

Future Information Security Trends

Kasi Research Project

Tekes Safety and Security Research Program

Final Report, March 11, 2011

Olli Pitkänen, Risto Sarvas, Asko Lehmuskallio, Miska Simanainen, Vesa Kantola

Helsinki Institute for Information Technology HIIT / Aalto University

Mika Rautila, Arto Juhola, Heikki Pentikäinen

VTT Technical Research Centre of Finland

Ossi Kuittinen

Sitra

Executive Summary

This report presents the major findings of the research project Kasi – Future Information Security Trends (*Kasi – tulevaisuuden tietoturvatrendit*) conducted by Helsinki Institute for Information Technology HIIT and VTT Technical Research Centre of Finland. The project is a part of Tekes Safety and Security Research Program (*Tekesin Turvallisuus-ohjelma*) and its purpose is to provide rigorous and systematic foreseeing knowledge for the implementation of the Finnish National Information Security Strategy (*kansallinen tietoturvastrategia*).

The aim of the project was to study near-future information security issues that are related to, for example, new technologies, services, and business models. Our approach combines perspectives from different disciplines in order to better address the complexity of the focus area. We identified relevant future information security trends especially from the Finnish viewpoint in the next five to ten years by collecting and analysing specialists' conceptions and knowledge of the various developments in their professional fields. In order to deepen the analysis, we also specified factors and attributes that affect the realization of the trends. In addition, our objective was to evaluate the need for establishing a separate program for continuous foreseeing activities and provide methodological and procedural guidelines for carrying it out.

Our research process went through five separate steps: 1) outlining possible future environments, 2) creating concrete future scenarios or stories, 3) analyzing information security issues in the scenarios, 4) identifying information security trends, and 5) specifying factors and attributes that affect the realization of the trends. Our major findings concerning the future information security trends in Finland in a 5 to 10 years scale are the following:

1. The interdependency between societal processes and information systems increases
2. New interdependencies between organizations and the state emerge
3. Information security issues become more international
4. Needs to manage private or confidential information and public appearances in ICT environments increase
5. Protection of personal data becomes a considerable political issue
6. It becomes increasingly difficult to ensure the correctness of information
7. The correctness of information becomes increasingly important
8. Data gathering increases
9. Data combination from different sources increases
10. Traceability of persons and goods increases
11. Malicious action against information systems increases
12. Quality and security issues are increasingly taken into account in software development
13. Automation/autonomous systems are increasingly employed to effect security
14. Availability of information increases as the public information resources are opened
15. Commercial interests drive actors to restrict access to proprietary information resources
16. Governance of access to information resources in organizations becomes more difficult

Realization and intensity of the trends are dependent on several factors that we have categorized as societal, economic, technological, and legal. The factors have either intensifying or constraining effects on the trends and the intensity of their effect varies.

We believe our work on future information security trends and issues and on the methodological questions of reliable foreseeing activities provides relevant information for commercial, policy and scientific interests. We propose that in order to get reliable foreseeing results in the long term, the process of identifying future information security trends should be continuous. While the continuous process would also provide grounds for improving the foreseeing method, this project sets a firm starting point with practical guidelines and the first round of results.

Acknowledgements

This report could not have been possible without the vision, support, ideas and expertise of a number of people. Therefore we want to convey our gratitude to the project's initiators, promoters, industry sponsors, and workshop participants who shared their knowledge and inspiration. The persons and organisations that have contributed to the conception, financing or fulfillment of this effort include: Jussi Jyrinsalo, Jyrki Pennanen, Toni Loivakari, Petri Mäkynen (Fingrid Oyj), Mari Herrala, Timo Kievari, Mirka Meres-Wuori (Finland's Ministry of Transport and Communications), Vilma Lehtinen (Helsinki Institute for Information Technology HIIT), Gabriel Waller, Kimmo Hätönen, Perttu Halonen (Nokia Siemens Networks Oy), Ossi Kuittinen (SITRA, the Finnish Innovation Fund), Suvi Sundquist, Janne Peräjoki (TEKES), Marja Dunderfelt, Tapio Haapanen, Arttu Lehmuskallio, Seppo Kalliomäki, Titta Penttilä (TeliaSonera Finland Oy), Anu Helkkula (Aalto University), Matias Vierimaa, Pasi Ahonen, Sami Lehtonen, Matti Penttilä (VTT Technical Research Centre of Finland), Jorma Laiho, Olli-Pekka Heinonen, Simo Alho, Mirva Savikko (Yleisradio Oy) and Pekka Nykänen (Pöyry Telecom). Since this project was not an isolated affair, but a part of a more comprehensive national program, we also wish to extend our thanks to those not directly related to our effort but who have paved the way for it.

1	INTRODUCTION	1
2	RELATED WORK	2
3	METHODOLOGY	3
3.1	SCENARIO METHODS IN GENERAL	3
3.2	BRAINSTORMING, DESIGN GAMES AND TREND ANALYSIS	4
4	FUTURE INFORMATION SECURITY TRENDS	6
4.1	INCREASING INTERDEPENDENCIES	7
	TREND: The interdependency between societal processes and information systems increases	7
	TREND: New interdependencies between organizations and the state emerge	7
4.2	INTERNATIONALIZATION	8
	TREND: Information security issues become more international	8
4.3	PRIVACY/PUBLICITY MANAGEMENT	9
	TREND: Needs to manage private or confidential information and public appearances in ICT environments increase	9
	TREND: Protection of personal data becomes a considerable political issue	10
4.4	VALIDITY OF INFORMATION	11
	TREND: It becomes increasingly difficult to ensure the correctness of information	11
	TREND: The correctness of information becomes increasingly important	12
4.5	DATA COLLECTION	12
	TREND: Data gathering increases	12
4.6	DATA COMBINATION	13
	TREND: Data combination from different sources increases	13
4.7	TRACEABILITY OF PERSONS AND GOODS	14
	TREND: Traceability of persons and goods increases	14
4.8	PROTECTION OF INFORMATION SYSTEMS	15
	TREND: Malicious action against information systems increases	15
4.9	SOFTWARE DEVELOPMENT	16
	TREND: Quality and security issues are increasingly taken into account in software development	16
4.10	AUTOMATION	17
	TREND: Automation/autonomous systems are increasingly employed to effect security	17
4.11	ACCESS TO INFORMATION	18
	TREND: Availability of information increases as the public information resources are opened	18
	TREND: Commercial interests drive actors to restrict access to proprietary information resources	18
	TREND: Governance of access to information resources in organizations becomes more difficult	19
5	DISCUSSION	21
5.1	PRIVACY ISSUES	21
5.2	INFORMATION SECURITY	22
5.3	TECHNOLOGICAL INNOVATIONS	23
5.4	SERVICE INNOVATIONS	25
5.5	LEGAL DATA PROTECTION	26
6	CONCLUSIONS AND RECOMMENDATIONS	28
6.1	GUIDELINES TO CONTINUOUS TREND ANALYSIS	29
6.2	SUGGESTIONS FOR FURTHER STUDIES	31
7	REFERENCES	33

1 Introduction

The Finnish government's resolution on the National Information Security Strategy (*kansallinen tietoturvastrategia*) was adopted in December 2008. The aim of the strategy is to secure everyday life in the information society. The vision of the strategy is that citizens and organizations can trust that their transactions in information and communications networks and services are secure. The strategy focuses on three priorities: 1) citizens' skills in the ubiquitous information society, 2) information risk management and process reliability, and 3) competitiveness and international network cooperation.

The strategy is implemented with an action program (*toimenpideohjelma*), which consists of nine different projects (*hanke*) that concentrate on timely security topics. One of the projects is called PROJECT 8: Research Project on Near-Future Information Security Trends (*HANKE 8: Tutkimushanke lähitulevaisuuden tietoturvatrendeistä*).

This report presents the results of the research project called Kasi – Future Information Security Trends (*Kasi – tulevaisuuden tietoturvatrendit*) conducted by Helsinki Institute for Information Technology HIIT and VTT Technical Research Centre of Finland and realized with a funding from the Tekes Safety and Security Research Program (*Tekesin Turvallisuus-ohjelma*). Kasi was initiated by PROJECT 8 and it has been working closely in parallel with the action program. The purpose of this project is to provide scientific support for the work of PROJECT 8. Kasi research project aims to study near-future information security issues that are related to, for example, new technologies, services, business models, and corporate structures, and identify information security trends, risks and opportunities. Information security trends and issues are assessed especially from the Finnish viewpoint. In addition, the project evaluates the need to establish a separate information security program for continuous foreseeing activities.

By studying future information security trends and finding threats and opportunities in them, we bring out knowledge that is relevant to both commercial actors and policy makers. The project analyzes information security trends in order to foresee emerging risks and opportunities in information society. The time span for the analysis is five to ten years from now. The study combines different viewpoints on information security: people, organizations, technologies, and services.

The research questions are:

- What are the most important information security trends in the next five to ten years? What are the factors and attributes that affect those trends?
- What kind of a method and process is needed to a continuous analysis of future information security trends?

In the study we address the research questions from several different disciplines. Our research group represents expertise in Social Sciences and Humanities, Service Design and Engineering, Computer Security, Human-Computer Interaction, and Legal Studies. We believe that this study will provide important, useful, and well-grounded new knowledge on future information security trends. We see this knowledge being fundamental in preparing us for future information security threats and opportunities, building future technologies and services, and in developing new businesses. It also helps in understanding online human behaviour, and the potential needs for future regulation and governance.

2 Related Work

A central goal of our work is to provide informational support for the implementation of the Finnish National Information Security Strategy. The actual action program consists of nine different projects that aim at increasing information security awareness, assessing service provider's responsibilities, rights and obligations, identifying information risks and data protection requirements, safeguarding continuity of business activities and the public's access to services, promoting Finnish information security expertise and active participation in international standards development work, increasing business competitiveness, accelerating the establishment of a National Communications Security Authority (NCSA) in Finland, enhancing and activating national cooperation in international information security issues, and measuring information security [1]. Our work concentrates on near-future information security trends in order to find out possible future paths that need to be taken into account if the other goals of the action program are to be achieved.

On the methodological level our work follows the example of other futures studies that apply scenario analysis and utilize experts' conceptions and knowledge as research data in order to foresee ICT related future trends [2]. This kind of work has been done both in academic and non-academic foreseeing activities.

From the European perspective, information security issues have been studied and promoted extensively by the European Network and Information Security Agency (ENISA). ENISA concentrates on issues of raising information security awareness, Computer Emergency Response Teams (CERTs), identity, privacy and trust as part of information security in general, reliable communications networks and services, and information security risk management. ENISA has made recommendations about contemporary and relevant research topics based on its own trend analyses. The topics are, for example, cloud computing, real-time detection and diagnosis systems, future wireless networks, sensor networks and supply chain integrity [3]. Future ICT trends have been analyzed in relation to more general social, economic and technical factors in several EU funded research projects including, for example, a Delphi survey on the future of Internet conducted by the Oxford Internet Institute [4], a research project on connectivity technologies led by RAND Corporation which combined scenarios, International Futures (IF) methodology and SWOT analysis [5], and a combination of system theoretic innovation analysis and impact assessment of the future software services organized by Pierre Audoin Consultants [6].

At HIIT, information security related topics have been studied, for example, as part of PRIMA research program, which concentrated on privacy issues in social media services and mobile Internet [7]. Within the PRIMA project Ovaska & Riihinen [8], for example, have elaborated the possibilities of using scenarios in privacy studies. Scenario analyses have been conducted at HIIT also within legal studies concentrating on the legal challenges of the future ICT businesses [9]. At HIIT, the connecting element in different information security and privacy related research projects has been a multidisciplinary approach to information security (see, e.g., [10]).

3 Methodology

3.1 Scenario Methods in General

In this study, we apply a combination of scenario analysis methods in order to approach the research problem of identifying future information security trends and factors that affect them. Scenario methods are especially useful for discussing *possible* futures and helping research participants to create and develop their viewpoints during the process. For example, interviews, questionnaires or related literature do not support the kind of playfulness and creativity necessary for thinking about possible futures. Our primary research data consists of conceptions and knowledge of specialists working in the field of information security. The primary material is complemented with comparable studies that have been conducted elsewhere and with a follow-up of current affairs related to information security in the media.

The scenario methodology originates already from the early futures studies conducted in the 1970s. It has been common to utilize specialists' knowledge in futures studies that apply so called "soft" futures research methods (in comparison, e.g., to computer simulations or statistical extrapolation from historical data). The soft methodology in futures studies is based on collecting and analyzing personal conceptions and knowledge that originates from individual experiences and understandings.

Conceptions and knowledge of specialists is often used as research data in future studies (particularly in Delphi processes, see [11]). The use of specialists' knowledge has been epistemologically justified, for example, by arguing that experts usually have the best understanding of the present state and the potential future of their professional field. It is also practical to use specialists as mediators or middlemen in the collection of data when the research problem would require a synthesis of a complex and wide-ranging set of relevant information [12]. The central problem with specialists' knowledge is the potential like-mindedness that prevents weak signals and alternative perspectives from emerging. Another problem concerns the sample of participants: how to make sure that all the relevant perspectives and understandings are represented in the data collection process? These problems are best resolved by calling in a diverse and competent group of participants and by creating a working environment in which also exceptional viewpoints can come out [13].

Scenario methodology is essentially concerned with "what if" questions. It is a proper choice when one tries to identify future trends that cannot be derived from historical data (as in the case of extrapolating from time-series) [14]. What is more, in order to grasp relevant aspects of a complex phenomenon, such as information security, the research data must be well contextualized (compare, for example, user statistics to use-case stories). Here concrete future scenarios provide a cognitively practicable instrument for identifying complex interdependencies between different factors, such as legal regulation, economic incentives, technological innovations and individuals' behaviour.

In the project we created scenarios in order to describe how the world might look like in the following 5–10 years, and what kinds of information security trends we might be facing. Scenarios in future studies are typically wide-ranging in their perspective and content, but here we have concentrated on possible services and use-cases that are grounded in literature, existing services, and discussions with content providers, operators, vendors, and other actors (cp. [15] [16]). We do not claim that the scenarios and trends identified here would come true in every imaginable future. Neither is their actual probability of coming true in the focus of our work. Instead, the trends are presented here in order to form a landscape of possibilities and concerns that might

exist in the future and that are deemed important future trends from a contemporary viewpoint. We attempt to answer, what would happen in given conditions. Methodologically, however, the trends must consist of believable and concise possibilities [17] [18].

The major difficulty in scenario analysis is to create scenarios that cover relevant and possible situations adequately. If we created them randomly, we would not be able to claim that they embody important issues sufficiently. To avoid such biasing, we need to create the scenarios in a systematic way. Unavoidably, the scenarios reflect participants' personal views. However, we believe that our systematic approach reduces the bias and makes the possible limitations visible to others for independent assessment.

3.2 Brainstorming, Design Games and Trend Analysis

Our approach consists of discussing and creating scenarios, identifying information security issues, pointing out future trends, and describing their relevant factors and attributes. First, we focused on sketching out possible future landscapes and their technological, human-related, and service-related conditions. Here we used the so called PESTLE method, which requires finding out *p*olitical, *e*conomic, *s*ocial, *t*echnological, *l*egal, and *e*nvironmental factors that might have a relevant role in the development of the society in the future [19, s. 317]. Second, the future landscapes (PESTLE results) were analyzed in order to provide relevant background knowledge for the concrete ICT related scenarios. After the scenarios were created, they were analyzed regarding their information security issues, and these issues again were grouped and categorized. Finally the information security issues were analyzed in order to identify relevant information security trends and factors that might affect their realization.

The collection and analysis of expert knowledge was conducted in three separate phases in connection with three separate workshops. Before the project begun, Sitra organized a preparatory workshop, in which several experts presented their views on information security issues and a large audience discussed freely the tentative ideas on emerging trends. After this, the first workshop was organized for outlining the future landscape in which the project was to operate. The special focus was in the PESTLE factors that affect future ICT services. The participants were encouraged to discuss freely about different factors that might affect the development of ICT services in the next 5–10 years. They were asked to identify different political, economic, technological, legal and environmental factors in order to gain a comprehensive understanding of the near future developments.

The workshop provided about 150 diversely categorized propositions about the future and, in addition, a punch of questions and personal opinions about future information security issues. In the analysis of the results it was discovered that there were more information security issues already in the first data set than was expected. The first workshop provided thus a first round for defining the focus of the research project, i.e. the relevant information security issues. However, when comparing to the related literature, there were limitations in the list of relevant PESTLE factors that were identified in the workshop. In order to reduce the limitedness of the PESTLE analysis, comprehensive background scenarios were presented as a background material in the second workshop [20].

The second workshop was organized in order to create four concrete future scenarios based on the previously gathered background information about the future. Two of the scenarios were created with a co-design method The Storytelling Group, which have been designed for collaborative creation of concrete use-case stories [21] [22]. The other two were created through a free brainstorming process concentrating on concrete

events on a timeline. The idea behind creating scenarios was to grasp complex issues with concrete future descriptions. The broad frameworks and themes of the stories were given beforehand but the actual stories were freely written by the participants. The resulting scenarios concerned a recruitment of a foreign employee, a future home help service, tracing of a person who had fallen ill on a journey, and a school bullying case.

About 50 different information security issues were identified from the scenarios by the research group. In the third workshop the transcribed scenarios were presented to the participants and they were asked to identify relevant information security issues in them. The issues brought out by the participants and by the researchers were then combined and grouped through an argumentative process. The process was an application of another design game called The Project Planning Game that has been used, for example, in the collaborative project design [23]. The main purpose of the game is to create a setting where different kinds of views and opinions can come out equally and deliberated collectively.

After the participants had grouped the information security issues, they were asked to evaluate them in order to sort out future information security trends, public interests, potential research questions, and issues that are of particular interest. Also the evaluation was an argumentative process. The results presented in this report are based on these evaluations and on the diverse arguments behind them.

After the workshops the trends were analyze in detail by the researchers in order to understand factors and attributes that would have an effect on their realization. The factors and attributes are presented in trend descriptions and tables in the following chapter (Ch. 4). The attributes of the factors describe the intensity (strong, medium, and weak) and the direction of the effect (intensifies (+)/constrains (-)) of the factor on the trends. The analysis was conducted in the project by the researchers who focused especially on research data provided by the participants in the three workshops. Related literature and work on information security trends has been used for extending the analysis.

4 Future Information Security Trends

This report is based on a general assumption that the role of information and communication technology (ICT) will increase as part of individuals' everyday life and societies' social, political and economic structures and processes. Technological infrastructure itself becomes more complex, more difficult to govern, and full of "black-boxes" that are often not understandable for users. Several trends that have information security and privacy implications were identified as relevant by experts in the project's workshops. These trends are presented and elaborated here in order to understand factors that affect them and mechanisms and conceptual relationships that connect these trends to information security and privacy issues. In the Discussion part (Ch. 5) information security and privacy trends and issues are analyzed more thoroughly from different viewpoints: these include privacy, information security and data protection, technological innovations, service innovations, and legal data protection.

The listed trends might cause societal tensions that can be interpreted as threats or possibilities depending on the evaluators' point of view (for possible points of view, see Privacy Issues, Ch. 5.1). For example, the proliferation of surveillance technology could be understood as a positive development for safety and security but also as a negative development leading to excessive control and impaired privacy. The trend analysis is supposed to reveal possible areas of societal tensions. These areas of conflict, whether they are interpreted as threats or opportunities, require action from individuals and societies. The solutions and instruments for governing these issues might be as diverse as law-making, technological improvements, self-regulation bodies, social norms and individual behavior. Both the areas of conflict and solutions to them might provide opportunities for commercial innovations, public policy and novel research.

The following sixteen information security and privacy trends and issues are not necessarily new, and some of them have already a long history. However, we suggest that they are emerging in new situations and in novel forms. Though the most trends have a global and long-term scope, here we focus on the Finnish environment within next 5–10 years. Based on the results of our foreseeing exercise, we summarize that:

1. The interdependency between societal processes and information systems increases
2. New interdependencies between organizations and the state emerge
3. Information security issues become more international
4. Needs to manage private or confidential information and public appearances in ICT environments increase
5. Protection of personal data becomes a considerable political issue
6. It becomes increasingly difficult to ensure the correctness of information
7. The correctness of information becomes increasingly important
8. Data gathering increases
9. Data combination from different sources increases
10. Traceability of persons and goods increases
11. Malicious action against information systems increases
12. Quality and security issues are increasingly taken into account in software development
13. Automation/autonomous systems are increasingly employed to effect security
14. Availability of information increases as the public information resources are opened
15. Commercial interests drive actors to restrict access to proprietary information resources
16. Governance of access to information resources in organizations becomes more difficult

4.1 Increasing Interdependencies

TREND: The interdependency between societal processes and information systems increases

Social and economic processes of our society are becoming increasingly dependent on the functioning of the existing information and communication infrastructure. This development is a consequence of increasing integration of ICT systems into our everyday lives. Information systems comprise a central part in many critical structures and processes from economic interaction (e.g., payments), electricity distribution, and communication networks to traffic systems. As the technical infrastructure becomes more complex and vulnerable, the same development applies to the functioning of the whole society which is dependent on the infrastructure.

On one hand, economic advantages of introducing ICT and the belief that ICT could help to cope with societal issues increase the expansion of ICT. The public sector plays a key role in this development with its productivity goals and standard of service obligations. On the other hand, the expansion of ICT might be slowed down by common resistance to change and by existing legislation that does not take specific properties of ICT adequately into account. Also the development of alternative and backup infrastructures might decrease the emerging interdependencies. The main motivation behind building backup systems is usually the fear of economic risks that, for example, infrastructure failures could cause.

Factor	Character	Intensifies (+) / constrains (-)	Effect
ICT is adapted to various societal processes	Technological	+	Strong
Alternative independent infrastructures and systems are developed	Technological	-	Weak
Economic incentives (such as cost reduction, increasing sales, productivity and effectiveness) foster the utilization of information technology	Economic	+	Strong
Increasing economic risks, such as infrastructure failures	Economic	-	Weak
Strong belief that ICT helps to cope with societal issues	Societal	+	Strong
Change resistance, criticism against the use of ICT	Societal	-	Med.
Government's productivity goals, standardization obligations, standard of service obligations	Legal	+	Weak
Outdated legislation	Legal	-	Strong

Table 1: Factors intensifying or diminishing the trend "The interdependency between societal processes and information systems increases"

TREND: New interdependencies between organizations and the state emerge

New interdependencies emerge also between organizations, companies and states. For example, if critical functionalities of public institutions are dispersed around different countries and handled by various private companies (for example, as a consequence of outsourcing) public institutions become dependent on the propriety of other actors' practices. Here also different regulation policies and legal structures might have a relevant effect on the autonomy of institutions' actions.

ICT enables tightening collaboration, but creates also new lock-ins between organizations. By lock-ins we refer to strong interdependencies or binding relationships between actors caused by, e.g., technological compatibility. These lock-ins could, however, be solved with technologies and standards that enable dynamic partnering.

The economic incentives behind the intense collaboration between organizations are the lower risks of long-term collaboration and the profits that the seller can gain by lock-ins. There is also a social incentive behind institutionalized collaboration relationship: it is usually more convenient to collaborate with partners that are familiar to actors based on previous experiences. On the other hand, dependencies that are packed by contracts and legal structures might cause increasing short-term risks as the flexibility of organizations in choosing their partners decreases.

New dependencies could also lead to the lack of competition in the market. Technological lock-ins in combination with the network effects typical of ICT can create exceptionally strong interconnections that require regulatory action (e.g., anti-trust cases of operating system and web browser tie-ins). However, these situations are usually covered by different competition and anti-trust laws.

Factor	Character	Intensifies (+) / constrains (-)	Effect
ICT enables tightening collaboration, which cause lock-ins	Technological	+	Strong
Technologies and standards that enable dynamic partnering (e.g., standard interfaces)	Technological	-	Med.
Strong and long-term collaboration decreases risks, lock-in increases seller's profits	Economic	+	Med.
Lock-in decreases competition and flexibility, dependency may increase risks	Economic	-	Weak
It is more convenient to communicate with partners that are familiar to actors based on previous experiences	Societal	+	Med.
Social reluctance towards dependencies	Societal	-	Weak
Contracts and other legal structures may strengthen partnerships	Legal	+	Med.
Competition and anti-trust laws increase competition	Legal	-	Strong

Table 2: Factors intensifying or diminishing the trend “New interdependencies between organizations and the state emerge”

4.2 Internationalization

TREND: Information security issues become more international

The international dimension of privacy and information security issues is a result of transnational information processes. As the ICT networks and businesses are global, and the users, servers, owners and companies are usually situated in different legal regimes, the need for international coordination of information security and privacy issues increases. However, the current lack of international legislation makes it difficult to solve the legal problems that have transnational effects. The current situation of parallel legal systems and dispersed official supervision is being taken advantage by, for example, spam distributors.

The globalization of information security occurs in parallel with economic and social globalization processes (global communication, streams of money and investments, movement of people and goods etc.). The opposing forces to these trends are the potential insecurity of markets and parallel localization trends that are caused by ideological or pragmatic motivations. In addition, although ICT is usually developed to function irrespective of the user's geographical location, it is sometimes actively used for blocking digital communication traffic beyond national borders.

Factor	Character	Intensifies (+) / constrains (-)	Effect
Expansion of transnational networks, interoperable technologies, development of technologies that function independently of the user's location	Technological	+	Strong
ICT is developed and used for national protection	Technological	-	Weak
Economic globalization	Economic	+	Strong
The growing insecurity of capital markets	Economic	-	Weak
Social globalization	Societal	+	Strong
Localization (ideological and/or pragmatic)	Societal	-	Weak

Table 3: Factors intensifying or diminishing the trend “Information security issues become more international”

4.3 Privacy/Publicity Management

TREND: Needs to manage private or confidential information and public appearances in ICT environments increase

Individuals, organizations and companies need to manage private or confidential information and public appearances because ICT-mediated activities increase in various societal spheres. Digital content creation on the one hand and digital footprints on the other are expanding while the original authors often have little control over the subsequent use of their information. Individuals produce content and traces, but they might also be objects of other individuals' actions (for example in pictures taken by others).

Factor	Character	Intensifies (+) / constrains (-)	Effect
Digital content created by and digital footprints left by individuals, groups and organizations will expand; actors have no sufficient technical control over their digital traces	Technological	+	Strong
Better usability and transparency of technologies and services (privacy management)	Technological	-	Weak
Economic importance of public image	Economic	+	Strong
Costs of developing tools and managing private data lead to individuals giving up their privacy management needs	Economic	-	Weak
Social importance of public image; citizens' consciousness of the relevance of privacy management issues increases; other actors produce information about data subjects	Societal	+	Strong
Certain types of private information lose their sensitiveness; in practice, people act only partly according to their privacy concerns	Societal	-	Med.
Strengthening data protection laws	Legal	+	Weak
Deregulation in respective legal fields	Legal	-	Weak

Table 4: Factors intensifying or diminishing the trend “Needs to manage private or confidential information and public appearances in ICT environments increase”

The control of one's digital content, footprints and privacy might be handled by individuals themselves or by groups interacting coordinately. An important issue here is the usability and transparency of information systems and services and their privacy management properties. In addition, individuals need ICT skills and a good understanding of the services they use.

The trend is intensified by the social and economic importance of individuals' public appearances. This factor pertains to organizations too. In addition to maintaining their public image, companies face the challenge of managing their confidential data in a sufficient and cost-effective way. The requirements of data management are mainly dictated by the data protection laws that might either become stronger or weaker, but they are also affected by the available technical tools that individuals and organizations have for the management of their private/confidential data.

The social change in valuations might affect the needs to data protection. If there is plenty of information available about individuals in the open networks, some types of private information might lose their sensitiveness. Based on various privacy studies (see, e.g., [24]), it is also reasonable to consider that people might act only partly according to their presumed privacy concerns.

TREND: Protection of personal data becomes a considerable political issue

Questions related to the individual's rights to use, determine or possess information that is created by her/him, or that concerns her/him, will be discussed more in public. In the future discussions will probably turn into questions of how to realize legal and moral rights in the quickly developing ICT environment, and if legal and technical means in general are adequate. The realization of rights in personal data might require that individuals *de facto* know, what information about them is being stored, where the information is being stored, and how it is being processed and distributed. These requirements could be satisfied, for example, with new technological and service solutions for personal data management.

The trend is a consequence of increasing amount of information that is collected, stored and processed about data subjects. It has been argued that in the future questions about privacy and information management and ownership would become as central as the environmental question was in the 1970's [25]. The intensity of the trend is affected by the acts of the legislator and the economic advantages and risks that might follow from the commercial use of personal data. Also, international discussions might have a considerable effect on Finnish public opinion.

Facto	Character	Intensifies (+) / constrains (-)	Effect
New technological innovations provide increasing opportunities for collecting, storing, processing and distributing information	Technological	+	Strong
New technology and services for the management of personal data are developed	Technological	-	Weak
The value of personal data as an economic resource will increase	Economic	+	Strong
Commercial use of personal data cause economic risks (bad reputation or accusations of careless data management)	Economic	-	Weak
Protection of personal data is a political question and related to the conceptions of humanity; the international discussions about protection of personal data influence Finnish publicity	Societal	+	Strong
In practice, most people do not care about how their personal data is being used	Societal	-	Strong
Personal data is an object of legal regulation; legislation is out-of-date and inadequate	Legal	+	Med.
Sufficient and sound legislation and supporting official actions	Legal	-	Med.

Table 5: Factors intensifying or diminishing the trend "Protection of personal data becomes a considerable political issue"

4.4 Validity of Information

TREND: It becomes increasingly difficult to ensure the correctness of information

Difficulties in ensuring the correctness of information are consequences of at least four interconnected developments. First, the amount of information that is collected and available continues to explode. Large amounts of information is collected and stored because actors prepare themselves for unforeseeable data uses. What is more, redundant information is rarely demolished.

Second, information is increasingly collected and combined from different sources. Third, as a result of combining different information sources, information itself will become more complex. Finally, the processed information is often a result of automatic collection and combination procedures, which function as “black boxes” in processing information.

As a consequence of the automation of complex information processes the users’ understandings of the properties of information and communication processes might decrease. The resulting question is how to assess the reliability of the available information. The assessment of information processes and actors might require, for example, new technical solutions or certification procedures. Because correct information is economically valuable, different actors have economic incentives to develop data collection methods and practices that ensure the correctness of information. On the other hand, as the number of information collectors and producers increase, the systems of trust and certifications become difficult to maintain.

Economic incentives for collecting large amounts of data strengthen the trend, since the correctness of particular information is usually of secondary importance when creating large databases (e.g., Google, Facebook). However, some parts of the information do have to be correct for the collected data to be of significance to anyone. Even our understanding of correct information might change along with novel business models.

Factor	Character	Intensifies (+) / constrains (-)	Effect
Technology becomes increasingly complex	Technological	+	Strong
Technology that helps to ensure the correctness of information, e.g., by comparing information from different sources and assuring the data integrity	Technological	-	Weak
Large amounts of information is collected and stored because actors prepare themselves for unforeseeable data uses and because redundant information is rarely demolished	Economic	+	Strong
Correct information is economically valuable and therefore there are economic incentives to develop data collection methods and practices that ensure the correctness of information	Economic	-	Med.
Need to protect privacy, to be anonym and even to lie	Societal	+	Med.
Social incentives to be identifiable and honest	Societal	-	Med.
The law requires restricting access to identifiable personal data	Legal	+	Weak
The law may require correcting errors	Legal	-	Weak

Table 6: Factors intensifying or diminishing the trend “It becomes increasingly difficult to ensure the correctness of information”

From a societal point of view, the difficulties to ensure the correctness of information are affected by two opposing factors. On one hand, actors might face social incentives or pressures to present themselves in an identifiable way. On the other hand, the

requirement of correctness might sometimes serve as a threat to the needs of privacy and anonymity in social interaction. These needs are supported by, for example, legal requirements to restrict access to identifiable personal data.

TREND: The correctness of information becomes increasingly important

The importance of correct information increases mainly due to the same factors as in the case of difficulties in verification (see the previous trend): e.g., the explosion of the amount of information and the complexity of technology. Social incentives have here an opposed effect: needs to identify data subjects will intensify and needs to act anonymously will decrease the trend. A central economic intensifier is the economic significance of correct information. Legal instruments have both intensifying and debasing effects: data protection law requires correcting errors in personal data while the disclaimers that limit the liability for incorrect information work in an opposite way.

Factor	Character	Intensifies (+) / constrains (-)	Effect
The amount of information explodes	Technological	+	Strong
Algorithms and other technology that do not rely on the correctness of information	Technological	-	Weak
The correctness of information is economically significant	Economic	+	Strong
It is profitable to collect large amounts of information	Economic	-	Med.
Social incentives to be able to identify people and assure correct information	Societal	+	Strong
Social incentives to let others be anonym or lie	Societal	-	Weak
Data protection law requires correcting errors in personal data; more in general the legal liability for incorrect information	Legal	+	Weak
Disclaimers that limit the liability for incorrect information	Legal	-	Weak

Table 7: Factors intensifying or diminishing the trend “The correctness of information becomes increasingly important”

4.5 Data Collection

TREND: Data gathering increases

In the following 5–10 years, data collection efficiency, volume, reach and minuteness of detail will increase. From a technical point of view, the underlying factors are the increased capacity and diminishing costs of computing resources. Whereas it seems probable that established data collection practices will remain important, we suggest that various new practices and purposes for data collection, storage and distribution will emerge. Several factors affect this development. First, a large number of societal actors are interested in collecting and using various kinds of data. Second, many companies see data as an important asset for creating revenue. Third, interconnected ICT-devices enable easy data collection, processing, storage and distribution.

The diminishing factors for the trend are information security technologies that restrict data collection, economic risks involved in unauthorized data collection, and social and legal norms that restrict data collection. The consequence of this trend is that plenty of data (of various kinds) is available for different societal actors like companies, public authorities etc. New information provides opportunities for service development and businesses. As the collected information proves to be valuable in economic terms or for public governance, opportunism and motives for using information to gain social, economic or political advantage will increase. However, when data, gathered for the initial purpose, becomes an important asset for the novel purposes, the initial purposes

for data collection have to be reinterpreted in order to stay within the accepted legal framework.

Data collection for public authorities' purposes – such as collecting citizens' fingerprints or taking electromagnetic body scans at airports – might be easily justified, for example, as an incremental improvement for safety and security. However, it is difficult to determine where to put an end for the data collection endeavors. When the public authorities collect fingerprints only for customs activity, it is a matter of time, when the collected information is needed or called for some other purposes.

Control and surveillance systems are also rarely demolished after they have served their purposes. Instead, they are sometimes put to novel uses. Data collection infrastructure that is once built will last long and provide new opportunities for data collection. New uses might not represent the original and publicly justified uses. Also the collected data might provide new unforeseeable uses of information. New uses are based on, for example, combining information of different types or from different sources (see Data Combination, Ch. 4.6).

Factor	Character	Intensifies (+) / constrains (-)	Effect
Technology enables collecting increasing amounts of data but also collecting new kinds of data	Technological	+	Strong
Information security technology restricts the amount of collectable data	Technological	-	Weak
It is profitable to collect large amounts of data	Economic	+	Strong
Costs of collecting data, compensations for damages if unauthorized data is collected	Economic	-	Weak
Socially beneficial to have lots of data, social power	Societal	+	Weak
Social norms that restrict acceptable data collection	Societal	-	Weak
Legal duties to record and be accountable	Legal	+	Weak
Legal rules that restrict collectable data (e.g., data protection law)	Legal	-	Med.

Table 8: Factors intensifying or diminishing the trend “Data gathering increases”

4.6 Data Combination

TREND: Data combination from different sources increases

Combination of different data types and sources will be an increasing trend in the following 5–10 years. At the moment new data combinations are challenging to produce because, for example, different information systems are not able to communicate together and data sources lack adequate semantic descriptions. However, in the next 5–10 years combining data from different sources will become easier as the techniques for data combination and systems interoperability (e.g., new data mining techniques and semantic standards) will be developed and introduced. Significant technical factors include also the diminishing cost and increasing efficiency of computer hardware and the interconnectivity of heterogeneous networks, which will increase the amount of data available and at the same time facilitate the processing of it. Other intensifying forces behind the trend are the interests of commercial actors to get better descriptions of their potential customers, and the objective of public authorities to combine and centralize information resources.

Previously mentioned technical factors provide unforeseeable ways to combine data from different sources. New information combinations might, for example, reveal new

aspects about the data subjects. This provides new opportunities for commercial purposes and service development, but it might as well threaten personal privacy. On the other hand, the increasing trend of data combination is potentially constrained by the lack of open interfaces, by the costs involved in data mining, and by the data protection regulations.

Factor	Character	Intensifies (+) / constrains (-)	Effect
Technological standards and interconnectivity of heterogeneous networks	Technological	+	Strong
Technological legacy systems complicate the combination of databases; lack of open interfaces	Technological	-	Med.
Data and data analysis are important revenue sources	Economic	+	Strong
Costs involved in meaningful data mining	Economic	-	Weak
Various societal actors benefit from novel data combination possibilities	Societal	+	Med.
Concerns regarding the implications of data combination to privacy and personal data	Societal	-	Med.
Obligations to publish governmental work results encourage officials to provide public electronic databases	Legal	+	Med.
Data protection regulations	Legal	-	Med.

Table 9: Factors intensifying or diminishing the trend “Data combination from different sources increases”

4.7 Traceability of Persons and Goods

TREND: Traceability of persons and goods increases

Traceability of persons and goods increases due to new sensor technologies and the growing trends in data collection and storage, surveillance systems and in the use of ICT-mediated services. Traceability of goods is strongly connected to the development of Internet of Things and RFID technology, whereas traceability of persons is a result of passive and active traces that individuals leave when they use various ICT-mediated services. Passive traces could be, for example, time-related or place-related data that is collected when using devices like mobile phones. Active traces are left when persons deliberately give information about themselves, for example, in social media services. While traceability of persons is not a new phenomenon (compare, e.g., to traceability of payments), it will increase as part of new applications and phenomena. An example of these phenomena is the growing use of social media services that already provide extensive records of personal information and continue to do so in the future.

Traceability might be restricted because specific ICT systems used for tracing persons and goods are often not connected to other systems that collect other kinds of information. Also legal privacy and data protection requirements might restrict the use of ICT for tracing purposes. Economic actors might even deliberately cover traces of their activities in order to, e.g., disguise the production circumstances of their businesses. On the other hand, traceability of persons (e.g., customers) and goods is a potential source for economic efficiency and new service innovations. Here tracing can be legally enabled by making it part of the provision of services. Finally, societal interests for surveillance, controlling and care are factors that naturally have a strong intensifying effect on traceability (e.g., social and healthcare services).

Factor	Character	Intensifies (+) / constrains (-)	Effect
ICT devices contain and are used to provide more accurate sensors which help in tracing both people and goods; servers can easily store huge amounts of data	Technological	+	Strong
Specific ICT systems used for tracing persons and goods are often not connected to other systems, complicating traceability across ICT systems	Technological	-	Weak
Economic efficiency, rising productivity, importance of data collection and new service possibilities	Economic	+	Strong
Some economic actors benefit from black-boxing their production chains (e.g., morally dubious production circumstances are sustained because they help to guarantee lower prices)	Economic	-	Med.
Societal interests for surveillance, controlling and care	Societal	+	Strong
Privacy and personal data protection issues	Societal	-	Med.
Traceability of persons and goods is enabled by making it part of the provision of services	Legal	+	Strong
Privacy, data protection	Legal	-	Med.

Table 10: Factors intensifying or diminishing the trend “Traceability of persons and goods increases”

4.8 Protection of Information Systems

TREND: Malicious action against information systems increases

The amount of malicious software has exploded and computer crime has developed professionally and organizationally. As individuals’, groups’ and organizations’ interactions are increasingly mediated through ICT, criminal and malicious action will follow them into virtual environments. One contemporary example of this development can be seen in electronic means-of-payment offences. Also, other kinds of destructive activities are getting their equivalents in the virtual world (e.g., cyber terrorism and cyberwar). A notable example of this is the Stuxnet affair [26], which was aimed exceptionally for industrial automation systems instead of relying on network connectivity. Also the evident technical virtuosity of Stuxnet manifested that there are parties capable of mustering substantial effort for malicious action when needed.

Interconnectivity and dependencies between information systems and networks creates vulnerabilities which are the target of malicious action. On the other hand, firewalls, separation of networks and other information security technologies work as a counterforce. Malicious action might be motivated by economic benefits and social incentives, the latter of which include, e.g., social respect and ideological justifications. However, public pressures to refrain from action might also decrease this trend. It is likely that international regulations for interfering malicious activities are difficult to implement.

Factor	Character	Intensifies (+) / constrains (-)	Effect
ICT systems are interconnected and interdependent heterogeneous networks	Technological	+	Strong
Separate intranets, firewalls and other means for protecting network connections of ICT systems	Technological	-	Weak
Various actors believe in gaining economic benefits from malicious actions	Economic	+	Strong
Economic losses if getting involved in these actions and getting caught	Economic	-	Strong
Ideological justifications for acting against “those in power” (multinational corporations, governments etc.)	Societal	+	Med.
Public pressure to stop actions	Societal	-	Weak
Difficulties in implementing functioning international laws	Legal	+	Strong
International agreements that are followed	Legal	-	Weak

Table 11: Factors intensifying or diminishing the trend “Malicious action against information systems increases”

4.9 Software Development

TREND: Quality and security issues are increasingly taken into account in software development

Attention to software development (e.g., Software Development Lifecycle methodologies SDL/SDLC) is increasingly paid in the industry and the trend will continue. The software industry is slowly transforming into a “routine” mode in creating new software and aiming for predictability and smooth flow of work. The buzzwords include “agile” and “lean” methodologies. Recently, the non-functional aspects of the development, like security, have been taken on the agenda as well. In Finland this is exemplified by the TiViT Cloud SW project [27].

The early “agile” and “lean” methodologies worked somewhat against the grain considering security, but the automated test and process solutions are coming to rescue here. These can take a lot of computing capacity, so advances in this field, including the so called computation clouds, will further speed up these developments.

Factor	Character	Intensifies (+) / constrains (-)	Effect
Increasing computing capacity (CPU/memory/devices/clouds) and more dynamic telecom/computing resource usage and management foster cloud computing	Technological	+	Strong
Technical complexity increases	Technological	-	Med.
Society's vulnerability to service disruptions will increase	Societal	+	Med.
Distrust in cloud services	Societal	-	Med.
Quality and data protection problems cost; criminal activity	Economic	+	Strong
Developing high-quality and data secure software is expensive	Economic	-	Med.
Legal liability for data protection, quality and security issues	Legal	+	Strong
Terms of use and disclaimers in use agreements	Legal	-	Weak

Table 12: Factors intensifying or diminishing the trend “Quality and security issues are increasingly taken into account in software development”

Also, the clouds themselves are a major driver behind the upsurge of interest to improve software quality and security; the stakes are simply too high to allow such cavalier attitude towards these issues that was commonplace in the past. With cloud-based software, failures and incidents are not isolated events affecting singular users, end-devices, or servers, but might have global repercussions (cp. Increasing Interdependencies, Ch. 4.1). Also the customers of such services are awakening to the risks and beginning to question the practices of those who develop the software that executes the services.

4.10 Automation

TREND: Automation/autonomous systems are increasingly employed to effect security

Automation/autonomous systems are increasingly employed to boost productivity and to alleviate negative effects of the “human factor”. In information security, human errors are a notable and notorious source of vulnerabilities. A recent study shows that 65 % of the cyber attacks are reported to make use of such errors [28]. The new “buzzword” seems to be “deep configuration assessment”. Increasing autonomy is no “Silver Bullet” [29], but the benefits are clear and the field will open up possibilities in the near term.

One should also remember the grim reality: recent reports state that only half of the end devices are protected in large parts of the world at all [30] [31]. Thus, to collect an army of victim machines is currently not a challenge at all for an intruder. The exploit writing can be accomplished routinely with specialised tools and for the usual end-user systems these can be even obtained “ready-made”. The challenging part of the criminal activity is to remain undetected and to break into guarded systems.

Factor	Character	Intensifies (+) / constrains (-)	Effect
Computing capacity increases (CPU/memory/devices/clouds), user I/O will be simplified, technical complexity increases, and smart grids will be more common	Technological	+	Strong
Difficulties in developing usable automation	Technological	-	Med.
Need to increase productivity; global competition (e.g., China rising) increases automation of work processes	Economical	+	Strong
Shortened horizon, quartile economy	Economical	-	Weak
Belief that technology supports good and environmentally friendly life	Societal	+	Weak
Societal fears of losing control because of (too much) automation	Societal	-	Med.
In narrow technical settings existing legislation supports automation (e.g., electronic signatures)	Legal	+	Weak
Complexity and deficiency of legal system inhibits automation	Legal	-	Weak

Table 13: Factors intensifying or diminishing the trend “Automation/autonomous systems are increasingly employed to effect security”

Of the related factors the “China rising” (one of the recognised factors in the workshops, that is, the foreseen commercial and technological weight of China) contributes to the trend by forcing western world to use automation for competitive advantage in all areas. “From physical products to the services” is another recognised factor referring to the shifting preference of consumers from ownership of expensive goods, say cars, to services like renting them. This development will entail related

automation of the service routines (say, automated reservations with a car rental service). As for the environment friendliness, automation contributes to the efficient use of raw materials and energy, fuelled by respective enlightened demand from the part of the consumer citizens. The factor “shortened horizon, quartile economy” has an effect of diminished future investments in automation technology including investments in automated security.

4.11 Access to Information

TREND: Availability of information increases as the public information resources are opened

Availability of governmental, municipal and other kinds of information that is being collected by public institutions increases as the public information resources are opened for citizens, researchers and commercial purposes. The process is intensified by new technical standards and open interfaces and a belief that opening data resources provides new ground for economic and social innovations. On the other hand, the process might be slowed down by technical restrictions (e.g. non-interoperable interfaces) and economic costs of opening databases. Moreover, although public demands for opening public information resources are strong, legal data protection issues and authorities’ slow actions might diminish the trend.

Factor	Character	Intensifies (+) / constrains (-)	Effect
New technical standards and open interfaces	Technological	+	Strong
Technical restrictions: old systems, no interoperable interfaces	Technological	-	Strong
Belief in new innovations based on open data resources	Economic	+	Strong
Costs in opening data bases	Economic	-	Med.
Ideology and public demands for openness	Societal	+	Strong
Unwillingness and slowness of authorities to open data resources	Societal	-	Strong
Obligations of public authorities to open their data resources	Legal	+	Med.
Data protection laws, IPRs	Legal	-	Med.

Table 14: Factors intensifying or diminishing the trend “Availability of information increases as the public information resources are opened”

TREND: Commercial interests drive actors to restrict access to proprietary information resources

Access to information resources might become increasingly chargeable or otherwise restricted. These developments are a potential impetus to a digital divide as some actors have economic resources to access and use information and others do not. Efficient technologies for managing access and payments of access would intensify this trend, although technical equipment like circumvention tools can also be used for bypassing restrictions.

From an economic point of view, both chargeable and free information can provide the basis for different business models. However, public demands for openness might work as a strong counterforce to the development of closed virtual environments.

Restrictions in the access to information resources might also be used in the market, for example, when a supplier favors certain retailers by regulating information distribution selectively. These restrictions are, however, regulated with competition and anti-trust

laws that may require the supplier to provide information not only to the partners but also to their competitors.

Factor	Character	Intensifies (+) / constrains (-)	Effect
Efficient tools for managing access and payments	Technological	+	Strong
Circumvention tools	Technological	-	Weak
Economic incentives; business models that are based on chargeable information	Economic	+	Strong
Business models that are based on free information (e.g., models based on advertising)	Economic	-	Strong
Social requirements for closed virtual communities and services	Societal	+	Weak
Ideology and public demands for openness	Societal	-	Strong
Better ways to control liability for third party applications and content	Legal	+	Weak
Competition and anti-trust laws may require that information is provided not only to partners but also to their competitors	Legal	-	Med.

Table 15: Factors intensifying or diminishing the trend “Commercial interests drive actors to restrict access to proprietary information resources”

TREND: Governance of access to information resources in organizations becomes more difficult

Access to information resources will become more difficult to manage and govern in organizations. There are two potential developments that might intensify this trend. First, outsourcing of functions in organizations makes it more difficult to control access to information resources. Second, the increasing number of fixed-time employees and volunteers in organizations is a potential cause for the same problem. From organizational point of view, these developments might lead to careless attitude towards good data management.

Factor	Character	Intensifies (+) / constrains (-)	Effect
Databases are connected to networks (malicious attacks), information systems become more complex	Technological	+	Med.
More efficient technologies for controlling and tracing accesses	Technological	-	Weak
Outsourcing, high turnover of employees, limited economic resources for sufficient data management and protection	Economic	+	Strong
Increasing costs of not being able to govern	Economic	-	Med.
Culture that encourages actors to leak out information (e.g., Deep Throat, WikiLeaks); careless attitude towards good data management in organizations	Societal	+	Strong
Loyalty, need to obey rules	Societal	-	Med.
Laws that restrict control and surveillance of access in organizations	Legal	+	Weak
Laws (e.g., data protection law) that require good practices in information security	Legal	-	Med.

Table 16: Factors intensifying or diminishing the trend “Governance of access to information resources in organizations becomes difficult”

Connectivity of information systems and networks is a potential cause for unauthorized accesses. These could be prevented with efficient controlling and tracing technologies

and practices. Implementation of sufficient data management and protection procedures might, however, become too costly for organizations. The social motives behind unauthorized accesses might be, e.g., different ideological justifications and a culture that encourage actors to leak out information. On the other hand, social pressures to be loyal and to obey law and organizational rules have opposite effects on the trend.

5 Discussion

5.1 Privacy Issues

The identified trends raise various privacy issues, which have to be dealt with one way or the other. For doing so, it is useful to understand that there are various conceptual approaches to privacy, ranging from different normative claims about how to build a “good” society to behavioral analyses of situated interaction, in which privacy is understood as a method for regulating contact. Because of differences in education and discourse, various actors working with privacy (lawmakers, lawyers, data protection experts and scholars such as social scientists, legal scholars and academics in information security) tend to understand privacy in different ways. It follows that it is especially important to be explicit about one's understanding of privacy, as well as the normative framework in which the understanding is embedded.

Value-based privacy discussions are especially important for deciding how to react (if at all) to the identified information security and privacy trends. Questions that arise in value-based privacy discussions are tied to the organization and government of society, to the rights of individuals, and thus to different notions of a “good” life. In value-based privacy discussions, various viewpoints tend to compete with each other and are in some cases irreconcilable. In tracing value-based privacy discussions we may differentiate roughly between three points of view, which follow a libertarian perspective, a communitarian perspective and a viewpoint in between a strictly libertarian and communitarian perspective.

A libertarian perspective underscores the role of privacy for self-realization, giving individuals control of how to realize a “good” life and simultaneously restricting the power of governments over it (e.g., [32] [33] [34]). Here, the right to be let alone [35] is a right that has to be fought for. A communitarian perspective again regards pursuing a common good to be more important than individual self-realization and thus favors communitarian values over individual privacy (e.g., [36] [37]). A third important perspective between the libertarian and the communitarian one highlights that individual privacy is not important because it allows individual self-realization, but because it is an inherently collective and egalitarian value. Without privacy, freedom of speech and freedom of association are at risk, since individuals cannot gather privately together in order to test and formulate statements that are not yet ready for public discussion. Also discriminatory practices based on collective differences are delimited because of privacy, since public discussants are ideally only judgeable in regard to their public statements instead of age, gender, ethnicity, religiosity, and political affiliation (see, e.g., [38] [39]).

The focus on the various understandings of privacy on the one hand, and differences in value-based frameworks for understanding privacy on the other, call for dealing with privacy issues of ICT use in a processual manner. According to this, various sources for possible societal tensions are worked out, and questions of privacy and societal values are actively debated. Privacy is not an issue that can be solved solely and once and for all with a regulatory practice, but an issue that attracts already heated debate (e.g., public discussion about the Act on the Protection of Privacy in Electronic Communications, amendment 125/2009) and continue to do so in the future.

The identified trends raise various issues for privacy debates. As data gathering, data combination from different sources and traceability of persons and goods increase, it is ever more difficult to retain private selves which do not appear to other societal actors. Individuals' digital trails, digital “selves” and their access to digital databases make societal actors part of ICT-mediated publicity that is difficult to control. The traditional

right to be let alone [40] taken up in many privacy discussions (e.g., right to opt out from ICT systems) is not a sufficient means to react to privacy issues in ICT environments. Instead, public discussion and policy makers should reflect on the specific ways in which a *right to be included* [41] can be secured. This is important because ICT users should not be at the mercy of exploitative corporations or possible future authoritarian governments, or simply outside the daily operations of an increasingly computerized society (e.g., citizens without skills or wealth to participate) because of malfunctioning ICT systems. Availability of governmental and community information to the public, business models supporting ethically and legally sound data transfer and users' possibilities to co-create the future of ICT in Finland are the first steps on such a road. The internationalization of information security issues, as well as increasing malicious action against information systems adds complexity to the question of how to build good practices.

5.2 Information Security

The threats to the protected systems will not fade away: the attacks will be more professional, and more narrowly targeted, and will try to utilize wider “attack surfaces” (the routes available for an attack, say, open network connections, listening communication ports in machines, software vulnerabilities present in systems, configuration errors, and the like). The present organised crime scene is multiparty, multistage and multimodal. Multi-party, since divisions of work have evolved, multistage, since the operations have several steps, performed by specialised parties, and multimodal in execution due to combination of, *inter alia*, traditional style confidence tricks, social engineering, “dumpster diving” and technological means. And, should these fail, there are also “rubber-hose crypto analysis” – use of physical violence to obtain passwords – and blackmailing available for criminals unscrupulous enough. Thus, to truly protect information resources the scope of the countermeasures must be wide, since the malefactors will choose the easiest method, whatever it is.

As for end-users, the easiest way to seize their valuable information is to apply what are essentially new applications of traditional confidence-tricks (e.g., phishing), not forgetting sneaking into unprotected user machines [42] [43]. The most valued targets are of course employees handling money-flows of substantial companies, although private persons' account and ID information (identity thefts) are not sneered at. There is hope that the situation will improve in future (5–10) years due to advances in automatic/remote security solutions (including clouds computing services). Also, the security of the end-user platforms will improve, as well as the software run on those platforms, due to increasing industry investment in these issues. This will make it harder for the malefactors to find suitable vulnerabilities to exploit. But the complexity of these devices will make it a safe bet for the near future that some slight lapse of diligence will now and then yield opportunities for sinister undertakings.

A remote intrusion attack against networked systems can be divided in reconnaissance, break-in using an exploit, reinforcement (bring in the rootkit etc.) and consolidation phases [44]. Of these, the reconnaissance is very difficult to detect, if professionals are in question, since the traffic used tries to closely mimic normal traffic. In fact, no easily detectable scanning tools like “nmap” are used against protected sites. Therefore the vulnerabilities open for exploits are tried to be blocked, and any exploit wandering around to be found out in time.

Further improvements will necessitate closer, more comprehensive and practicable surveillance (the current “buzzword” being “situation awareness”) and management (especially configuration) activities. The detection of exploits is however facing

difficulties since the adversaries have not been idle either; zero day (no known predecessors) attacks and (self)mutating malware are undermining this approach.

Hardware assisted security functions, e.g., trusted platform modules (TPM), processor memory area protection and the like, will appear little by little. For example, Intel has recently announced that it has developed a cure for “zero-day” attacks. Whether such solution has been found (even for a class of such attacks), remains to be seen [45].

Of the basic security services, authentication has always been a headache. In recent past things like IDM (IDentity Management) has been one of the major causes for this. Lately authentication has gained attention due to the use of virtual machines within cloud services. To sort out the basic fact of the identity of the virtual machine communicated with TPM – trusted platform module – might come into rescue to authenticate Virtual Machine instances (in clouds) with confidence [46].

Attacks aiming for service disruptions, DDoS (Distributed Denial of Service), are tricky to handle, and are known to include extortion as one of the motives. Political tensions (cyber-attacks on Estonia [47]) and even spontaneous protests (to support, e.g., WikiLeaks, by operation payback [48]) have stimulated attacks. In the future, networks will evolve to provide some autonomic response to these, but the prerequisite will be an overhaul of the underlying Net.

Taking a look at confidentiality within networks, the spreading of data into various remote caches, swap and other memories is an ever more acute problem (due to uprise of cloud services, again) waiting for a solution. And, there are concerns about cloud based espionage, even cloud services specifically deployed to collect data for foreign states who wish to keep their domestic industry supplied with up-to-date foreign competitor secrets. [49.]

Keeping up privacy is challenging in the current form of Wold Wide Web. Even those removing diligently their cookies, supercookies (local data saved by browser plug-ins like Macromedia’s Flash) and browsing histories cannot be sure that they are entirely invisible, new tricks are being introduced when the user gets too acquainted with the old ones. Currently, the “leading edge” includes things like “Evercookie” [50] and “Panopticlick” [51].

Long-term durability of data is a growing concern, since the currently used memory technologies have a data lifetime expectancy of a few decades only. The nanotechnologies being researched to solve this problem are simply amazing; promising durability of billion years and density of one trillion bits per square inch [52]. Another emerging technology, Digital Rosetta Stone, is expected to keep the data intact for a thousand years [53].

5.3 Technological Innovations

The technological scene of the world within 5–10 years will certainly be more complex, diverse, potent and pervasive than today. The very basics of the subsistence of citizens of the developed world will be in the verge of change; the most valuable of his/hers technological possessions – for most people the automobile – is about to experience a metamorphosis into fully electric form due to vastly improved batteries being developed today. This will be a slow change, but it is one force driving the evolution of the electric grid, the “blood circulation” of the technology, to a “smart grid”, capable of optimising the production and consumption of energy, involving storage for handling intermittent energy sources/sinks and transactions needed to cater for the growing fleet of electric cars. In short, smart grids will be highly conversant and conversing.

The nervous system of the society – the communication networks – will thus be ever more tightly intertwined with the critical infrastructures, also other than electric grid. This development will be in full swing, though not yet completed in the time frame under study here. Already now some major players like SAP and Siemens [54] are teaming up to be able to offer new solutions in the area. This will surely be an arena for innovative applications needing likewise innovative solutions to secure them.

Aside that information networks will pervade other infrastructures, they will evolve themselves. Future Internet and cloud computing technologies will share common ground. Particularly, both will understand application layer dealings and prefer true names, i.e., names like URN (Uniform resource names [55]), over IP-addresses when discussing with each other. This will both complicate the network side and simplify the client side, the respective amount of security responsibility shifting to the network. This is an emerging area, being moved forward by the need for such solutions by the cloud computing technologies [56]. Those who remember the appearance of the World Wide Web, surely recall the commotion surrounding URLs, that is, the race for the best domain names. Something similar might be in store for the future. Naturally, the security side will require further thought.

From (cloud) end-users point of view, there will be no definite borders and gateways (within clouds) to oversee traffic, or to see it at all. This state of affairs will mean that the user visibility will be restricted to application level, leading to emphasis being placed on application level security. To meet the need, clouds need to offer appropriate tools, say for DLP (Data Loss Prevention, IDM Identity Management), application aware & user modifiable IDS (Intrusion Detection System/IPS), Intrusion Prevention System, and the like.

Taking the cloud service providers view, they will need to deploy tools to deter attacks, to detect suspicious (potentially criminal) user activity, and means to collect forensics data. For fast response, public law enforcement agencies are developing to engage quickly ("net-traffic police").

For users and providers alike an approach for IDS/IDP could be white-listing scripts/code, perhaps in cloud context, since the hash-based detection has lost its power against the mutating variety of malware and the amount of code to be tracked is huge in both cases anyway. The "walled garden" services like Apple could be thought to be a step into this direction. Within a "walled garden" the service assortment is controlled by a singular provider, that is, the services are subject to centralised approval and charging procedures. Also, demarcation and enforcement of computational zones (geographically restricted clouds) to fulfil legal requirements is in demand, and solutions are likely to appear.

In addition to the above, the cloud context will provide a wealth of challenges for:

- Autonomous checking of cloud (security) configurations.
- Setting up specialised "honey pots" – computer systems set up with an intention to lure intruders and to collect incriminating evidence about them.
- Seeing over insecure end-devices with increasing sophistication. Examples of this include offerings like Symantec.cloud [57]. And where the users are moving to, criminal activity is also heading for, with intention to counter the new defences [58].

The development of new software will embrace a set of new tools, dedicated to better cope with the security requirements. Due to the nature of the affair, the other alternative

would be “stiffen” and “fatten up” the newly adopted “agile” and “lean” approaches. This will be still needed for some degree, but where tools can assist, they will be adopted. Such tools can be developed in Finland, and perhaps offered as a service (e.g., as a cloud computing service).

The demand for traceability, due to counterfeit prevention and surveillance of say, foodstuff manufacturing, will open up possibilities for those who will come up with economical and secure solutions.

5.4 Service Innovations

The emerging global trends in ICT will form the future service ecosystems and are expected to cause remarkable impact by breeding new opportunities for service innovation. The global trends are rooted in technology, since new technology often opens possibilities for new services. What is important for the future of service innovation is that service can be created, accomplished and delivered by tapping into the collective power of various ICT trends to deliver new forms of meaningful services to users.

The future trends in technology and social life will enable quantum leap for future service innovations. In five to ten years we will experience rich flora of new and innovative services appearing suddenly on the market together with technical innovations. We may think that societies today are already too dependent on the Internet and computerized services but the obvious trend is that even more aspects of everyday life, commerce and working environments will become digital and will be served and used over the net. The social communication and co-living over the networks will be adapted on all the levels in the society.

The private life experiences and its management will become important to people in the digital world, which will offer new opportunities, for example, for assistive privacy services. Privacy is an integral part of the social life and allows relationships, e.g., to one's mother, manager, friend, etc. to stay on a private level. Strong privacy mechanisms are needed in the future to manage our individuality in social relationships and its emotional depth. Privacy is not only a personal phenomenon, but a common and equal value, which allows freedom of association and of expression, and limits discriminatory practices. Life would be difficult without means to regulate privacy and publicity. This creates a need for service innovations for management of privacy/publicity in social relationships. As we are experiencing today it is extremely difficult to manage personal information in the web. When any unwanted information appears there, it is very difficult or impossible to correct it or remove it. However, future developments in regulations will open up new opportunities for solutions and enable a new service innovation area for the management of digital information about individuals, enterprises or any other identified entities.

As we have pointed out earlier, a strong ICT trend today is the growth of cloud based solutions, where the Web services are produced in a pool of servers with virtual platforms. The solution looks like a traditional central computer system upgraded with virtual technology, which it basically is. The current Internet and web technologies give freedom to process the web service call anywhere in the net and it can be done most effectively in large server pools. The cloud solutions are challenging to information security but also affordable to service providers. Information security can be improved by offering improved protection in cloud systems. But clouds also enable an effective platform for creation of new vulnerabilities and threats. Thus the race between exploiters of vulnerabilities and antivirus solutions will continue. New service innovations are needed to keep the cloud services trustworthy.

The cloud services, operated in Finland, could offer a natural platform for secure data storage and backup serves globally. The driver for utilizing such a storage and backup services is usually the fear of economic risks that infrastructure failures, vulnerabilities, cyber attacks, fire etc. may cause. Finland as a neutral, reliable and stable society would offer optimal environment to offer such a service world wide [59]. Some approaches in that directions can be obtained when Google establishes a large server park in Kotka within a couple years.

The information we receive via Internet and Web has become economically valuable and important to people, the enterprises and societies. Unfortunately there exists a lot of unreliable and even fraud information in net and it is difficult to verify the correctness of received information. There might be an opportunity to develop Finnish-based services for data analysis and verification, collection methods and practices that ensure the correctness and integrity of information.

5.5 Legal Data Protection

From the legal point of view, an essential part of information security is the data protection law. In Europe data protection is extensively regulated by directives and regulations. The two most important legal texts in this context are Data Protection Directive (95/46/EC), which is about the protection of individuals with regard to the processing of personal data and about the free movement of such data, and Directive on Privacy and Electronic Communications (2002/58/EC), which applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks.

In addition, numerous national laws include rules that affect data protection. They may stipulate more in detail and more strictly how personal information is to be handled in certain situations, or they may authorize certain usage of private information more freely than general rules would allow. Privacy is also protected by penal codes. Consequently, the legal construction of data protection rules is quite complex. Unfortunately, the rules governing privacy cannot be found in one law, but they are spread out in numerous statutes.

In general, the law restricts the processing of private data. For example, there has to be an acceptable purpose to process personal data and it is not allowed to use the data against that purpose. However, if the person gives consent, then almost any processing is allowed, but the consent needs to be specific and informed. Thus, it is central what the end-user knows and understands about the processing of the personal data.

It is important to realize that the data protection law is not prohibiting businesses and services to avail of personal data. On the contrary, it tries to define a legal framework that enables business. It is quite possible to develop services in a way that they comply with the data protection law. However, the rules are quite complex, and it is also easy to develop services that do not follow the law, if the data protection law is neglected while designing the new service.

The trends identified in the project illustrate the big changes that are happening. The legal system, by its nature, is not proactive or even dynamic. The laws will always follow somewhat behind the general development. Therefore, the conflicts between new phenomena and outdated laws will increase. The legal certainty and predictability require that one is able to reasonably foresee how an act will be assessed legally afterwards. On one hand, the legal system needs to be quite stable to provide certainty. On the other hand, the stable system may produce unpredictable legal results when new phenomena appear. Thus, to overcome this dilemma of legal uncertainty, it is likely that

especially business actors tend to rely more and more on contracts instead of laws while creating new ways of doing business.

The data protection law, however, includes mandatory rules that cannot be overridden by agreements. Therefore, all the problems with outdated laws cannot be solved by contracts. Thus, the lawmakers will face increasing demands to deregulate data protection, while private people may need more protection in the ever more complex environment. This conflict between needs of regulation and deregulation as well as a stable and a dynamic legal system will increasingly colour the discussion on data protection in the future.

6 Conclusions and Recommendations

The aim of the project was to study near-future information security issues that are related to, for example, new technologies, services, business models, and corporate structures. We identified relevant future information security trends by collecting and analysing specialists' conceptions and knowledge of the various developments in their professional fields. In order to deepen the analysis, we also specified factors and attributes that affect the realization of the trends. The trends and issues have been assessed here especially from the Finnish viewpoint and the time span for the analysis is five to ten years into the future.

The research process went through five separate steps: 1) outlining the future environment, 2) creating concrete future scenarios or stories, 3) analyzing information security issues in the scenarios, 4) identifying information security trends, and 5) specifying factors and attributes that affect the realization of the trends. Our major findings concerning the future information security trends have been presented in the previous chapters. As a summary, we conclude that different societal and organizational interdependencies will increase, management of private and confidential data and the correctness of information will become increasingly important, data collection and combination will increase, access to data sources will meet both opening and restricting developments, and traditional data protection issues will remain central.

The realization and intensity of these trends are dependent on several factors that we have categorized as societal (e.g., changes in social valuations and behavior), economic (e.g., economic incentives, business models and potential risks), technological (e.g., new innovations, the expansion of ICT into everyday life) and legal (e.g., outdated legislation, slow regulation process). The factors have both intensifying and constraining effects on the trends and the intensity of their effects might vary. We find the analysis of effecting factors important because it shows the contingent nature of the identified information security trends.

Our approach combined perspectives from different disciplines in order to adequately address the complexity of information security issues. From the privacy point of view, the identified information security trends call for rethinking how privacy should be granted in future ICT environments. Our suggestion is to employ a continuous process for assessing information security and privacy issues in order to detect developments in societal ICT use. From the traditional information security point of view the stage is changing, not so much due to disruptive technologies but due to ways of organising the production of computing services; the direction is towards outsourcing remote, operationally distributed services. The scene of action is also expanding: smaller, intelligent mobile end devices are beginning to experience the same menaces as the workstations after having made their breakthrough. The same fate will await other sufficiently smart devices to be connected to Net (Internet of Things). And, the formerly largely undisturbed areas, like infrastructure and industrial control systems, are will follow.

From the service innovation point of view the future society will be ever more infused with the various technical manifestations of the people's need to interact, influence and to present themselves to the world. To work well, such systems need to be accompanied with means of managing individuals' exposure and to assist in making the right choices. From the technological innovation point of view several challenges are presented: in the creation of more secure software that is needed for cloud computing services, and in the field of operational security of those services. New solutions for protecting users and their privacy, securing vulnerable end devices, guarding networks (future Internet, infrastructure control) and tracking goods are possible. From the legal point of view

there will be increasing demands to deregulate data protection, while private people may need more protection in the ever more complex environment. This conflict between needs of regulation and deregulation as well as between a stable and a dynamic legal system will increasingly colour the discussion on the legal side of information security and especially data protection in the future.

At least two limitations concerning our results must be mentioned. First, our purpose was to outline possible futures that have been derived systematically. In addition, we have tried to understand and explain complex interdependencies between different factors that might affect the realization of the future information security trends. Even then, our findings must be treated as contingent matters: instead of forecasting, our work is about foreseeing. Second, the results represent conceptions of a particular group of information security specialists working in the public sector, companies and research organizations. A different group of participants could have highlighted different issues. However, this limitation does not diminish the relevance of our findings. On the contrary, it should be considered as a methodological finding for improving the foreseeing method and extending the results in further studies.

Taking into account the previously stated reservations, we believe that our work on future information security trends and on the methodological questions about reliable foreseeing activities provides relevant information for commercial, policy and scientific interests. We propose that in order to get reliable foreseeing results in the long term, the process of identifying future information security trends should be continuous. The continuous process would also provide good opportunities for improving the foreseeing method. In any case, this project provides a firm starting point with practical foreseeing guidelines and with the first round of results concerning future information security trends.

6.1 Guidelines to Continuous Trend Analysis

We suggest that, from now on, the process of analysing future information security trends should be continuous. The method that we have used in this project has shown to be productive, and with adequate improvements, it can serve as a basis for a continuing process.

The foreseeing process is based on a series of three or four workshops, which will be repeated. Between the workshops, the results are analysed and refined, and the next workshop is prepared. In our project, we had a preliminary workshop before the project actually started. It discussed information security trends on a general level. In the future, this kind of preliminary workshop will not be necessary. The three workshops that the project organised were essential and successful and should be included in the continuous process. Based on the experiences it is reasonable to organize one more workshop to discuss the trends further, or to change the last workshop to include more trend analysis. Therefore, we suggest that the future process would follow the path described in the figure (Figure 1).

Each cycle starts by planning the first workshop that applies the PESTLE method to find *political, economic, social, technological, legal, and environmental* factors that affect information security in the next ten years [60]. Before the second workshop, the factors are analysed, grouped, and refined, and the next workshop is prepared. This includes finding a set of suitable large macro scenarios that can be used as backgrounds for the concrete scenarios that will be created in the workshop [61]. In the second workshop, a few scenarios are created representing possible situations that are somehow related to information security within ten years. In the workshop, playful methods, e.g., The Storytelling Group, could be applied [62].

Before the third workshop, scenarios are analysed, tentative information security issues are pointed out and the next workshop is prepared. The third workshop is organized for identifying information security issues from the scenarios. Here, e.g., The Project Planning Game can be applied [63]. After the workshop, the information security issues are analysed, grouped, and refined, and the fourth workshop is prepared. The fourth workshop is about defining information security trends. The issues are discussed in order to find the directions into which they are developing and thus forming the future trends. The trends are described and it is discussed how technology, economy, social norms, and legal system strengthen and weaken them. Also, it is analysed what kind of consequences the trends might have and what conflicts they might cause. Finally, the cycle ends with refining the process, planning the next cycle, and reporting the results.



Figure 1: A suggestion for continuous information security trend analysis.

There are two major prerequisites for the process to succeed. First, it is essential to make sure that the participants in the workshops represent widely enough all stakeholders and actors in society, and that they have enough expertise. In each of our project workshops, we had about 15 participants. They were highly qualified experts, but as most of them represented either corporations or research institutes, the distribution of their backgrounds could have been more diverse.

Second, it is mandatory to have enough resources between the workshops to refine the workshop results and to prepare for the next workshop. Also, to succeed, the workshops require capable leaders, who know the methods and are able to make the participants to contribute to results. In that sense, our project was very successful, since the project researchers were able to elaborate the results and make preparations for the workshops,

and Vesa Kantola was an experienced workshop leader. In the future, however, it is essential to take care of providing the process with enough resources and personnel.

6.2 Suggestions for further studies

We suggest that the work done in this research project would be continued in four different branches of further studies: examination of complex interdependencies in regulation, analysis of different information security discourses, investigation of the prerequisites for gaining the envisioned interest in Finland as a safe haven for data, and further development of the foreseeing method that was applied in the project.

Different interdependencies between regulation, economic incentives, changes in valuation etc. comprise a complex system, where effects of a certain change are difficult to anticipate. Here we have evaluated potential effects of a change in complex systems by analyzing different factors and attributes that might affect the realization of identified information security trends. However, the identification of complex relationships is a central problem in almost any study representing policy research. The analysis methodology presented here could be developed in more detail in another research project that concerned a different policy issue. Even here, different social, economic, technological and political effects on information security issues could be simulated more thoroughly with a model that described complex interdependencies, e.g., in a situation, where pricing or the availability of services were changed. This kind of a modelling study would provide information, e.g., on the problem of unforeseeable consequences of over-regulation and under-regulation of economic activities.

Another interesting question is how the conceptions and knowledge of information security issues are being constructed. The current project already provides research data for analyzing how information security issues are framed and conceptualized among information security specialists. The framing of information security could be analyzed, e.g., in connection with contemporary discussion of securitization in the social sciences. Central questions in discourse analytic approach to information security would be: what issues are understood as information security issues, how are they articulated and framed, and how are these conceptual processes affected by professional and disciplinary discourses? These questions lead essentially to the problem of how our information security needs are actually created. As a concept of traditional information security studies, information security might be adequately defined and without high controversy. As a policy concept, however, information security becomes an instrument for advancing certain interests and for suppressing others.

On the technological side of things, the prerequisites for gaining the envisioned interest in Finland as a safe haven for data [64] are proposed to be investigated. These include infrastructure related aspects, of which we mention smart grids, future internet and cloud technologies. These developments are not isolated, but rather intertwining, and they involve many information security challenges. These include research related to the secure software development and operational information security, not forgetting autonomous features, data back-up, data durability and reliable data removal. In case of remotely provided services the ability to provide proofs of the (security) measures taken will become an issue. Additionally, the advancement of privacy will require technological measures that could develop into commercial activity. These are suggested as a candidate for further study, too.

Finally, we propose that the foreseeing method that has been used here would be assessed more rigorously in connection with the original goals of this project and in the light of its future applications. Our experience already provides good grounds for improving the method and analyzing its advantages and disadvantages. We find it

reasonable to apply the method also in other kinds of foreseeing projects that are not necessarily related to information security issues. A different application context would produce comparable results on the usefulness of the method in general foreseeing activities.

7 References

- [1] Ministry of Transport and Communications, Action Programme "Everyday Security in the Information Society: A Matter of Skills, Not of Luck". Implementation of the government resolution on National Information Security Strategy. Liikenne- ja viestintäministeriön julkaisuja, 51. 2009. <http://urn.fi/URN:ISBN:978-952-243-127-1> (downloaded on 1 Feb 2011)
- [2] Karlsson, B., Bria, A., Lönnqvist, P., Norlin, C. & Lind, J., *Wireless Foresight: Scenarios of the Mobile World in 2015*. Wiley, Chichester. 2003.
- [3] Gorniak, S., Ikonomidou, D., Saragiotis, P. et al., *Priorities for Research on Current and Emerging Network Trends*. European Network and Information Security Agency. 2010. <http://www.enisa.europa.eu/act/it/library/deliverables/procent> (1 Feb 2011)
- [4] Forge, S., Guevara, K., Srivastava, L., Blackman, C., Cave, J. & Popper, R., *Towards a Future Internet: Interrelation Between Technological, Social and Economic Trends*. Interim report. Oxford Internet Institute. 2010. <http://www.future-internet.eu/publications/view/article/towards-a-future-internet-interrelation-between-technological-social-and-economic-trends.html> (1 Feb 2011)
- [5] Cave, J., van Oranje-Nassau, C., Schindler, R., Shehabi, A., Brutscher, P.-B. & Robinson, N., *Trends in Connectivity Technologies and Their Socioeconomic Impacts*. Final report of the study: Policy Options for the Ubiquitous Internet Society. RAND Corporation. 2009. http://www.rand.org/pubs/technical_reports/TR776.html (1 Feb 2011)
- [6] Aumasson, A., Bonneau, V., Leimbach, T. & Moritz, G., *Economic and Social Impact of Software and Software-Based Services*. Pierre Audoin Consultants. 2010. http://cordis.europa.eu/fp7/ict/ssai/study-sw-2009_en.html (1 Feb 2011)
- [7] Bylund, M., Johnson, M., Lehmuskallio, A., Ovaska, S., Rähkä K.-J., Seipel, P., Tamminen, S. & Turunen, M., *PRIMA: Privacy in the Making*. Final financial and scientific report. 2010.
- [8] Ovaska, S. & Rähkä, K., *Teaching Privacy with Ubicomp Scenarios in HCI Classes*. Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group. OZCHI 2009, 411, pp. 105–112. ACM, New York. 2009.
- [9] Pitkänen, O., *Legal Challenges to Future Information Businesses*. Doctoral thesis at Helsinki University of Technology. HIIT Publications 2006-1. Helsinki Institute for Information Technology HIIT. 2006.
- [10] Bylund, M., Johnson, M., Lehmuskallio, A., Seipel, P. & Tamminen, S., *Privacy Research through the Perspective of a Multidisciplinary Mash Up*. In Greenstein, S. (ed.), *Nordisk årsbok i rättsinformatik 2006–2008*. *In press*.
- [11] Adler, M. & Ziglio, E., *Gazing into the Oracle: The Delphi Method and Its Application to Social Policy and Public Health*. Kingsley Publishers, London. 1995.
- [12] Martino, J. P., *Technological Forecasting for Decision Making*. McGraw-Hill, USA. 1993.
- [13] Van Gundy, A. B., *Techniques for Structured Problem Solving*. Van Nostrand Reinhold, New York. 1988.
- [14] Masser, I., Svidén, O., Wegener, M., *The Geography of Europe's Futures*. Belhaven Press, London. 1992.
- [15] Bell, W., *Foundations of Futures Studies*. Vol. 1 & Vol. 2. Transaction Publishers. 1997.

-
- [16] Mannermaa, M., Politics + Science = Futures Studies? In Dator, J. A. (ed.), *Advancing Futures*. Praeger. 2002.
- [17] See Pitkänen, O. 2006.
- [18] May, G. H., *The Future Is Ours: Foreseeing, Managing and Creating the Future*. Praeger. 1996.
- [19] Metsämuuronen, J., *Tutkimuksen tekemisen perusteet ihmistieteissä*. International Methelp, Helsinki. 2006.
- [20] We chose four global scenarios created by EVA (a Finnish policy and pro-market think tank) because their preparation process was broadly-based, they covered current topics and they had been tailored particularly to the Finnish environment. Alternatively we could have created the background scenarios by ourselves or by combining future visions of different actors. http://www.eva.fi/wp-content/uploads/files/2443_EVA_SCENARIOS_playing_fields_of_the_future.pdf (1 Feb 2011)
- [21] Johansson, S., Kaarin, P., Kankainen, A., Kantola, V., Runonen, M., Vaajakallio, K. & Kuikkaniemi K., *Cookbook: Extreme Service Design Methods*. 2010. <http://www.hiit.fi/files/admin/publications/other/eXdesignreseptikirja.pdf> (1 Feb 2011)
- [22] Kankainen, A., Vaajakallio, K., Kantola, V. & Mattelmäki, T., *Storytelling Group: A Co-Design Method for Service Design*. *Behavior & Information Technology*. *In press*.
- [23] See Johansson, S. et al. 2010.
- [24] Acquisti, A. & Grossklags, J., *Privacy and Rationality in Decision Making*. *IEEE Security and Privacy*, 3(1), pp. 26–33. 2005.
- [25] Järvinen, P., *Yksityisyys. Turvaa digitaalinen kotirauhasi*. WSOY, Jyväskylä. 2010.
- [26] More about Stuxnet, see <http://en.wikipedia.org/wiki/Stuxnet> (1 Feb 2011)
- [27] More about TiViT Cloud Software Program, see <http://www.cloudsoftwareprogram.org/> (1 Feb 2011)
- [28] Telcordia, *The Case for Deep Configuration Assessment of IP Networks*. White paper. http://www.telecomtv.com/docDownload.aspx?fileid=184a8c35-9f55-4779-aae6-4444a35ea12b/849179_deep-config-assessment.pdf&id=1342 (1 Feb 2011)
- [29] For a definition of Silver Bullet, see http://en.wikipedia.org/wiki/Silver_bullet (1 Feb 2011)
- [30] Wisniewski, C., *Smartphone Security: 50% of Devices Unprotected, 24% Unsure*. Article in *Naked Security* blog. 1.2.2010. <http://nakedsecurity.sophos.com/2010/02/01/smartphone-security-50-smartphones-unprotected-24-unsure/> (1 Feb 2011)
- [31] Thorsberg, F., *Half of U.S. Broadband Users Unprotected*. Article in *PCWorld*. 16.7.2001. http://www.pcworld.com/article/55154/half_of_us_broadband_users_unprotected.html (1 Feb 2011)
- [32] Locke, J., *Two Treatises of Government*. Cambridge University Press, Cambridge. 1960.
- [33] Westin, A., *Privacy and Freedom*. Atheneum, New York. 1967.
- [34] Rössler, B., *The Value of Privacy*. Polity, Cambridge. 2005.
- [35] Warren, S. & Brandeis, L., *The Right to Privacy*. *Harvard Law Review*, 4, pp. 193–220. 1890.

-
- [36] Etzioni, A., *The Limits of Privacy*. Basic Books, New York. 1999.
- [37] Etzioni, A. *The Common Good*. Polity Press. 2004.
- [38] Regan, P., *Legislating Privacy: Technology, Social Values and Public Policy*. University of North Carolina Press, Chapel Hill. 1995.
- [39] Bennett, C. J. & Raab, C. D., *The Governance of Privacy. Policy Instruments in Global Perspective*. MIT Press, Cambridge. 2006.
- [40] See Warren, S. & Brandeis, L. 1890.
- [41] Seipel, P., Alone No More. In Bakardjiev, A. et al. (eds), *Festschrift till Marianne Levin*. Norstedts Juridik, Stockholm. 2008.
- [42] See Wisniewski, C. 2010.
- [43] See Thorsberg, F. 2001.
- [44] Bejtlich, R., *The Tao of Network Security Monitoring: Beyond Intrusion Detection*. Addison-Wesley. 2004.
- [45] Gaudin, S., Intel Developing Security “Game-Changer”. Article in *Network World*. 26 Jan 2011. http://www.networkworld.com/news/2011/012611-intel-developing-security.html?source=NWWNLE_nlt_daily_am_2011-01-26 (1 Feb 2011)
- [46] Krauthem, J., Trusted Virtual Machine Identification (TVMI). Presentation in Xen Summit 2008 Boston, MA. 2008. <http://www.xen.org/files/xensummitboston08/IdentifyingTVM.pdf> (1 Feb 2011)
- [47] More about 2007 cyberattacks on Estonia, see http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia (1 Feb 2011)
- [48] More about Operation Payback, see http://en.wikipedia.org/wiki/Operation_Payback (1 Feb 2011)
- [49] Nygård, O., Myndighet slår larm om it-läckor. Article in *Svenska Dagbladet*. 2 Feb 2011. http://www.svd.se/naringsliv/nyheter/myndighet-slar-larm-om-it-lackor_5909395.svd (1 Feb 2011)
- [50] More about Evercookie, see <http://samy.pl/evercookie/> (1 Feb 2011)
- [51] More about Panopticlick, see <https://panopticlick.eff.org/> (1 Feb 2011)
- [52] Begtrup, G. E., Gannett, W. Yuzvinsky, T. D., Crespi, V. H. & Zettl, A., Nanoscale Reversible Mass Transport for Archival Memory. *Nano Letters*, 9(5), pp. 1835–1838. 2009. <http://www.physics.berkeley.edu/research/zettl/pdf/361.NanoLet.9-Begtrup.pdf> (1 Feb 2011)
- [53] Fitzpatrick, M., ‘Rosetta Stone’ Offers digital Lifeline. Article in *BBC News*. 29.7.2009. <http://news.bbc.co.uk/2/hi/technology/8172568.stm> (1 Feb 2011)
- [54] For more information, see, e.g., <http://www.sap.com/press.epx?pressid=14195> (1 Feb 2011)
- [55] More about functional requirements for URN, see <http://www.ietf.org/rfc/rfc1737.txt> (1 Feb 2011)
- [56] Celesti, A., Villari, M. & Puliafito, A., Design of a Cloud Naming Framework. *Proceedings of the 7th ACM International Conference on Computing Frontiers*. CF 2010, pp. 105–106. ACM, New York. 2010. <http://portal.acm.org/citation.cfm?id=1787275.1787305> (1 Feb 2011)

[57] For particular features of Symantec Endpoint Protection.cloud, see <http://www.symantec.com/business/endpoint-protection-cloud> (1 Feb 2011)

[58] Li, J. & Zhou, Z., Bohu Takes Aim at the Cloud. Article in Threat Research & Response Blog. Microsoft Malware Protection Center. 18 Jan 2011.
<http://blogs.technet.com/b/mmpe/archive/2011/01/19/bohu-takes-aim-at-the-cloud.aspx> (1 Feb 2011)

[59] Vuokola, J., Suomesta voi tulla datan paratiisi. Article in Tietoviikko. 30 Jan 2011.

[60] See Metsämuuronen, J. 2006.

[61] We chose four global scenarios created by EVA (a Finnish policy and pro-market think tank) because their preparation process was broadly-based, they covered current topics and they had been tailored particularly to the Finnish environment. Alternatively we could have created the background scenarios by ourselves or by combining future visions of different actors. http://www.eva.fi/wp-content/uploads/files/2443_EVA_SCENARIOS_playing_fields_of_the_future.pdf (1 Feb 2011)

[62] See Kankainen, A. et al. *In press*.

[63] See Johansson, S. et al. 2010.

[64] See Vuokola, J. 2011.