionalized risk environments, as economic and administrative activity in network, which influence on living conditions of people. These are build on basis of risk calculation by supposition that the security arrangements created are sufficient for activities in frame of acceptable risk. This however depends on independent activities of organizations or people (point 1).
3. The experience of security is based on balance between trust and acceptable risk. Trust is based on assessment by expertise in communications and information security.
4. There exists a consciousness about risk as a risk. Consciousness is widely diffused: threats of communications network are well known.
5. Consciousness of the limits of expertise: any system based on expertise is not without defects and there is no exact information what follows from its foundations.

Accidental risks, their treatment by independent activities on the other hand and institutionalized risk environments on the other build a contradiction. On foundation of independent activities in social division of labour, as for example in local area networks of organizations or their co-operation, is not possible to create risk management supposed in global network. Risk management cannot either be implemented on foundation of procedures typical to these kinds of social formations, as fixed rules; they must rather be based on probability assessment.

The other contradiction is between consciousness of existence of risks in society and foundation for their treatment by expertise. Risk consciousness is wide; the whole risk management in Internet rests on that all users in network are aware of risks. On the other hand consciousness of the limits of expertise is also wide. The consequence, that by encryption or smart cards could be build a reliable scope of activity, is not trusted; not even when factual reasons exist. By these prerequisites it is not possible to develop social trust required in institutionalized services.

---

<sup>4</sup> Following has a connection, in reference to communications network, with 'the risk profile of modernity' presented by Giddens (Giddens, 1990, 124 – 125, also Giddens, 1990, 33 – 36).

### **Risk Network and Technical Risks**

The technical structure of network is a reason for Grand threat. The flooding or blocking of network by normal traffic is not a genuine threat – though network can partly or temporally be blocked by a denial of service attack. The technical breakdown of Internet because of traffic overflow is predicted at regular intervals, but up to now Internet has got through very well - due to dynamic routing.

Network services however have turned out to be liable to crises. Service problems are accidental events from the point of view of network's user. Virus protection in a system is possible to accomplish effectively and service providers can manage it also at network level, but it is principally accidental, is this really done. If these accidents realise, viruses can at network level produce unforeseen damage; and it is not possible to cease this. Filtering of spam at servers can also be effective, but it can anyway produce an unforeseen damage at network. Great deal of network's email is spam. Spyware programs can spread out anywhere.

Risk management cannot be implemented in a reliable way at the network level. In a separate system it presupposes continuous update of operating systems, communications programs, virus control and regular use of programs which erase malicious software. It presupposes also firewall which breaks the end to end logic of Internet.

In general every detail in Internet is possible to manage by risk assessment. But from the point of view of user they are accidental incidents. For management of risks in a whole network there exist no algorithm or procedure. Risk management is driven to individual level: responsibility on risk management activities is always at network's user. Network itself has no service or information security level.

Network's services must be based on solutions which come up from the risk assessment. Central problems are prevailing confidentiality of information and transmission of all information into the right address and only there.

Against networks listening and capture of messages one can protect itself by cryptography. The revelation of content of transfer – confidentiality – can be prevented – for a certain time – by encrypting messages. Integrity of transmission – all packets of the message have been transmitted – can be checked by cryptographic checksums. So is found out that message has transferred totally and in a right format but capture of message cannot be prevented. Denial of service – availability of network – can be prevented by cryptography. For example every email-message or transmission packet can provide a certificate and email-service or router can accept only one message or packet which has this certificate and reject all the others. Denial of service attacks are also possible to manage by differentiated services with the same principle, but without cryptography, by regulating transmission at the boundary of the service (IETF, RFC 2475).

By cryptography it is further possible to build a connection between users or nodes over a connectionless, dynamically routing, network, where participants are identified and authenticated. These solutions are known as PKI – Public Key Infrastructure and VPN – Virtual Private Network. Into these concepts, accomplished by firewalls, is based the information security which in practice is possible to implement in frames of bare Internet-logic.

The breaking of encrypting algorithms is very improbable if the length of encryption key is long enough. By these algorithms it is possible - at certain time interval - have a technically zero-risk system in relation to information's confidentiality and a small risk system in relation to other threats. But this does not mean that the system is socially riskless or its risks specified by probability and consequences.

All the time in network exist certainly thousands of machines which are trying to break encryption. Those who are aiming to decryption have networks of their own, where they exchange information efficiently. And this refers only to individual persons, 'hackers'. States have activities of quite another scale. Information security can be reached only if the length of encryption keys is regularly irregularly increased and algorithms stay ahead the breakers<sup>5</sup>. By separate activities network protection is possible to reach only to a certain time interval. It is not possible by encryption to protect for example information in long-term storage or information whose value otherwise prevails in the long run.

Encryption is however a quite reliable way to protect information. But it presupposes a risk assessment which specifies how long information must be protected, for example to be confidential. If this is not done, situation is unstable. It must be outlined what kind of information is possible to use in network. In this case too information security is totally dependent of the activities of the network's user.

The breaking of encryption or forgery of information, breaking confidentiality or capture of information, are social credibility problems, although they are essentially more difficult to accomplish than for example forgery of passport or identity card. The validity of the latter is however controlled all the time. But if information moves in network without control, its forgery or listening is not necessarily observed; information can reach its destination as valid or valid-looking but has however been involved in wrong hands or used in a way which user has not intended. Probability that a separate encryption key reveals or is caught in wrong hands can be assessed and its consequences estimated and managed with the methods of risk management. But it is impossible to control how information which has been 'released' in this way is spread out in the network.

Communications network is global and transmits information globally. It cannot be compared with other forms of information transmission. In global communications network information can genuinely be imperishable.

### **Risk Network and Rationality**

Communications network is a form of general interaction. Its special features, differentiating it from other forms of interaction, is that it is genuinely global and its rationality, predictability and reliability are determined only in global network (Mäkinen, 2008, 216, Mäkinen, 2007/8, Mäkinen, 2008/12).

In network exist no hierarchy and rules specified on basis of it. The only guarantee for predictability and reliability is information security. Social division of labour and organizations operating in it do not guarantee security, and in global environment

---

<sup>5</sup> There are more effective ways to break encryption than breaking algorithms. Such are for example corrupting key person, breaking into the premises of firms generating smart cards, stealing a card or abuse of a card found. These are however quite 'normal' risks which can be managed by risk assessment. Measures against them are possible to plan and to diminish risks to an acceptable level.

either states, not even in the case they are operating according to principle 'network state' (Castells, 2004c, Castells, 2004d).

The uncontrollable properties of risk network are global. They are not dependent on unique factors or risks, but on risk network as network but on the other hand build according to logic of social division of labour, as 'network Inter networks'. An occasional information security attack – for example a virus send into the computer of public authority or enterprise to deliver information out there - can in principle be extremely harmful, but from the point of view of risk management there is nothing special in it. It can be predicted, its probability and consequences are possible to specify and measures to be planned. Measures can be successful or not, but there is a risk to be calculated. Same concerns also massive network attacks which aim to paralyse for example government offices.

In risk network between the levels of organizations and their local area networks and global level, is build an area controllable – according to this logic – only by mutual agreements of participants or public authority. Rationality in organization presupposes hierarchy and organizational rules according to which are acted. This order is not rational, predictable and reliable depending on action itself. Between organizations, in 'society', principles of hierarchy and rules are implemented in operations of state governed by law.

Internet's, actually IP-protocol's, logic is build on rationality based on social division of labour, separate organization operating in it and local area networks. Between them are created connections. In such an environment a global system is build only supposing that units in division of labour are producing commodities. In basic IP network commodities cannot be constituted, if there is not possible to determine information security and service level. This is possible in certain degree by virtual circuits or differentiated services build on foundation of IP. Either SMTP-email, FTP-filetransfer, DNS-nameservice or http-network protocol do not develop products or commodities (Mäkinen, 2008, 228 – 234) .

In social division of labour separate information security solutions do not create probable social relations in network environment. Their development presupposes rationality based on ubiquitous knowledge, ubiquitous network and - above them - global risk management constituting logical networks. This is called network rationality. The genuine information security, constituted on Bindings, identification, authentication and non-repudiation, (CommonCriteria, Mäkinen, 2008, 91 – 96) between individuals, is developed in information society services.

Basis for network rationality is global knowledge relation. It – among other things – presupposes understanding the information security, not as protection of information, but its transfer and delivery according to objectives. In Internet objective is too - in principle - global availability of information and end-to-end connection and usability between network resources. Internet is however one special case of arrangement; special case where are not determined quality, service or information security criteria or level to availability of information or other services in network. The basic property of Internet, or risk network in general, is its basic logic of logical network which does not allow development of genuine network rationality. Communication services used in Internet however allow it.

Organizational rationality, as for example bureaucracy (Mäkinen, 2008/12, Mäkinen, 2008, 37 – 41), in network, mean that information security and sociality are not possible to specify. This builds a risk network, usually Internet. Network

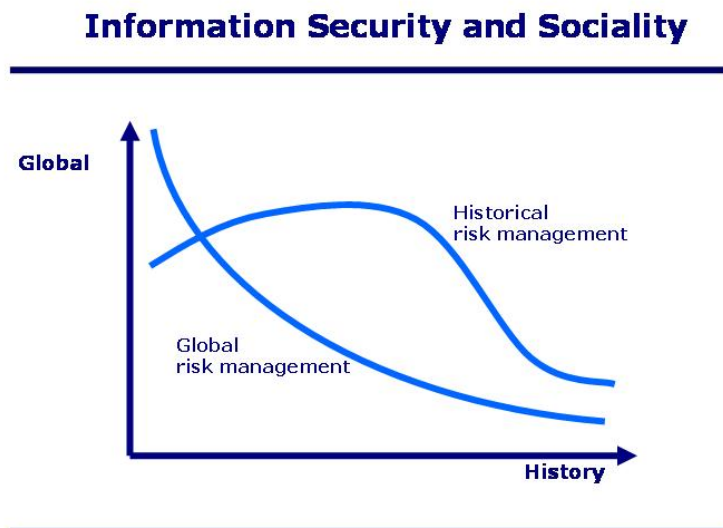
rationality means management of information security and sociality in network. Its organizational form is information society service and its network Globalnet.

#### 4. Network's Technical Information Security and Social Risks

Information security solutions by global measures in Internet-type network are possible only based on technological protection procedures. Technology as such is not important in this connection but it carries the global dimension of information security. By technical means of protection is not possible to manage **social** risks in an Internet-like network. This is the key problem.

Global technological measures are principally based on cryptography. When Internet's security problem is social in principle, it is not particularly interesting to discuss about the probability of breaking encryption algorithms: in any case it can be proved to be very small – if the key-length is increased. This breaking is not excluded and if it happens for example in RSA-algorithm which is basis for asymmetric encryption and PKI, no-one can forecast consequences. This is not a risk but a real Grand Threat.

More important than the probability to break information encryption, is how information protection, its life time, self-life (Lloyd, 2007), is related into time and interest for information revelation. Social trust build on technical protection is dependent on that. It influences to information life time almost linearly: incidents threatening information viability may in global environment be considered accidental. Technical information security influences events principally in the same way; information's global applicability is reduced steadily by increasing duration. If in risk management environment is possible to increase social meaning, for example in organization or information society service, development may be possible to change. Sociality is build on relationship of global and history.



Information security level is determined by objectives established for information protection. In this sense level is constant in relation to information security measures. It is based on risk management changing the relationship of global, risk, and history, probability, in social relationship.

If these are developing accidentally, the relationship of global and history is changing according to function 'Global risk management'. Social relationships constitute according to it in global network, as in Internet. It is a social relationship where knowledge is concerned as network information, whose risk is managed at this level. Depending on technical solutions, as communications and program solutions, their importance is changing, and the level of function 'arises'. Importance of this is essential: technical security is cheap and social security expensive; it is important that technical security reaches the greatest potential share of total security.

In rational social relationships, as in organization or in other socially meaningful relationships, is build a continual social relationship according to function 'Historical risk management'. In organization and information society service knowledge is determined as socially meaningful, conceptual and in activity connected knowledge.

The assessment of social trust, created by technical security, should identify risks directed to information, as interest, and time. Their confidentiality, integrity and availability should be preserved. This presupposes definition of risk management environment. Into it are further directed the same risks as in global environment, but their management can be specified by acceptable probability.

In network the social whole is affected by so many factors out of control of network user, accidental to him, that user hardly can forecast this whole. User should just trust the system. But consciousness of networks threats is wide, well diffused and knowledge about insufficiency of protection methods widely deployed. Social trust is not developed. Either trust according to relation 'Historical risk management' is not absolute, but it is probable enough.

It is irrelevant, is protection of information sometimes broken: when its probability increases, increases also uncertainty. When network has not a service-level, it can be managed only by social risk management: network or other technology gives no chance to management. And risk management is on a non-hierarchical environment on one's own responsibility.

This is a relative matter. It is possible to specify such communications situations where technical protection, for example by cryptography, certification and smart cards, is quite sufficient from the point of view of activity. Such is for example electronic signature, which must be protected only so long it is verified that subscriber is the one he insists. After this protection of signature is at the responsibility of archiving: it should create systems by which the verified document is stored. This system guarantees the validity of signature, although the algorithm it is based on, would sometimes be improper.<sup>6</sup>

The other example is purchase in network. Need for its protection ends when money has leaved the account. This presupposes that in network is not left over - for certain time - information concerning the purchase, as for example number of credit card. If identification happens for example by services of banks, there is almost a zero-risk.

In general at activities required by eGovernment-services and eBusiness, the protection events require is so short-term, that the methods used can be

---

<sup>6</sup> Electronic signature's becoming general increases significantly the importance of archiving in the activities of organisations. The certification of archiving activities must began in some phase. For this purpose shall in future probably be a standard.

considered reliable, if former conditions are fulfilled; supposing that information is not left over in network somewhere. Anyhow it is not a question of technical reliability but reliable social institutions carrying out this technology or lack of them. Reason to trust on bank card is smaller than reason to trust on communications connection based on use of smart card, and it is not trusted but the banks.

Network storing and developing relevant information considering social action can in Internet be implemented utmost by firewall. This however breaks Internet's end-to-end principle, and thus information's universal viability, and foundation of network rationality. If information is located into general Internet, it is possible to gather, and so is surely done, somewhere. Its management is out of control of information owner.

The equilibrium of acceptable risk and trust constitute information security on whose foundation sociality may consist in. This is possible only if risks on environment and rational action according to this are possible to specify.

The social significance of cryptography in network depends on trust directed to it. It is an abstract system based on expertise which are typical to modern society (Giddens, 1990, 1991). Its contents are abstract for network's users and are understood properly only by experts.

This as such does not distinguish communications network from other abstract systems of society. They are always based on specified knowledge which is somewhat opaque from the point of view of 'lay-men'. "Specialisation is actually the key to the character of modern abstract systems" (Giddens, 1991, 30). Social activity in modern society presupposes trust to the system from side of people who are acting on it.

In case of Internet consciousness of risk level is higher than trust on its social relations. Spam, viruses, spyware are well known threats and quite well seems to be known also that it is always possible to break encryption. It is evidently impossible to diminish the risk to the level where network solutions have trust required by the reliable working of eGovernment or eBusiness services otherwise than by specifying social relationships in network whose risks are manageable.

Network can be listened and information gathered and centered on databases which are used for example in commercial purposes, control or revealing business secrets. In Internet it is however impossible to create social relationships where for example commercial interests should delimit network listening; in other words: where service providers should on commercial reasons be obliged to prevent it. The physical structure of network is practically under control of commercial operators, and thus at that level control is principally possible, but in Internet's network operations and services not. Interactivity and reciprocity of control based on network's surveillance and listening could in global economic system in practice be created only by competition. If it does not exist, surveillance can contribute to activities which are against the benefits of network's users<sup>7</sup>. On the other hand by Internet it is possible to promote democracy, for example to act independently of totalitarian governments.

---

<sup>7</sup> In media is on regular intervals presented as 'news', that USA and some of its allies have a system called ECHELON which is listening network and gathers information from it. This is news as little as that all the other great powers have a same kind of system. – The war against terrorism seems to offer to states good grounds for network surveillance. A fact however may be that the most important application for information gathered in this way is revelation of business secrets.

At least characteristics of Grand Risk in Internet are fulfilled continual preparing to virus attacks, spam<sup>8</sup> and spyware and the race of encryption and its breakers and inability to specify what is a sufficient protection level in relation to time and interest for revealing information. And the last threat the inability to control the network. Risks are impossible to specify according to these features. They are accidental matters from the point of view of network's user and he is very conscious of them. The more user knows about the network and its functioning, the less he trusts on it.

As single factors these do not fulfil the characteristics of Grand Risk but they become ones through networks technical structure where messages and problems can spread out unrestricted. All protection activities are dependent on users, who often have not enough information or skill, not even firms. Probability of threats cannot be specified and consequences cannot be estimated and there is no social procedure to regulate them. The only way to react is continual uncertainty and race which can be limited only by individual risk assessment. Its quality and efficiency depends on know-how of individual. This results in inequality of network users and the 'individualisation of social inequality' (Beck, 1986, 85).

Here is not developing a network structure which should support the mutual trust of participants.

In Internet risk management is totally at separate social unit's level. But it exists anyhow. In that sense Internet is a foundation for a social relationship. It is aiming at the boundary value of sociality. That may be called 'chaotic sociality' (Mäkinen 2005/1).

## 5. Globalnet

Communications network is a form of social interaction. The foundation of its change is development of transmission path. It is not the 'cause' of development; as well it is possible that network is not implemented, if there were not social interaction, or at least network should not have meaning and importance. The development of transmission path changes the risk management environment where socially meaningful relationships are determined and changes thus these relationships self.

Development of transmission path means that communications is changing genuinely global. Internet's basic logic is not global. Its foundation is development of connections for separate networks - based originally in organizations and their local area networks. From the point of view of technology this structure is passed by, but it is technically supported by IP-routing and especially appearance of organizations as socially basic elements of network, instead of networked formations. In the 'middle area' of organization and global network is an area of uncontrollable risk. It makes Internet a risk network and social formations based on it risk society formations.

---

<sup>8</sup> If VoIP (Voice over IP) spreads out in network in a same way as email, it is possible to confront by same kind of disturbance as spam. The problem can be even bigger: voice uses bandwidth much more than data-message and by it is possible to make more damage. If this is not prevented, it is clear that Internet calls will be disturbed as soon as there are remarkable economic values in VoIP. Then we have a glorious 'new information society': mail is not delivered and phone does not work.

The development of network structure based on acceptable risk and trust required presupposes that network is build on both components of sociality, global and on historical probability based components, and security of them both. Events which are considered are same. When they are historically probable, they are in area of acceptable risk and can constitute socially meaningful relationships. This forms a continuum of network's service- and security levels according to the requirements of specific services.

This totality is called **Globalnet**. It is the communications network of information society (Mäkinen, 2008, 282 – 338). Internet is one special case of it where it is realised a zero-level service and information security level.

Global network corresponds global social organizational formation, **information society service**. Organizations and their co-operation are going to represent a special case of information society service. The rational form of interaction is based on network. The socially meaningful totalities of communications network are build on information society services and thus also network security. Network's information security is not merely a presupposition for service but also a result of their security. Information society service is a relationship of global and history. There are concerned same risks as in global network, but they are managed by acceptable probability.

Information society services reside on logical network constructions which are views of global communications transmission path. These views are based on information security policy, specified for service. On its background can be one or several organisations or it can be based on general, for example on standards based, information security policies. Network totality, logical network, can be constituted on foundations of whatever social relationship. Their development takes place on risk management. Information security is based on bindings of particular levels. Organizational formations are based on these.

Into communications network is constituted social risk management environments. They are particular relationships of global and history. Depending on this relationship is constituted for example organizations separate local area networks and logical networks on foundation of information society services<sup>9</sup>. From the point of view of information security their management, and risk management, is a principal social element, as action is generally a principal social element. Information security should be understood as meaningful social action and process of its meaningful development (Mäkinen, 2008, 100 – 122).

Development of risk management, information security, organizational formations and network constructions is based on action which is characterized by rational selections in a historically continuous environment. These selections are adapted into risk management environment constituting the global dimension of risk management. 'Real' are only historical events, incidents, threats, security measures and management activities.

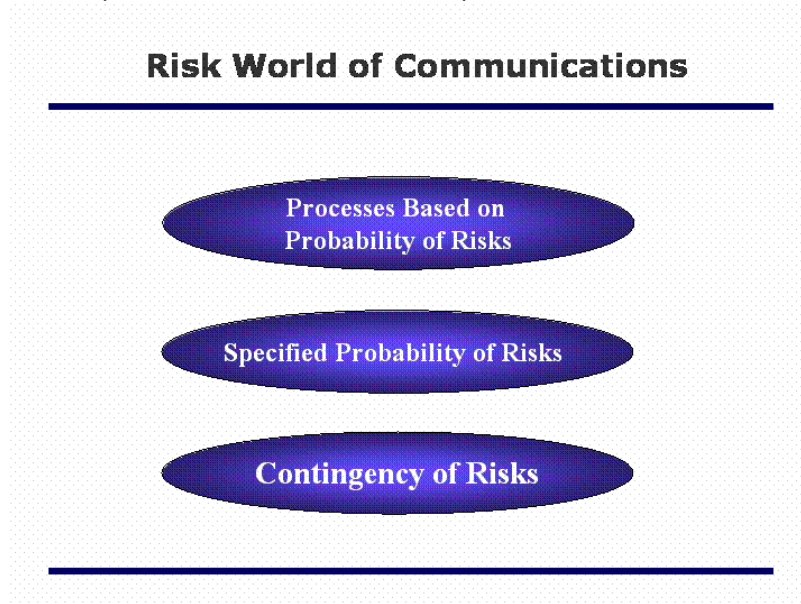
The foundation for organization's local area network is social division of labour. It has no global connection; in such environment global is based on production of commodities. Risk management environment is dominated by continuity.

---

<sup>9</sup> Organization as form of socially meaningful interaction and risk management environment is older than communications network in the modern sense. It is however interaction environment and based on communication in this sense. In this sense organization's local area network is a relic from time before network.

Information society service and its network basis is genuinely global environment and risk management environment is dominated by risk.

Risk management environments constitute three layers determining the service structure of network (Mäkinen, 2008, 222 – 228).



The basis of network is transmission path. It has no special social structure but it is global platform for information. It has as such no information security; incidents appear as contingent risks. In transmission path is implemented management environments of communications – historical dimension of risk management - where are applied various technical security requirements.

Specification of risks by probability and consequences builds logical network environments. Risk management environments are foundations for processes where are produced, delivered and stored information and knowledge. They are build on basis of management as Bindings. They can in social division of labour form functionally local area networks of organizations, and have a technical spatiotemporal structure, or be formed according to information society service specified virtual networks (Mäkinen, 2007/8, Mäkinen, 2007/11).

Organisations' processes are implemented according to specified risks by means of communications services.

On this risk management basis the socially organized structure of network is developed as follows:

## The Structure of Network

---

Applications Services

Logical network environments

Transmission path

---

Transmission path is an ubiquitous, technologically coherent, coincident and contingent space-time system. Network has special social structure only in logical networks. On their basis are build information society services, organizations and processes connected.

Logical network environment's constitution by risk management and information security presupposes specification of connection between users, persons, nodes or services, and object by identification and authentication and non-repudiation of communication. Then connection is build as Binding (Common Criteria, Mäkinen, 2008, 91 - 96).

The only relevant characteristics of information society, distinguishing feature in comparison with other social formations, is that it is global. Process where it is constituted should be called **genuine globalisation** compared with **pre-globalisation** based on worldwide economic interdependence due to transfer of factors of production.

## 6. After Risk Network

Social action is spatio-temporal. Communications network has spatio-temporal dimensions when it is connected to logical networks of information society services, organisations and processes situated in them. In network it is possible to construct social systems, as for example certification services, which are required for management of social processes (Mäkinen, 2006/7).

Network's of companies and authorities are build according to the concept of logical network. Only few organisations make their communications connections on Internet's ground. 'Internet-services' of authorities or commercial organisations are (in Finland) such only in commercial sense: in principal Internet is utilized only in user interface of an individual. When this is substituted by connection authenticating itself directly to transmission path or logical network, 'Internet' fades away.

If network is defined by logical networks and information society services carried in them, communications network shall not be riskless. Onwards it is possible for example to listen transmission, pick up messages from it and gather databases

from these messages. But by agreements and by setting requirements to information security of network actors, as service providers, certifiers and agreement partners, risk can be identified and managed. If path of message is possible to detect, it is also possible to know whose network was accessed. Alike it is relatively well known which are the groups doing network monitoring. Risks can be specified, there are possibilities to avoid them and to repair the consequences of risks.

Internet is a phase in the history of Globalnet. All properties in Internet, which user needs, as global accessibility of nodes, users and files, are possible to have also in an information secure way, which however is not absolute but probable, based on accepted risks. The paradigm of global accessibility and availability of information is possible to preserve.

Society is still risk society: modern society is always. But basis for social activities can be communications network where risks are managed by a way reasonable in commercial and administrative activities.

### Literature

- Beck, Ulrich: Risikogesellschaft. Auf dem Weg in eine andere Moderne. Suhrkamp, 1986
- Beck, Ulrich: Gegengifte. Die organisierte Unverantwortlichkeit. Suhrkamp, 1988
- Beck, Ulrich: The Reinvention of Politics. Rethinking Modernity in the Global Social Order. Polity Press, 1997
- Beck, Ulrich: World Risk Society. Polity Press, 1999
- Beck, Ulrich: What Is Globalization?. Polity Press, 2000
- Beck, Ulrich – Giddens, Anthony – Lash, Scott: Reflexive Modernization. Politics, Tradition and Aesthetics in the Modern Social Order. Polity Press, 1994
- Bell, Daniel: The Coming of Post-Industrial Society, Basic Books Inc. Publishers, 1973
- Castells, Manuel: The Rise of the Network Society. Blackwell Publishers, (second edition), 2000a
- Castells, Manuel: Information Technology and Global Capitalism. Teoksessa Hutton-Giddens, 2000b)
- Castells, Manuel (ed): The Network Society. A Cross-Cultural Perspective. Edward Elgar Publishing Ltd, 2004a
- Castells, Manuel: Informationalism, networks, and the networks society: a theoretical blueprint. In Castells, 2004, Castells, 2004b
- Castells, Manuel: The Power of Indentity. Second Edition. (The Information Age: Economy, Society and Culture, Volume II). Blackwell Publishing, 2004c
- Castells, Manuel: End of Millennium. Second Edition. (The Information Age: Economy, Society and Culture, Volume III). Blackwell Publishing, 2004d
- Common Criteria for Information Security Evaluation, Version 3.1 and 3.0, ([www.commoncriteriaportal.org](http://www.commoncriteriaportal.org))
- Giddens, Anthony: The Consequences of Modernity. Polity Press, 1990
- Giddens, Anthony: Modernity and Self-Identity. Self and Society in the Late Modern Age. Polity Press, 1991
- Giddens, Anthony: Sociology. 4th edition. With the assistance of Karen Birdsall. Polity Press, 2001.
- Giddens, Anthony (ed): The Global Third Way Debate. Polity Press, (2001b).
- Hutton, Will – Giddens, Anthony (eds): Global Capitalism. The New Press, New York, 2000.
- IETF, Internet Engineering Task Force, RFC, 2475: An Architecture for Differentiated Services, ([www.ietf.cnri.reston.va.us](http://www.ietf.cnri.reston.va.us))

- IETF, Internet Engineering Task Force, RFC 3631: Security Mechanisms for the Internet
- ISO/IEC, International Standardisation organisation, Standard 27001: Information Technology - Security techniques- Information Security Management Systems – Requirements, 2005
- ISO/IEC, International Standardisation organisation, Standard 27002: Information security management. Code of practice for information security management systems, 2007
- ISO/IEC 27005, International Standardisation organisation, Standard 27005: Information technology - Security techniques - Information security risk management, 2008
- Lash, Scott: Critique of Information. SAGE Publications, 2002
- Lloyd, Bruce: Knowledge Management: What has wisdom got to do with it?. Teoksessa Rikowski (ed), 2007
- Mead, George Herbert: The Philosophy of the Present. The University of Chicago Press, 1980 (original 1932)
- Mead, George H.: Mind, Self, and Society. From the Standpoint of a Social Behaviorist. The University of Chicago Press, Chicago and London, 1972 (original 1934)
- Mäkinen, Heikki: Yhteiskunnan tieto. Acta Universitatis Tamperensis ser A vol 381, Tampereen yliopisto, Tampere 1993 (in Finnish)
- Mäkinen, Heikki: Yhteiskunnan tiedon turvallisuus, 2008, Versio 2.0 (In Finnish: Knowledge of Society: Security, Version 2.0), yhteiskunnantieto.fi
- Mäkinen, Heikki: Risk, Trust and Security, 2005, yhteiskunnantieto.fi, White Papers 1
- Mäkinen, Heikki: Globalnet and Knowledge of Society, 2005, yhteiskunnantieto.fi, White Papers 2
- Mäkinen, Heikki: For Development of ISMS standards, 2006, yhteiskunnantieto.fi, White Papers 4
- Mäkinen, Heikki: Globalization: Information, Knowledge and Networks, 2006, yhteiskunnantieto.fi, White Papers 5
- Mäkinen, Heikki: Knowledge Society or Information Society, 2006, yhteiskunnantieto.fi, White Papers 6
- Mäkinen, Heikki: Globalnet as Directories of Information Security Profiles, Version 2.0, 2006, yhteiskunnantieto.fi, White papers 7
- Mäkinen, Heikki: Space, Time, Sociality, 2007, Version 4.0, yhteiskunnantieto.fi, White Papers 8
- Mäkinen, Heikki: The Social Foundations of Knowledge Management, 2006, yhteiskunnantieto.fi, White Papers 9
- Mäkinen, Heikki: The Social Foundations of Information Security, 2007, yhteiskunnantieto.fi, White Papers 10
- Mäkinen, Heikki: The Social Foundations of Information Society Services, 2007, yhteiskunnantieto.fi, White Papers 11
- Mäkinen, Heikki: Information Society Services and the Change of Social Rationality, 2008, Proceedings of EBRF-2007 conference 26.9.2007, ebrf.fi, yhteiskunnantieto.fi, White Papers 12
- Nonaka, Ikujiro - Takeuchi, Hirotaka: The Knowledge-Creating Company. Oxford University press, New York, 1995
- Nonaka, Ikujiro – Teece, David J. (eds): Managing Industrial Knowledge. Creation, Transfer and Utilization. SAGE Publications, London, 2001
- Nonaka, Ikujiro – Toyama, Ryoko – Konno, Noboru: SECI, Ba and Leadership: a Unified Model of Dynamic Knowledge Creation. Teoksessa Nonaka – Teece, 2001
- Polanyi, Michael: The Tacit Dimension. Doubleday & Company, inc. Garden City, New York, 1966

- Rikowski, Ruth (ed): Knowledge Management: Social, Cultural and Theoretical Perspectives. Chandos Publishing, Oxford – England, 2007.
- Schutz, Alfred: Collected Papers, I. The Problem of Social Reality. Martinus Nijhoff, The Hague, 1962.
- Sun Tzu: The Art of War. Shambhala, 2005.
- Takeuchi, Hirotaka – Nonaka, Ikujiro (eds): Hitotsubashi on Knowledge Management. John Wiley & Sons (Asia) Pte Ltd, 2004
- Weber, Max: Wirtschaft und Gesellschaft. Grundriss der verstehenden Soziologie. Fünfte, revidierte Auflage, mit textkritischen Erläuterungen herausgegeben von Johannes Winkelmann, 1. Halbband. J.C.B. Mohr (Paul Siebeck), Tübingen, 1976 (original 1921)
- Webster, Frank: Theories of the Information Society. (Second edition) Routledge, London, 2002

**History of Modifications**

<b>Date</b>	<b>Version</b>	<b>Writer</b>	<b>Modification</b>
22.2.2006	1.0	Heikki Mäkinen	1. accepted version
27.7.2006	1.1	Heikki Mäkinen	Standard BS7799-3: 2006 'Risk management' Developments in concept 'Information Society Service' Stylistic modifications and corrections
10.9.2008	2.0	Heikki Mäkinen	Modifications according to 'Yhteiskunnan Tiedon Turvallisuus', Version 2.0