Security in the "Digital Society" - New Risks and their Management

Herbert Burkert*

Online-Publication of the statement held on the International Expert Conference "Security and Development of Global Information Society" on July 19th, 2005 in Beijing. Development of Internet in Germany and China, Security in the Electronic Era, Online-Journalism and e-Government were the topics of the conference that brought together media experts in cooperation with People's Daily Online. Beijing, July 2005, English, 15 pages.

* Professor (Dr .habil.) for Public Law, Information and Communication Law and President, of the Research Centre for Information Law, University of St.Gallen, Switzerland and Senior Researcher, Fraunhofer Institute for Mediacommunication, St.Augustin, Germany (currently on leave of absence) - hb@herbert-burkert.net. - All weblinks in this paper have last been verified on July 8, 2005. All links point to sources in English unless stated otherwise.

1 Introduction

new risks

A general description of the some of the new risks of the Digital Society will be followed by an overview of possible measures against such risks. "Digital Society" refers to societies in which individuals and organizations use information technology for their daily work and leisure and communicate with other individuals and organizations over digital networks.

risk management

Measures against risks can only reduce the probability of the occurrence of damage or reduce the amount of damage. It is the nature of risks that they can rarely be eliminated altogether. Term of "risk management" will therefore be used to indicate the continuing presence of risks.

role of the State

For each type of risk introduced one or two risk management measures will be described. The presentation concentrates on risk management measures by the State. While in a Digital Society the private sector is increasingly asked to address risk issues directly, and while the private sector has already been very active in implementing technical and organizational strategies, the State is still needed to set examples, to encourage or to deter, and to address general issues for the whole of the society.

global implications

Examples provided are taken from Germany. But we have to remember that Germany's approaches are embedded in European Union approaches. Where necessary I will therefore make a reference to European Union activities.

global implications

Finally, Digital Society do not end at national borders. So national examples even when embedded in their European context are but examples for the need for global solutions, as was shown again last week in Geneva at a thematic conference on Cybersecurity[1] in preparation of the Second Part of the World Summit on the Information Society in Tunis in September this year, where I had the honor to preside a session on the relation between security and data protection. This issue will reoccur in this presentation.

[1] http://www.itu.int/osg/spu/cybersecurity/index.phtml.

2 New Risks

2.1 Types of Risks in the Digital Society

new risks

This presentation will concentrate on risks which are typical for the Digital Society as such. There are various ways to group such risks, according to motives, means, or values which might be endangered. This presentation seeks a neutral approach: In the Digital Society there are three layers which are open to risks: the general infrastructure mainly resting on networks, the communication relations and the information. We may accordingly structures risks as

- infrastructural risks,
- risks to communication and
- risks to information.

2.1.1 Infrastructural Risks

infrastructural risks

Infrastructural risks refer to the partial or total, temporary, mid-term or long-term non-availability of general communication infrastructures. These risks may occur not only from threats to the digital infrastructure as such. Such risks can also occur because elements of the structures which support the digital infrastructure are affected. Such risks are generally referred to as national risks

2.1.2 Communication Risks

communication risks

The term "communication risk" refers to risks occurring on the middle and micro level of social communication: These are risks which primarily - although not exclusively - affect the communication process between organizations of the public sector or private sector, between individuals and between individuals and organizations. In the Digital Society these communication links have been primarily designed to support the ease of communication rather than to guarantee secure communication. Consequently the design of these systems favors open access. Security measures are not implemented as a default but only - if at all - as extra assets which need to be specifically applied. Since users have the habit to stay with system defaults, such communications are open to unwanted intrusion, unwanted eavesdropping and communication under false identities.

2.1.3 Informational Risks

informational risks

The last group - information risks - refer to risks for the informational content and the information context of digitally processed information, such as unauthorized destruction, alternation, or theft; falsification of information, or presenting information out of context.

informational risks as IS risks

Information risks, in particular, may, of course, also occur outside digital communication networks; a letter may be stolen; a newspaper may present a person in a false light. What makes such risks typical Digital Society risks is the dimension of "traditional" risks in the new environment. To present a person in a false light in a village news paper has, after all, different implications than making this same mistake on an internet website.

This example leads us to a more general risk in Digital Society, a risk which may even turn any "old" risk into a "new" risk typical of the Digital Society:

2.2 A General Risk in the Digital Society : The Asymmetrical Effect

What is meant by the "asymmetrical effect" can be explained by using an example taken from the area of the infrastructural risk:

A single person - an eighteen year old German who has last week been sentenced by a German court had released a computer virus (more precisely a "worm") which has led to breakdowns of computer systems world wide about a year ago (The "Sasser virus"). The action of the young man was punishable under a section of the Criminal Code which has been in force since several years. So the criminal law system had been prepared. What had not been prepared were the practical security measures and the behavior of users opening every mail addressed to them.

small causes - large effects

What is more important in this context, however, is that a single person had been able to create such consequences which have led to a break down of a large part of the infrastructure. It only requires little effects to cause large reactions in societies which have become highly dependent on technical infrastructures. This asymmetrical vulnerability is not only typical of the Digital Society but of technology dependent societies in general. However, the largely automated character of the information and communication technology magnifies and accelerates this "asymmetrical effect."

This asymmetry has consequences for risk management: It will always take proportionally more resources to meet the probability of such attacks, than those resources a single attacker might need to create damage.

disproportional response

However, the "asymmetrical effect" of the Digital Society has another more hidden effect which in itself may create risks: Since small causes may cause large effects, and since protective measures demand more resources than those which are needed to cause harm there is the danger that risk management may loose its understanding of proportionality. The issue of disproportional response is currently debated in the context of intellectual property rights: The new technologies have made it possible to make and distribute high quality copies with little effort in comparison to the effort it has taken to create the original. This disproportional risk to property and innovation has led to a legislative response which now in turn is seen as disproportional and endangering the proliferation of ideas and innovation.

3 Risk Management in the Digital Society

Three general aspects of risk management in the Digital Society have to be mentioned to understand the specific examples which will be shown later:

- To a large extent risk management in the Digital Society does not differ much from risk management in traditional societies. This will be shown with a brief look at law in the Digital Society (3.1 below).
- Risk management in the Digital Society, however, also creates specific problems which are typical for the Digital Society. These phenomena will be discussed under the term "risk control paradox" (3.2 below).
- Finally, since this presentation focuses on risk management by the State some special conditions for state intervention need to be briefly mentioned (3.3 below).

3.1 Traditional Measures: Law as an Example

legal measures

Risk management measures in the Digital Society - in many cases - do not differ very much from risk management in traditional societies. Organizational, financial and psychological measures are used for risk preparedness and risk avoidance. One central response is response by law. Law is after all a risk management mechanism:

- Criminal law e.g. seeks to establish a system of deterrence; and where it fails in deterrence it seeks to answer by retribution. *criminal law*
- Private law establishes a system of expectations of behavior or sets the framework for parties to establish such a system of expectations by contract. Where this line of defense in private law fails it establishes rules of compensation. *private law*
- A highly sophisticated sub-system of law is liability law outside contractual obligations. Liability law establishes responsibilities and compensation when these responsibilities have not been kept. Such liability laws have interesting consequences: Those responsible seek to insure themselves against the financial consequences of such failures. Insurance companies on the other hand have an interest in the optimal relation between the insurance premium and the amount they may be forced to pay if responsibilities are not met. In order to optimize this relation insurance companies often set up control procedures and force them on the insured party with a threat not to pay in case of an accident if these control procedures are not put into place. Insurance companies so contribute in raising the level of security. *liability law*

3.2 The Specific Character of Risk Management in the Digital Society: The Risk Control Paradox

There is, however, one feature which seems to be specific to risk management in the Digital Society. This phenomenon may be called the "risk control paradox" and causes many of the public debates around the effects and risks of the Digital Society.

The meaning of the "risk control paradox" can be explained by an example taken from the area of communication risks:

communication risk example

As we have seen above open access design invites malicious attacks. Open access is facilitated by a network structure which has no prescribed routes for information to travel. However, in networks each piece of information has to be clearly identified as to its origin and as to its address. Network routers have to store this information in order to guide these packages through the network. In meeting the risks of the open structure such information can be used to trace the source of a malicious attack.

first level

In other words with digital technologies the same characteristics which create risks also provide mechanisms to combat these risks. But this is only the first level.

second level

The "risk control paradox" does not stop there: The risk management mechanisms provided by the technology to manage the risks of the technology may in turn create risks: Increasing monitoring of networks e.g. not only affect the performance of networks but create large collections of control information which in itself has new risk potentials of misuse. Constant monitoring may have chilling effects on open discussions. Open discussions, however are the basis for legitimacy and authority.

3.3 The Specific Character of Risk Management by the State

risk management by the State

The presentation will concentrate on risk management measures provided by the *State* (the government and/or the law making bodies).

responsibilities of risk management

This does not imply that the State is the only responsible actor for risk management. Quite to the contrary. Individuals and private sector organizations are responsible to manage their own risk sphere. Private sector organizations exchange experiences and make use of services and products by other private sector organizations to improve risk management and to educate individuals.

Still, the Sate has a broad responsibility and means to implement it: Due to its responsibility for internal and external security the Sate has to undertake measures to improve the security of public sector organization. The State can also set standards for contracts of public sector institutions with the private sector and can thus influence the level of security in the private sector.

Law State4 principle

Any activities of the State have to be guided by the "Law State" principle. The concept of the "Law State" comprises several principles. In our context the "Law State" concept requires that all State actions need to have a basis in a law which provides the State with the competence for these acts and sets limitations as to what extent such actions may interfere with rights of individuals. Individuals then have the possibility to challenge these measures in the courts. It is then for the courts to strike an adequate balance of the interests involved. These principles also apply with regard to security measures; the mere qualification as a security measure does not free the measure from the "Law State" concept. The importance of the security issue may, however, influence the balance made by the courts.

In our context the Law State concepts requires that whenever any of the these risk management measures are taken by the State - whether they are organizational; psychological; financial or technical - they must all be based on a law or there must be some clear connection to a law authorizing such action.

There are - of course - a lot of laws already in place as basis for state authority meting security risks; the Digital Society also poses the question to what extent new laws are required. The presentation will contain some such examples.

The system of laws in which state institutions operate may sometimes be cumbersome and create bureaucratic obstacles, particularly in a time of fast and deep technological and social changes. No matter, however, what kind of solutions are being prepared, it is obvious that the change cannot mean no law, but laws which allow for greater flexibility, laws which encourage cooperation between the public and the private sector, without, however, effacing responsibilities and opportunities for citizens to seek redress in the courts when they feel that their rights are at stake.

4 Managing the Risks of the Digital Society - Examples

For each of the types of risks identified above in section 2 at least one risk management measure will now be described in more detail.

infrastructural risk

As an example for meeting the infrastructural risk I will describe the installation, role and function of the Federal Office for Information Security in Germany.

communication risk

With regard to the communication risks I will describe two approaches:

digital signature

- The Digital Signature approach: This is an approach of meeting at least some of the communication risks by establishing a national infrastructure for secure and identifiable communication.

data retention

- The second approach is the Data Retention approach. This approach is also an example for the risk control paradox in Digital Societies: It is an example of using information technology against information technology risks. But it also an example on how a risk management approach can create new risks which need societal discussion.

contents

The last example will show one set of legal measure which seeks to reduce risks for information contents, its quality, its meaning and its context.

4.1 Managing Risks for the Infrastructure - The "BSI" example

In Germany - as elsewhere - there are a number of measures in place - legal, organizational and technical - which have the purpose to minimize the risks for the (German) information infrastructure. Such measures come under the com-

petence of the (federal and regional) governments and their responsibility for national and internal security.

On the European Union level a recent Decision of the Council of Ministers has asked all its member states to harmonize criminal law so as to have a common deterrent against possible attacks on all levels.[2]

One such measure I will describe in more detail is the installation of the Federal Office for Information Security , a measure which goes beyond national security and seeks to contribute to risk awareness and risk preparedness in the whole of the German society:

BSI

In 1990 the Federal Office for Information Security (abbreviated in German as "BSI") was established as a special office of the Federal Ministry of the Interior.

The BSI[3] is

- *service/support* the central IT security service provider for the German government, giving advice and support on information security issues to all of the federal government.
- *research* The BSI undertakes research and organizes seminars on information security issues and makes the results - in most cases - available to the general public;
- *products* it produces information security software, guidelines and organizational manuals for all levels of public administration;
- *services for the general public* it undertakes measures in information security education addressed to the general public.

For internet security alone the BSI has established six operational units:

- The BSI's Computer Emergency Response Team (German CERT) is the central coordinating body for the solution of computer and network security problems for government organizations. Security-relevant information from manufacturers and other sources is analyzed, evaluated and processed for the target groups. The service runs an information mailing system to alert user groups. It provides - with the help of manufacturers - appropriate measures to answer security risks. This section of the Office also has en emergency group which can intervene in special situations.

---

2 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems - Official Journal 16 March 2005 - L69/67.

3 http://www.bsi.de (with web pages in English).

- The Section on Internet Security Analyses and Procedures is concerned with basic research into internet security. It publishes methods, procedures and tools
- The Section for Support for Criminal Prosecution Authorities and Prevention is the central coordinating body with respect to technical support for criminal prosecution authorities in the prevention and investigation of criminal offences that are directed against the security of information technology.
- The Section on Malicious Programs, Computer Viruses gives recommendations on the protection against malicious code and advises users and manufacturers on security aspects of current operating systems and application programs.
- The IT Penetration Centre examines the computer systems of public administrations for weaknesses and makes recommendations on how to eliminate these weaknesses. When necessary this section assists public administrations with the analysis of and defense against such attacks.
- And finally the Critical Infrastructures section examines the IT risks for critical infrastructure sectors relevant for Internet information security.

The BSI has annual budget of about 45 Million Euros and has more than 380 employees; the Office has developed a high standing in the public and private sector, although there has been some criticism because it is politically dependent on the policies of the Ministry of the Interior.

4.2 Managing Communication Risks

Two measures will be described under this heading: The Digital Signature concept and the issue of data retention.

4.2.1 Digital Signature

e-commerce context

Digital Signatures are usually discussed in the context of e-commerce to facilitate business interactions. The function of digital signatures, however, goes beyond such usage: Digital signatures can address the problem that communication in digital communication media does not provide for clear identification of communication partners in general and - that the contents of the communication could be repudiated by either partner.

the Digital Signature concept

The concept of digital signatures makes use of an encryption scheme called "Public Key Encryption". Each participant receives two keys. One is secret, called the "private key" usually embedded in a computer readable card which the par-

ticipant receives; the other key is a so called "public key" which can be made known to anybody and can be contained in a public register. If e.g. a person A wants to send a message (M) to a recipient called B, A encodes the message M with his secret key and sends it to B. B - knowing that the message comes from A - looks up the public key of A in an open register. B can decrypt the message by A with the public key of A only if the message was really from A.

In practice this procedure is used for signing contracts electronically: To do this an additional technical procedure is used which mathematically creates a "fingerprint" of a text in a way that is specific for that text and only for that text, so that even if only one sign of that original text would be changed another "fingerprint" would result. In this context A sends the contract and the fingerprint of the contract to B. The contract is not encrypted. But A encrypts the finger print of the contract with his secret key. B takes the contract from A, and creates a fingerprint of the contract for himself. B then looks up the public key of A and uses it to decrypt the fingerprint of the contract he has received from A. If the decrypted fingerprint from A is identical with the fingerprint B has created himself then B knows that

- the text came from A and only from A, and that
- the text of the contract has not been changed after A had encrypted its fingerprint.

a nation wide identity system?

For this system to work nationwide one would need a trusted institution that would hand out key pairs only after the recipients have verified their identity to this authority. Another model would be that competing companies could hand out such pairs, but a central authority certifies these companies to ensure standards and safety of operations. The latter approach has been suggested by the European Union in a directive on electronic signatures in 1999.[4]

German example

Within this framework Germany has established a central authority that certifies other authorities or companies.[5] This central authority is the Regulatory Authority for Post and Telecommunications which has by now authorized more than 15 such service providers. Laws on the formal quality of signatures on paper documents have already been changed in Germany so that this system could be used on a wide scale basis for contracts meeting the formal requirements of law.[6]

But still this method is not too widely used in Germany: Currently this method is mainly used by the legal profession, for lawyers communicating with each other

---

4 http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf

5 Electronic Signature Law of 16 May 2001.

6 See also Art.11 of the Contract Act of the People's Republic of China (1999).

or with courts. Others use such systems within limited user groups, as e.g. tax accountants.

In order to foster a nation wide proliferation it has already been suggested that such key pairs could be handed out together with the national identity card.[7]

4.2.2 Data Retention

terminology

The term "Data Retention" refers to the obligation of communication service providers - including internet service providers - to keep records on network traffic which identifies each client for a given period of time and to make this information available to law enforcement authorities upon request.

German example

In Germany currently there is no legal obligation for data *retention.*

There are - based on the German Telecommunication Act (current version of June 2004) and its regulations - obligations to share real time traffic and contents information with law enforcement authorities; law enforcement agencies can - if properly authorized -

- require information service providers to send direct copies of current traffic to law enforcement authorities,
- require information service providers to hand over copies of information which they have stored anyway (e.g. for billing purposes),

but they cannot require information providers to *store* information.

What information providers store depends on the contracts they have with their clients and the way in which they administer their clients. What they *may* store and how long is regulated in the data protection section of the German Telecommunication Law. According to these regulations service providers may not store such information beyond a maximum of six months. The largest German internet provider - t-online - currently stores traffic data of its customers for eight months. Last week a German court has declared this practice to be illegal.[8]

European Union and current discussions

The European Union - through its Council of Ministers has tried several times to harmonize national legislation of Member States so as to make all member states introduce regulations which would require such storage.

---

7 (German:) http://www.br-online.de/wissen-bildung/thema/egov/signatur.xml

8 For the text of the judgement (in German only) see: http://www.jur-abc.de/de/ip.htm.

In January 2005 the German Parliament has mandated the German Government not to go beyond the existing regulation which sets the maximum time of six months.

Last month the European Parliament has rejected a proposal by the Council of Ministers. The issue will be discussed again in September.

opposing arguments

The opposition against data detention is partly based on the costs such detention would cause for communication service providers. The main arguments against such a retention, however, is that it is excessive in comparison to its purpose and that it affects privacy rights to an extent which cannot be sufficiently justified.

4.3 Managing Information Risks - Data Protection

contents and context risks

Information handling involves the risk of information mishandling. Mishandling personal information affects people's privacy rights. While these risks have occurred before the Digital Society, it is the asymmetry effect described before which requires new solutions to manage those risks which occur when personal information is handled electronically. These risks are addressed by data protection laws. The term data protection law has developed historically. The term is misleading. What are protected are the privacy, integrity and liberty of individuals against misuses of information.

German example

In Germany data protection laws - as I will continue to call them - exist in the provinces and on the federal level. They apply to all public sector institutions and the private sector. For specific areas there are special sector privacy regulations like in the area of telecommunications as already mentioned. The German data protection laws are in conformity with the European Union Data Protection Directive of 1995.[9]

The main principles of data protection legislation can be summed up as follows:

- There must be a legitimate reason to collect and process personal data. Such a legitimate reason may be a law prescribing such handling of personal data, a contract or the consent of the individual concerned (in the private sector), or - under special conditions an overriding private or public interest.

---

[9] For more information on the situation of European Union data protection see: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htmFor PRC:

- The information collected or processed must be kept correct and up-to-date, it should not be excessive and used only for the purpose for which its collection was legitimate.
- Persons on whom data is being collected or processed have the right to know the data (with some exceptions); if it is false they may require that it is corrected; if it was illegally collected they may require to have it destroyed.
- Independent authorities are established which educate the public sector and the private sector on how to handle personal data, and which control that the data protection regulations are being followed in the public and the private sector.

difficulties

In practice such an approach to regulating the handling of personal data meets with several difficulties - particularly in the age of the internet. While these laws are applicable to the situation on the Internet because they have mostly been formulated in a technologically neutral way, the main problems are more of a practical kind: Users of the Internet e.g. have to learn that information on how they click their way through web pages can be monitored by national, but also by foreign companies who may then use this information for advertisement purposes; other users have to realize that their personal email-addresses are being distributed to others who then flood them with spam mail.

limits of national law

National data protection laws make only sense if governments can guarantee their citizens that other governments will help them to respect their rights. Within the European Union such mutual recognition is achieved by the general directive on data protection mentioned above which sets the level of data protection for the Member States. The European Union can also make agreements with third countries to facilitate the transfer of personal data with these countries, provided these countries have legislation in place which is adequate in comparison to the European regulations. The European Union has already made agreements with such third countries.

Finally, it should be noted that already in 1990 the United Nations General Assembly has recommended data protection guidelines to its member states.[10]

[10] Guidelines Concerning Computerized Personal Data Files - adopted by the General Assembly on 14 December 1990.

5 Conclusion

From the many risks for today's Digital Society I have identified three types of risks: risks affecting the national information infrastructure of a country; risks affecting the communication of organizations and individuals, and risks affecting the information itself.

I have emphasized two general characteristics which seem to be specific for theses risks in the Digital Society: the asymmetry between cause and effect and the risk control paradox.

For each type of risks I have given examples of risk management approaches: the example of the Federal Office for Information Security as an institution to deal with infrastructural risks, the Digital Signature scheme as an example to deal with identity problems in communication, the data detention issue to show how technical risk solutions must also be measured against their possible impacts on society, and finally I have shown data protection as a mechanism to deal with certain risks affecting the quality and context of information.

Within the given time, I could only introduce examples. And although I have illustrated these examples with national examples I have also pointed out that the true challenge lies in finding internationally compatible solutions.

I am aware that for many of these issues the People's Republic of China has developed solutions, like e.g. Electronic Signature Act (ESA), with has - I believe - taken effect in China three months ago, or the privacy regulations in Art. 38 of the PRC Constitution and Article 18 of the Implementing Measures for the Provisional Regulations of the PRC for the Administration of International Connection of Computer Information Networks (1998), and Article 40 of the PRC Constitution together with Article 7 of the Measures for the Protection of Security and Administration of International Connection of Computer Information Networks (1997)..