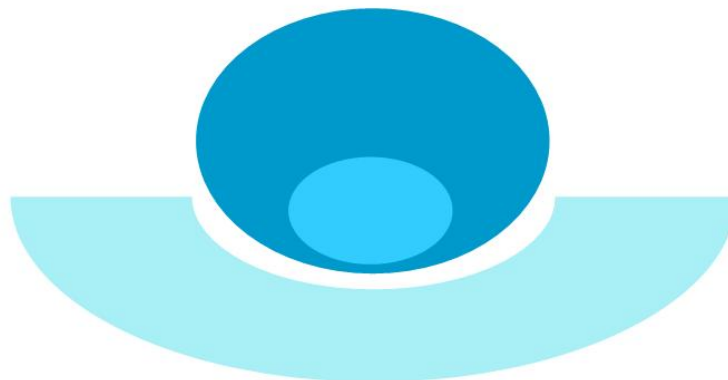




**Heikki Mäkinen**

**Risk, Trust and Security**



**Version 1.0  
1.11.2005**

**Knowledge of Society White Paper: 1**

**This Document is OBSOLETE**

**Superseded by  
[Global, History and Social](#)**



## Heikki Mäkinen

### Risk, Trust and Security

“Modernity is a risk culture” (Giddens, 1991, 3).

”The social significance of information processing is a function of information security. Question is, what is the shape of that function?” (Mäkinen, 2005a, 6).

#### Risk society and risk network

Modern society is a risk society (Beck, 1986, Beck, 1988). This is a general statement about the characteristics of modernity. In general case the aim of risk management – both economic and security risks – is to control threats which organisation or society encounters by specifying the consequences and probability of these threats. This is definition of threats as risks. After this it is possible to plan activities to manage risks. The acceptable risk, ‘residual risk’, is defined and described. (ISO/IEC Guide 73, 2002; FERMA, 2003; ISO/IEC 17799:2005, ISO/IEC 27001).

The situation is different if there are some risks, or threats, Grand Risks (Grossgefahren, Beck, 1988) which cannot be managed by general methods of risk management. These constitute the realm of specific risk society. It cannot be identified by any social characteristics which realise in societies like nation states. Risk society is global in its foundations and manifestations (Beck, 1999, 2000).

For a Grand Risk it is not possible to define probability and its consequences are impossible to assess. Consequences are furthermore such that there is no socially regulated or reasonable means to control them. Typical Grand Risks are environmental and other risks stemming from created environment, ‘socialized nature’ (Giddens, 1990, 124 -125 ) for example from gene technology (Beck, 1988).

In this paper I shall discuss about risk realm settled in communications network. The behaviour of risks in network is partly obvious - as for example with viruses or other malicious software. They can be controlled fully only if everybody in network participates. Nobody can control that it happens but control is possible at least in an individual node. Much more interesting is if the chaotic structure of global network creates a realm of global risk network comparable to global risk society.

#### Modernity and after

Modernity can be understood roughly as the industrial society although this is not its only dimension (Giddens, 1991, 5). Dissolving of industrial society is described in different ways. Such are at least ‘post modernity’, ‘risk society’ and ‘information (or knowledge) society’.



I shall not consider the situation in this way. I would rather think the issue from the point of view of knowledge, how it is managed and social implications of this.

It is useful to make a difference between knowledge and information. They are realised in specific kinds of assets, information and knowledge assets<sup>1</sup>. The former has an external carrier as for example document, file or database. This presupposes that knowledge is conceptualized and expressed in explicit form. Knowledge assets can be information assets but they can be also tacit knowledge which is realised in organisation's processes as "a dynamic human process of justifying personal belief toward the truth" (Nonaka-Takeuchi, 1995, 58). Knowledge is always meaningful for human action.

Communications networks are environments where processes reside and knowledge is created, delivered and protected. These environments are managed totalities or not managed. Latter may be called risk networks. In latter environments there can be information (also disinformation and misinformation) but rather not knowledge.

Information is a general global resource. Its development and protection environment is global network. It has no specific structure. Knowledge is also global but it is meaningful for social action. Environment where it is created, delivered and protected must have a structure and it must have security involved in it. This means that in this environment risks must be managed and trust towards the offered services specified.

One point of view about information society is that "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).

I am not quite sure that the term 'informationality' is relevant; and in no case I am suggesting term 'knowledgeality'. But if we have knowledge, which has its dimensions of social action and tacit knowledge, it must also have a kind of identifiable social context<sup>2</sup>.

According to Giddens "the dynamism of modernity derives from the *separation of time and space* and their recombination in forms which permit the precise time-space 'zoning' of social life; the disembedding of social systems (a phenomenon which connects closely with the factors involved in time-space separation); and the *reflexive*

---

<sup>1</sup> About definition of information assets see ISO/IEC 17799:2005 and ISO/IEC 27001. Discussion on knowledge assets see Nonaka – Toyama – Konno, 2001, 28 – 33, Teece, 2001, Mäkinen, 2005a, 56 – 57.

<sup>2</sup> Knowledge management theories discuss of a Japanese term 'Ba' which means time-space context of knowledge creation, delivery and protection (von Krogh – Ichico – Nonaka, 2000, 7, 47 – 49, 178 – 182; Nonaka- Toyama – Konno, 2001, 21 – 28; Mäkinen, 2005a, 15, 23 - 25).



*ordering and reordering* of social relations in the light of continual inputs of knowledge affecting the actions of individuals and groups” (Giddens, 1990, 16 – 17).

Modern communications network is global. This means not only ‘internationalization’ or global transferability of factors of production. Information, knowledge and communications network are concurrently present regardless of time and space. I call this phenomenon **genuine globalization** in contradistinction to **pre-globalization** of ‘world-market’ of production factors (Mäkinen, 2005a, 210 – 212, Mäkinen, 2005c).

Knowledge makes possible social action in highly differentiated time and space. It makes possible ‘disembedding<sup>3</sup> of social systems’ (Giddens) or as I shall say ‘meaningful space-time context’ in social system. Connection or context as such is not enough; it must have a defined content.

Also the concept of risk is a dimension of modernity as separation of time and space; “the notion of risk becomes central in a society which is taking leave of the past, of traditional ways of doing things, and which is opening itself up to a problematic future” (Giddens, 1991, 111). Globalization in its genuine form “is not only, or even primarily, about economic interdependence, but about the transformation of time and space in our lives” (Giddens, 1998, 30 – 31).

### **Trust and security**

Modern society presupposes systems which make possible both the differentiation of activities extensively in time and space and yet the joint action of these activities. According to Giddens these systems are about two types:

1. Symbolic tokens,
2. Expert systems, systems based on expertise<sup>4</sup> (Giddens, 1990, especially 21 – 29, 54; Giddens, 1991).

An example of symbolic token is money. It makes possible commercial transaction which takes place at large-scale market. Expert systems in this sense are for example transportation systems, water supply, electric power supply - or – much more interestingly and importantly- communications network’s certification services. Social relations which are formed by these systems have not an immediate context.

Functioning of ‘disembedding’ systems depend upon trust. Especially operations of expert systems are opaque for most people (‘lay-men’). “Trust is therefore involved in a fundamental way with the institutions of modernity. Trust here is vested, not in individuals, but in abstract capacities<sup>5</sup>” (Giddens, 1990, 26).

---

<sup>3</sup> “disembedding ... the ‘lifting out’ of social relations from local contexts of interaction and their restructuring across indefinite spans of time-space.”(Giddens, 1990, 21).

<sup>4</sup> Concept ‘expert system’, has a special meaning in ICT-technology. It is based on modelling of human knowledge, it is one form of ‘artificial intelligence’. That is why it is reasonable to make a specification ‘system based on expertise’.

<sup>5</sup> That is why individual risk management of risk networks (control of viruses and other malicious software) discussed earlier is not capable to create trust in network.



Security is a situation where risks encountered are reduced by special activities to a level of acceptable risk which depends on trust we have on system's functioning. "The experience of security usually rests upon a balance of trust and acceptable risk" (Giddens, 1990, 35). Same principle is followed in information security management system standard ISO 27001 (ISO 27001, ISO17799:2005) which requires that information security must be defined according to objectives of organisation – trust required – and risks it encounters. Principle is rather old: Chinese general Sun Tzu formulated it circa 2000 – 2500 years ago in book 'The Art of War': "If you know others and know yourself, you will not be imperiled in a hundred battles; if you do not know others but know yourself, you win one and lose one; if you do not know others and do not know yourself, you will be imperiled in every single battle"

Security does not presuppose the elimination of risks. But it can be defined only on such a system where risks can be managed and acceptable risks specified. This does not imply that the system is riskless. But risk must be controllable and there must be measures to manage it if we want to talk about security in the system. This issue is on a quite non-trivial sense connected with the kind of the social characteristics, sociality, of system.

Information security, based on balance of trust and acceptable risk, is the organisational and social side of ICT-technology – although not merely that. It is based on development of trust in environments where knowledge is created, processed, delivered and stored. It is not ICT-technology, although utilizes it.

### **Disinformation, misinformation**

"... 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 perhaps not a paradox at all. It seems rather to be substantial in this context. Information in global communications network has not necessarily any kind of connection to social relations where people live in. If communications network is chaotic, has not special structure or management, it is almost certain that it includes also disinformation and misinformation.

Communications network is generally constructed of three levels (Mäkinen, 2005a, Mäkinen, 2005c):

- transmission path,
- logical network structures and
- applications and services level.

Transmission path and services level, from general services part, are global. By logical network structures are designated here a set of network connections which are governed



by an information security policy of one or several organisations or by publicly accepted information security principles. Transmission path and general communications services are managed by communications service providers but their connection is necessarily not. If it is based on dynamic routing or at services level on universal addresses by which can be reached any peer entity in network, connections are not managed. In this case network is chaotic: any change in any node, service or connection can affect any other. This is the situation when for example viruses or other malicious software can spread out unrestricted in network.

Internet is a chaotic network in the sense defined. It fulfils also quite well the definition of Risk society or Risk Network. In Internet there is not, and eventually cannot be, such systems or totalities where it is possible to manage risks. Internet's information security problematic is insoluble. It is quite clear that it cannot be any basis for formation of any kind of sociality, for example basis of 'information society'. There can, too, exist information which has no social meaning – even disinformation and misinformation.

Internet is of course not the only chaotic connection where this kind of information – information without social meaning - occurs. In media there is many similar appearances. Celebrities news or reality TV give 'acquaintance' with no social connection or with an irrational connection to lives of people who only 'exist out there' in media. Witch hunts of politicians or other decision-makers, which yellow-journalism regularly arranges, dig after 'sniper-dears' with null-connection to rational social behaviour - not to mention rational social decision making. These relationships live only in 'informationality'.

This indicates that phenomenon is general. It is part of global networks where is no difference between the technology used in information's transmission or its type – is it data, voice, picture, motion picture or all together.

### **Security of information. Surveillance**

Surveillance is an integral part of security. It is also part of administrative systems of society. Its basis is storage of relevant control information of the conduct of people at the realm of the system in question. The other part of surveillance is the direct supervision of that conduct (Giddens, 1981, 5, 169, Giddens, 1985, 14 -15, 46, 172 - 181).

Surveillance and information gathering for its purposes is also an element of activities against democracy and human rights (Giddens, 1981, 175, Giddens, 1985, 200 – 206, 341). This 'dialectics of surveillance' asserts that surveillance itself must be object of scrutinizing of its risks and trust involved with it. Information must be secure in the way that it is not used against personnel in organisation or people in society.

Dialectics of surveillance is perhaps one aspect of difference between unstructured, chaotic, and global, information and socially meaningful knowledge. Security data gathered without social reflexion by analysis of risks and trust, is out of control of subordinates.



In organisation reflexive monitoring presupposes that surveillance is done by a formal system of organisation. It should not be dependent on any person but on organisation's formal activities. On the other hand surveillance system must be transparent to personnel and public inside organisation – which does not mean that the information gathered by surveillance system should be public; it should of course be treated according to general principles of information assets management in organisation.

The problematic of transparency of surveillance is even more important when network environment is concerned. In a chaotic network people participating in its activities have no means to control what kind of information is gathered about them. This information can be used to commercial (Lyon, 2001, especially 101 – 103) or control, also opinion control, purposes. No-one, not even nation states or network's operators have possibility to manage this kind information gathering.

The other side is that chaotic network makes it possible to manipulate social decision making for example by anonymous lobbying in network. By generating emails and in future also network phone calls, there is possible to create an artificial 'public opinion', which is not public at all, to direct social decision making.

Surveillance has a close connection to information management. In a quite non-trivial sense the history of surveillance is history of information management. Writing has in a considerable extent been developed from requirements of administrative systems and surveillance (Giddens, 1985, 41 - 49). Writing is the first form of information - and also knowledge - management (Mäkinen, 1993, 191).

From the preceding it does not follow that history of information management should be history of surveillance. It is obvious that 'information society' gives surveillance better possibilities than earlier. This is even more important when network is developing. In basic Internet there are moving mainly IP-addresses, addresses of web-sites and email-addresses. In future there are moving also usernames and certificates whose entering into non-intended databases is a bigger threat than earlier.

If information is not protected according to objectives of organisations or individuals but is possible to gather it from a chaotic media, as for example from Internet, there is forming a hierarchy which is out of control of everybody.

### **Information society service<sup>6</sup>**

Information, knowledge and communication network are also global. The meaningful social connections, which form a society, in this environment, are not possible to identify with nation state or any other spatially bounded zone. Meaningful social connections are principally global too. Global in this context does not mean 'world-wide'; it means independence of place or other spatial dimensions.

Instead of governmental services or national economic units which reside in nation state, it is discussed about information society services. They can be administrative or

---

<sup>6</sup> For more detailed review on this issue see Mäkinen, 2005a, 195 - 207 and Mäkinen, 2005c.



economic services in a broad sense of these concepts including for example 'production services'. They constitute of application of knowledge to a service 'customer' requires; 'customer' instead of 'citizen'. This knowledge is applied in communications network. The quality or type of services as such does not matter. Service only presupposes that specific risks of them are analysed and trust they require defined.

This is a prerequisite for socially meaningful and understandable systems. Communication networks used must be defined from the point of view of the service. Security in the environment has two components: organisational-social and technical component.

Security must create conditions for existence of social activities in large-scale time and space, as an 'disembedding' mechanism. Technical methods can be used to get people to know whom they are dealing with. They must identify network entities which they have no other connection than network. Entities must be identified, authenticated and their identity must be non-repudiated.

From the point of view of trust, network entities are in a different position if they are organisations participating in administrative or economic activities in networks or individual human beings. In the first case they must have an Information Security Management System which is generally accepted in relationships in question. Certification authorities have a special role in this, because they are arranging the technical security operations.

To individuals in network it is not usually reasonable to settle this kind of requirements. If they are not part of some organisation they are always at least partially in the realm of risk network.

### Literature:

- Beck, Ulrich: Risikogesellschaft. Auf dem Weg in eine andere Moderne. Suhrkamp, 1986  
Beck, Ulrich: Gegengifte. Die organisierte Unverantwortlichkeit. Suhrkamp, 1988  
Beck, Ulrich: Risk Society. Towards a New Modernity. SAGE Publications, 1992  
Beck, Ulrich: World Risk Society. Polity Press, 1999  
Beck, Ulrich: What Is Globalization? Polity Press, 2000  
Federation of European Risk Management Associations (FERMA): A Risk Management standard, 2003, (www.ferma-asso.org)  
Giddens, Anthony: A Contemporary Critique of Historical materialism. Vol 1, Power, property and the state. The MacMillan Press, 1981  
Giddens, Anthony: A Contemporary Critique of Historical materialism. Vol 2, The Nation-State and Violence. Polity Press, 1985.  
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: The Third Way. The Renewal of Social Democracy. Polity Press, 1998  
ISO/IEC, International Standardisation organisation, Standard 17799: 2005: Information Technology - Security techniques. Code of practice for information security management, Second Edition 2005-06-15  
ISO/IEC, International Standardisation organisation, Standard 27001: Information Technology - Security techniques- Information Security Management Systems – Requirements (2005-10-15)  
ISO/IEC, International Standardisation organisation, Guide 73: Risk Management, Vocabulary, Guidelines for use in standards, 2002



- von Krogh, Georg – Ichijo, Kazuo – Nonaka, Ikujiro: Enabling Knowledge Management. How to Unlock the Mystery of Tacit Knowledge and Release the Power of Innovation. Oxford University Press, 2000
- Lash, Scott: Critique of Information. SAGE Publications, 2002
- Lyon, David: Surveillance society. Monitoring everyday life. Open University Press, Buckingham – Philadelphia, 2001
- Mäkinen, Heikki: Yhteiskunnan tieto. (In Finnish) (Knowledge of Society) Acta Universitatis Tamperensis ser A vol 381, Tampereen yliopisto, Tampere 1993
- Mäkinen, Heikki: Yhteiskunnan tiedon turvallisuus (In Finnish) (Knowledge of Society: Security), 2005 (2005a), [www.yhteiskunnantieto.fi](http://www.yhteiskunnantieto.fi).
- Mäkinen, Heikki: Globalnet and Knowledge of Society, 2005 (2005c), [www.yhteiskunnantieto.fi](http://www.yhteiskunnantieto.fi)
- 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
- Sun Tzu: The Art of War. Shambhala, 2005
- Teece, David J.: Strategies for managing Knowledge Assets: the Role of Firm Structure and Industrial Context. Teoksessa Nonaka – Teece, 2001.