Ministry of Transport and Communications

Enhancing the usability and availability of information infrastructure essential for securing the vital functions of society

Final Report

Publications 3/2011

Ministry of Transport and Communications

Mission
The Ministry of Transport and Communications of Finland promotes national well-being and the efficient functioning of society by making sure that people, commerce and industry have access to high-quality, safe and reasonably priced transport and communications networks, and by furthering the competitiveness of transport and communications companies.

Vision
Finland is a global leader in transport and communications through its focus on quality, efficiency and international expertise.

Values
Courage, equity, cooperation

Ministry of Transport and Communications

Date
17.1.2011

Title of publication
Enhancing the usability and availability of information infrastructure essential for securing the vital functions of society. Final Report

Author(s)
Working group, Mr Kari T. Ojala, Ministry of Transport and Communications (chair), Mr Mats Kommonen, University of Turku (secretary)

Commissioned by, date
Ministry of Transport and Communications, 31 August 2008

Publication series and number	
Publications of the Ministry of Transport and Communications 3/2011	ISSN (online) 1795-4045 ISBN (online) 978-952-243-210-0 URN URN:ISBN:978-952-243-210-0 Reference number

Keywords
critical infrastructure, information security, YETTS

Contact person	Language of the report
Mr Kari T. Ojala	English

Other information
This report has also been published in Finnish (LVM:n julkaisuja 50/2009)

Abstract

Enhancing the usability and availability of ICT systems and services essential for securing the vital functions of society signifies an advancement of the information society at all levels, from businesses and organisations to citizens, and in all security situations from normal conditions to disturbances and emergencies.

The advancement of the information society increases productivity, competitiveness and social growth in all sectors, and increases the satisfaction of the individuals therein. Depending on the characteristics of the national economy, the information society represents an increase of nearly 40% in productivity.

The information society is affected by different developmental factors, trends and related threat scenarios, such as the growing importance of international cooperation and business networking, the rapid growth and innovation in cybersecurity, and the growing role and importance of ICT in the face of new global phenomena, such as emission reduction (green ICT).

The Internet has developed into a critical infrastructure. Internet components and services in Finland are an integral part of society. According to the working group, the Internet, as a neutral and critical networking platform, should be secured so that it provides sufficient and reliable services to the entire society. Different networks must be connected to form a single and adequately meshed communication infrastructure, thereby improving the reliability of services, especially in dispersed areas.

The security and availability of vital data pools and information must be guaranteed. For example, in order to prevent data leaks and denials of service, data pools should be widely decentralised. Critical ICT systems should be arranged so that it is possible to influence their management through the use of national regulations and decisions.

Society should promote protection interests in situations in which the market does not sufficiently encourage the private sector to invest in ICT protection to the level required by society.

CONTENTS

EXECUTIVE SUMMARY

Background and aims

The project entitled 'Enhancing the *usability and availability* of information infrastructure essential for securing the vital functions of society' (YKÄ)[1] is concerned with the wider adoption of information society technologies at all levels, from corporations and organisations down to individuals and citizens, and in all security situations, from normal circumstances to disruptive situations and emergency conditions.

The Finnish Government Decision on Safeguarding the Security of Supply (539/2008) identifies critical infrastructure and critical production. Critical infrastructure is a system which, together with its constituent processes, is essential for producing or supplying a certain service or product.

The aim of the YKÄ project has been to compile a clear status report on the *usability and availability* of information infrastructure essential for securing the vital functions of society at all levels in society and in all security situations, and to present solutions for the problem areas identified along with concrete proposals and measures, including indications of the parties responsible and the costs involved.

With this in mind, the report defines a general operating framework for information infrastructure essential for securing the vital functions of society and which can be used for analysing critical information infrastructure. The framework can be used to determine the ICT functions and components that are critical for the underlying structure of these vital functions, as well as industry and sector-specific critical ICT functions and components.

The report analyses at a general level the critical nature and current status of information infrastructure, also in relation to contingency preparations, and considers whether usability and availability are supported sufficiently by the legislation. It also looks at the adequacy of current measures for protecting critical infrastructure. The report presents a number of potential problem areas and vulnerabilities concerning critical information infrastructure, and outlines possible solutions and proposals for improvement.

The YKÄ working group has conducted its work in close collaboration with other working groups charged with developing security projects within the public sector, and has consequently sought to avoid duplication of effort.

Development trends and threat scenarios

Progress towards information society goals is affected by the nature of developments that take shape and by the trends and threat scenarios emerging. These can include the growing significance of international cooperation and networks, the rapid increase in cyber crime and its changing nature, and the role and importance of information infrastructure as new global phenomena emerge (e.g. emissions reduction/green ICT).

[1] The project entitled 'Enhancing the *usability and availability* of information infrastructure essential for securing the vital functions of society' is also referred to in this report by its Finnish acronym, YKÄ. The 'information infrastructure' in the project name refers collectively to all information and communication technology (ICT) systems, services and networks.

The wider adoption of information society technologies will boost the productivity and competitiveness of the national economy and growth and development in all segments of society, and will increase the satisfaction of the individuals therein. Information society technologies have in fact accounted for as much as almost 40% of productivity growth, though the figure varies according to the particular characteristics of the national economy in question.

In businesses, the competitive pressures of the market economy brought by networking appear to have reduced the level of contingency preparations to a minimum. Competition has also led to companies specialising further, and thus to the enlargement of value networks and lengthening of value chains, which exacerbates the vulnerability of the system in a crisis situation. As no single participant can alone achieve a significant benefit from contingency preparations, common strategies are needed.

A key share of the services used and needed by businesses and citizens rely on the Internet, which has now become a critical infrastructure. In 2008, the World Economic Forum estimated that over the next 10 years the probability of a major breakdown in information infrastructures critical to society is 10-20%. This could lead to costs of as much as EUR 170 billion globally.

Critical information infrastructure and the relationship between the YKÄ work and contingency preparations

The work under the YKÄ project has a direct impact on contingency preparations because information society functions must remain usable and available in all security situations. Contingency preparations mean analysing threat scenarios and securing operations even in normal circumstances.

For businesses, contingency preparations focus on the fundamentals for business operation, agreements made with customers, and risk management in these areas. To the extent that this falls short of the needs of society at large, additional responsibilities for contingency preparation are specified through legislative obligations and other special measures. In certain areas the role of public authorities is restricted to guidance, and the active role is given to a private company. The statutory obligations for contingency preparation must not be allowed to disrupt the operation of the market or distort equitable competitive conditions. Particular attention must be given to Finnish competition legislation and that of the European Union. Finland's National Emergency Supply Organisation has different sectors and pools in which various companies and business organisations take part in contingency planning on a contractual basis.

Critical information infrastructures are in many cases global and are closely interconnected. They are also mutually dependent on other infrastructures, which means that their information security and resilience cannot be guaranteed on a purely national basis or without coordination.

On 30 March 2009, the European Commission published a Communication laying out plans for immediate action to strengthen security and resilience in critical information infrastructures. Recent examples of the situations referred to in the Communication include the extensive cyber attacks in Estonia in 2007 and the cutting of undersea cables.

Conclusions

The conclusions and measures set out below are not in order of importance.

- Finland's telecommunications legislation, statute monitoring, and issuance of standards regarding information society issues, and the structure, protection and operation of networks and services, are of a good standard internationally in terms of **usability and availability**. Specifications, security classifications and other standards are of a high quality. Continuous development is nevertheless essential.

- **Ensuring the usability and availability** of communications and telecommunications systems is, for the most part, in good shape in terms of administration, organisation, legislation and products/services.

- There is room for further development in the **usability and availability** of information infrastructure. The information system and service sectors do not, however, have comprehensive standards-based regulatory mechanisms, such as those in the electronic communications field.

- The **usability and availability** of information infrastructure is planned, implemented and managed as part of business processes. Purely technical solutions and standards are not sufficient.

- In Finland, ICT contingency preparations cover not only emergency conditions but also disruptions under normal circumstances, through sectoral legislation and with the aid of commercial service-level requirements.

- The joint working on contingency preparations between the public and private sectors functions well and there is an established practice regarding the distribution of costs.

- The Internet has become critical infrastructure. Services for businesses and citizens via the Internet have become vital. The elements of the Internet located in Finland and the Internet services available in Finland are an integral part of society's fabric today.

- A characteristic of recent developments in ICT services has been the globalisation of supply and the outsourcing of functions, possible side-effects of which could cause serious market disruptions and problems with the accessibility of ICT services. Globalisation, economic swings and future threat scenarios involving networks have led to attempts to use national resources to ensure critical ICT functions.

- The market does not always encourage private operators to invest in the protection of critical information infrastructure to a standard required for society's contingency preparations. This was also concluded by the European Commission.

- The **usability and availability** of ICT services cannot be guaranteed in all cases, and this will affect society's contingency preparations. An ICT company and a critical subcontractor company serving it could, for instance, dismiss a high proportion of their staff, discontinue certain services or even go bankrupt.

- Today's tough competitive environment leaves few spare resources in a company, and this could weaken its risk-bearing capacity and thus make the company's operations more vulnerable to various threats in a crisis situation.

- As a consequence of international cooperation, new operating models have been formed from complex value networks. An organisation's operating processes may be partially or wholly located outside the country's borders, making it more difficult to control the security and reliability of operations.

- Besides conventional telecommunications, information society networks include communications traffic from various newer sources too, including the entertainment industry and pay-to-access services. Control of these is based on different needs than that for ICT functions (e.g. filtering, obligation to store). As a consequence, the usability and availability requirements for networks and services can be conflicting (quality classification, pricing).

- The report does not take a view on the ownership of critical information infrastructures or their components.

Measures

- ICT business operations and markets, especially telecommunications networks and services, should only be subject to guidance and control to the extent essential for ensuring diverse and sufficient markets and services. The guidance mechanisms should consist of standards, operating licence conditions and funding. Competition will increase the alternatives, also in regard to usability and availability.

- Public sector involvement is important for establishing a protection body for critical information infrastructure for situations in which the market does not offer sufficient incentive for private operators to invest in protecting critical information infrastructure to a standard required for contingency preparations in society at large.

- The functioning of the Internet as a neutral, evolving and critical data transfer platform must be secured with the aid of international collaboration, regulation and technical solutions, to ensure that it serves society at large in an adequate and reliable manner.

- Attention must be paid to ensuring that the development of service structures at EU level and the measures to secure vital functions domestically are in harmony with each other and mutually compatible. One example is the way in which payment transactions have developed in the financial sector; another is the development of shared structures among different operators (e.g. energy, telecommunications). Further development should be facilitated by exporting good solutions from Finland to the EU, in addition to Finland adopting solutions from the EU.

- Verification of information assets and data that are vital to society and accessibility to these assets and data must be guaranteed in all security situations. In preventing information leaks and denial-of-service attacks, for example, it is good if information assets are widely dispersed. Managing information systems critical to the functioning of society must be arranged in such a way that it can be influenced through national legislation and decisions.

- Enhancing usability and availability requires investment in strengthening expertise and in training. Maintaining Finland's critical information infrastructure and

drafting procurement and operating agreements of a high standard will require a strengthening of national expertise in normal circumstances. Improving the level of expertise will also require additional investment in R&D projects in this field, both within the public sector and in owner organisations and organisations with responsibilities.

- In maintaining the security of supply, the role of ICT activities and logistics is a strategic and growing one. The role of the information society in ensuring the vital functions of society in normal circumstances has also expanded and is of growing significance. The role of the National Emergency Supply Organisation should be further strengthened and expanded in regard to ICT.

- The working group feels it important that the YKÄ work be developed further and preparations made regarding the shape this will take. It also proposes that the rights to this preparatory work should lie with the National Emergency Supply Organisation's information society cluster. The preparatory work should also include R&D activities in YKÄ field. Sufficient resources must be allocated for further developing the YKÄ work.

- The working group has also set out a number of technology and service-related proposals for measures to improve the usability and availability of critical information infrastructure. These are presented in the report, along with justifications (section 9).

- There must be a functioning, reliable, simple and sufficiently widely accepted identity recognition procedure in use within the information society. The working group proposes that identity management should form a separate concept in the field of critical infrastructure. To develop this concept, an investigation should be conducted into whether it can be linked up as part of some existing and sufficiently broad identity management development project.

1 INTRODUCTION

1.1 Information society goals and the YKÄ project

The project entitled 'Enhancing the **usability and availability** of information infrastructure essential for securing the vital functions of society' (YKÄ) focuses on the challenges in this area for society as a whole (businesses, organisations, citizens) and in all security situations, namely normal circumstances, disruptive situations, emergency conditions. The importance of the YKÄ work and the general aims for it are set out in the Ubiquitous Information Society Programme run by the Ministry of Transport and Communications.

The broader mission underlying the YKÄ project is based on the principle that the **wider adoption** of information society technologies will have a positive impact on the following in all sectors of society as a whole:

- productivity in the national economy
- competitiveness
- growth and development in society, and
- people's comfort and convenience, and equality among citizens.

The impact of different developments, trends and threat scenarios will be important in this, including

- the growing importance of international collaboration and networking
- rapid growth in cyber crime and a shift in its character
- the role and importance of information infrastructure in the face of new global phenomena (e.g. emissions reduction (green ICT), emergence from economic downturn).

In terms of information society goals and gaining the trust of citizens, key roles are occupied by the Strategy for Securing the Functions Vital to Society (known by its Finnish acronym, YETTS), society's critical infrastructures, and the implementation of Internal Security Programme objectives. Greater focus must be attached to contingency preparations for threat scenarios concerning different programmes.

Making contingency preparations under normal circumstances for dealing with both disruptive situations and emergency conditions will become increasingly important. Society is completely reliant on electrical power and on ICT, and these go hand in hand everywhere within the information society.

1.1.1 Usability and availability

The *usability and availability* of information infrastructure critical to society are defined in the accompanying box[2]. In this report, usability and availability refer to both convenience of use and accessibility. Today's information society has become completely dependent on the 24/7 operation of information networks.

Information security is also a key factor when considering usability, availability and accessibility. A good standard of information security means a situation in which threats concerning the reliability, integrity, usability and availability of data, systems, services and telecommunications do not pose a significant risk.

[2] http://fi.wikipedia.org/wiki/Käytettävyys. (In Finnish, on usability and availability)

Usability and availability are defined below.

Usability
ISO 9241-11 defines usability as the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. Effectiveness refers to how accurately and comprehensively users can achieve their objectives. Efficiency refers to the level of resource use in achieving the objectives. Satisfaction refers to user satisfaction regarding use of the device or system, the ease of interaction and the outcome.

Availability
In production environments, availability generally refers to the functioning and performance of technical systems. Another commonly used term for this is ***accessibility***. Accessibility refers to how great a proportion of the day the system is in operation and accessible by users. For example, the accessibility of a system may be 99%, which means that it has been functioning 99% of the time.

Accessibility as a planning goal
At the planning stage of online services the aim is to identify the parameters and requirements set by users and by the purposes and terminal devices in question. Identification of user needs could follow user-oriented planning principles. Taking accessibility into account as early as the planning stage will guarantee a better end result than 'fixing' an existing service to make it accessible.

Accessibility as a feature of the service
Accessibility can also be seen as a feature of an online service. Various lists of recommended features for online services have been compiled, e.g. W3C's checklist 'Web Content Accessibility Guidelines 1.0'. Such lists can also be used in evaluating the accessibility of an online service.

Accessibility and usability/availability
Drawing a line between problems of usability/availability and of accessibility is difficult.

1.2 Significance of information society technologies for productivity

The wider adoption of information society technologies (Figure 1.1) will boost the productivity and competitiveness of the national economy and growth and development in all segments of society, and will increase the satisfaction of the individuals therein. Information society technologies have in fact accounted for as much as almost 40% of productivity growth, though the figure varies cording to the particular characteristics of the national economy in question, such as total population and location in relation to markets and partners[3].

1.2.1 Well-founded trust

The wider adoption of information society technologies can only occur if all the parties involved feel that there is sufficiently well-founded trust in the information society and its services. Each party has its own perspective, whether a public sector organisation, businesses or citizens.

The different aspects involved include safe Internet access, convenience and accessibility of electronic services, consumer protection, legality of content, information security and the universal usability and availability (accessibility) of basic services. Improving the position of consumers requires a responsible approach from all concerned, including consumers themselves.

[3] Eurostat, theme: Science and Technology/Information Society, http://epp.eurostat.ec.europa.eu.

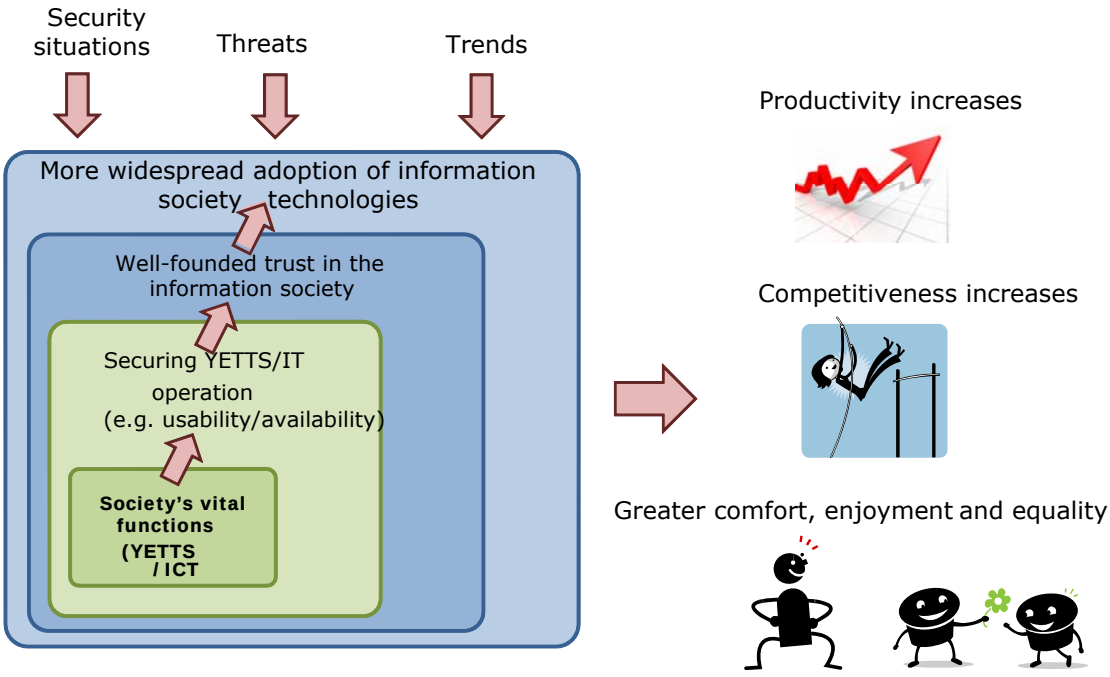


Figure 1.1 The wider adoption of information society technologies will boost the productivity and competitiveness of the national economy, make people's lives more comfortable and enjoyable and improve equality among citizens.

1.2.2 Ensuring operations

The prerequisites for trust are built on the following: ensuring the operation of information infrastructure critical to society (by guaranteeing usability and availability, at a high standard of service); information security measures; intervening in cases of harmful and unlawful content; investing in CERT (Computer Emergency Response Team) activities; securing online banking; individual protection projects; making contingency preparations for cyber attacks and malware, etc.

Ensuring the operation of information infrastructure critical to society requires the identification of processes, systems and their components, a realistic survey of threats and risks, and the outlining of solutions. This is especially important at the infrastructure level where impacts are both deep and wide.

In component identification it is important to note the individual functions and operators as elements of a process. This allows information security, for instance, to be treated as part of business processes.

In surveying threats and risks, it should be possible to take realistic account of their probabilities and of the interrelationships of risks and threats.

Finally, outlined solutions should focus on ensuring operating processes and on the most probable and most serious threats and risks, and should take a view on ownership, solution methodologies, resources and timetables. These are extremely challenging objectives.

1.3 Society's reliance on electricity

Society is almost totally dependent on electricity. Disruptions in power distribution can paralyze everyday functions. Water distribution, wastewater operations, fuel distribution, operation of shops, bank cash dispensers, telecommunications and heating all rely on electricity. They would come to a standstill in the event of a power outage due to a storm or technical fault. The implications of power outages for society's vital functions have been studied in a recent Ministry of Defence publication[4].

Power distribution and telecommunications are in a critical symbiotic relationship (see Appendix 1[5], not for publication, section 24(1)(8-9) of the Act on the Openness of Government Activities).

1.4 Eco-efficient information society

The research company Gartner estimated that the ICT industry produces two per cent of the world's carbon dioxide emissions.[6,7] This is about the same as the aviation sector. Gartner believes this is an unsustainable situation, despite the environmental benefits of ICT overall. ICT emissions are forecast to grow and even to double in the next few years.

1.4.1 Great potential for ICT sector

The ICT sector has great potential to contribute to a reduction in emissions in those sectors of society that produce the remaining 98 per cent of carbon dioxide emissions. ICT technology could reduce Europe's total energy consumption by as much as 15 per cent by the year 2020.[8] Estimates indicate that unless ICT is harnessed to improve energy efficiency, it will not even be possible to achieve the emissions and energy efficiency targets set for 2020 by the Council of the European Union.

The ICT sector cannot of course alone be responsible for achievement of the energy efficiency targets, but it does have a uniquely important role in accelerating the type of structural change that would produce improved energy efficiency in different areas of the economy. At stake is a structural change in the ICT sector and in other sectors towards better utilisation of the added value afforded by technology, such as more efficient management of industrial and service processes, more intelligent ICT-controlled transport and logistics, and electronic transactions and the wider adoption of information society technologies in other areas.

It is essential to move towards a 'ubiquitous information society' in order to establish a framework in which ICT can be harnessed to improve energy efficiency and thus to mitigate climate change. Network infrastructure should be of a high quality and should meet the rapidly growing telecommunications needs, thereby enhancing trust in information society services. Advancing this is what the YKÄ project is about.

---

[4] Long-duration power outages and securing vital functions of society, Ministry of Defence, 2009. (In Finnish)
[5] The appendices referred to in this report are classified.
[6] Gartner: ICT emissions match those of aviation, Digitoday, 27 April 2007. (In Finnish)
[7] http://www.vihreaict.fi/fi/fi_6.html.
[8] Towards an ecologically efficient information society, Minister of Communications Suvi Lindén, ICT and environment seminar, 1 April 2009.

1.5 Development of information society at international level

1.5.1 Global risks

The world economy and progress towards information society goals are affected by various global trends, each with its own risk functions. Moreover, circumstances can change quickly, and risks with them. Global risks have an impact on the national situation via the global economy and via factors such as the outsourcing of operating functions by businesses, and on the information society at national level via the Strategy for Securing the Functions Vital to Society (YETTS) and the critical infrastructure (CI) and critical information infrastructure (CII).

Current global trends of greatest importance, according to the World Economic Forum[9], include systematic financial risks, food security, 'hyper-optimisation', the vulnerability of distribution channels, and the role of energy:

- Systematic financial risks give rise to financial risks throughout the entire financial system, which is seen in rapid asset depreciation and reduced economic activity. Financial systems in these circumstances are unstable, deepening the crisis of confidence in the financial sector as a whole.

- Food security is defined as being a situation in which all people, at all times, have physical and economic access to sufficient, safe and nutritious food.[10] As with energy security, food security includes not only the satisfying of a physical need but also the concept of economic access.

- Hyper-optimisation and the vulnerability of distribution channels are an unseen global risk. Economic globalisation has altered the operating structures of both private and public sector organisations. Outsourcing, especially in production but also increasingly in basic business services, is a fundamental force in global wealth creation, where limited global resources are allocated to businesses and territorial areas that produce the greatest relative competitive advantage. A more globally integrated economy is nevertheless more vulnerable to distribution channel disruptions. Securing the economy is no longer dependent on its internal functioning.

- Energy and the global risk: interconnected risks, separate incentives. Energy is a key factor in the global economy, but securing the energy supply and ensuring its sustainable delivery are becoming more challenging all the time. In the face of a long list of global risks (such as climate change, economic and other geopolitical risks), current and future political decisions on energy will inevitably reshape the entire global risk landscape. Incentives to reform the global energy economy in a way that would reduce global risks are not in evidence, however.

Global risks are often interconnected in chains, especially in regard to energy transmission and information infrastructures. Where risks have become reality, the loss and damage caused has normally been measured in financial terms or as loss of human life.

1.5.2 Changing nature of crime

Organised and serious crime, cyber crime and terrorism are all examined in Finland's Strategy for Securing the Functions Vital to Society (YETTS), and are be-

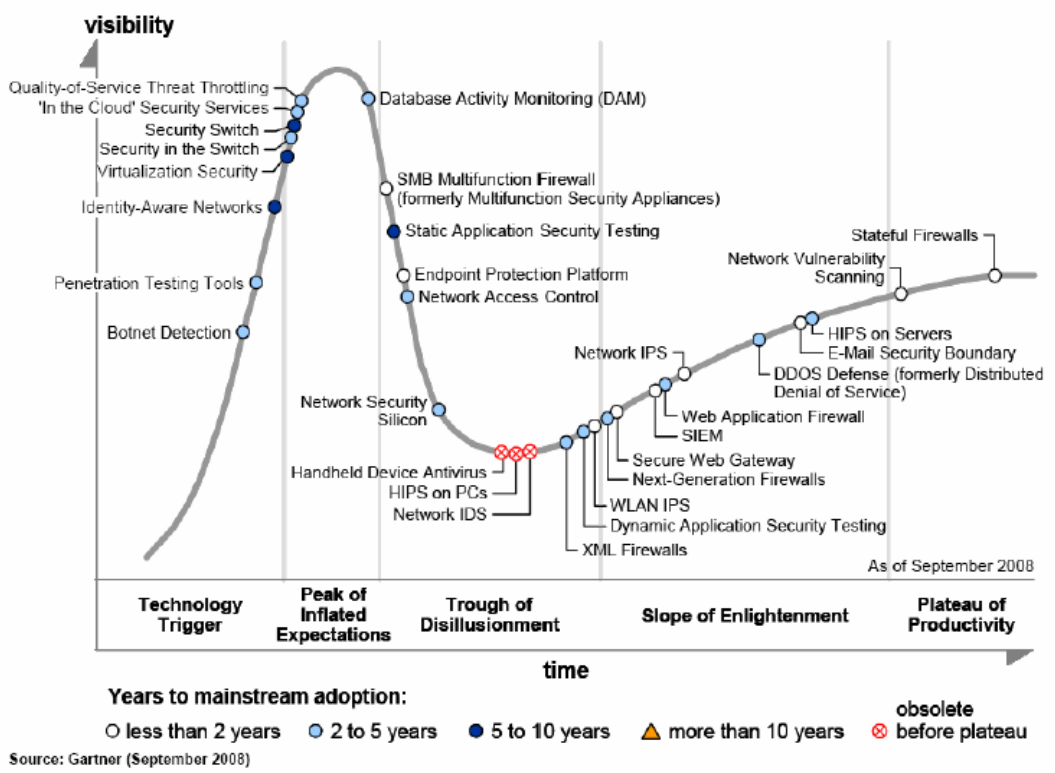
[9] World Economic Forum, Global Risks 2008.
[10] Food and Agriculture Organization (FAO).

ing tackled for instance with the aid of the Internal Security Programme. Information networks and critical infrastructures allow the emergence of new forms of crime, ensuring that this is an extensive theme and one affecting all areas.

1.5.2.1 Cyber crime

One of the fastest spreading phenomena in the changing nature of crime is cyber crime, a more serious side of which is cyber terrorism. In cyber terrorism terrorists use information networks (mainly the Internet) for their attacks and for other activities supporting terrorism.

Combating cyber crime has given rise to numerous different protective procedures and technologies. Figure 1.2 shows a Gartner hype cycle[11] for infrastructure protection (September 2008). The problem is that protective procedures are fragmented, incompatible with each other and separated from business processes. In many cases, protective procedures have even led to new information security problems.



DAM	Database Activity Monitoring	IPS	Intrusion Prevention System
DDoS	Distributed Denial of Service	SIEM	Security Information and Event Management
HIPS	Host-based Intrusion Prevention System	SMB	Server Message Block
IDS	Intrusion Detection System	XML	eXtensible Markup Language

Figure 1.2 Hype cycle, infrastructure protection 2008 (Gartner).[12]

1.5.3 Critical Information Infrastructure Protection (CIIP)

On 30 March 2009 the Commission of the European Communities issued a Communication on critical information infrastructure protection (CIIP)[13,14]. Politics will deter-

[11] Gartner's hype cycle, http://en.wikipedia.org/wiki/Hype_cycle
[12] Gartner, 2008.

mine the plans for immediate action to strengthen the security and resilience of critical infrastructures. Recent examples include the series of cyber attacks on Estonia in spring 2007, which brought banks, police stations and government offices to a standstill for a week, and the cutting of undersea cables in 2008.

The World Economic Forum estimated in 2008 that over the next 10 years the probability of a major breakdown in information infrastructures critical to society is 10-20%. A disruptive situation could lead to costs of as much as EUR 170 billion globally.[15]

1.5.4 Unpredictable ICT ecosystem[16]

The number of components and their interdependencies in the Internet's technical and financial ecosystem have grown so great that it is better to think of the entirety as being a complex system rather than just a machine. This system is not planned but is instead the outcome of its component parts and their interactions. A disruption in one part of the system can lead to changes elsewhere that are hard to predict.

Conventional risk management, i.e. focusing on identifying and eliminating hazards, is no longer applicable. Contingency preparations must be made to deal with problems (resilience and continuity planning). In parallel with resilience, it would also be necessary to split up an overall problem into controllable functioning parts, and to operate within these ("new sustainable economy").[17]

1.6 Role of contingency preparations: preventing realisation of threats in normal circumstances

The YKÄ work is directly related to contingency preparations, because information society functions must remain available in all security situations. Contingency preparations mean analysing the threat scenarios and ensuring operations under normal circumstances.

1.6.1 Integrated contingency preparation system

Finland has a contingency preparation system based on integrated contingency planning and on stockpiling critical production inputs. ICT plays a central and growing role in this integrated planning. Critical infrastructures, and through them society's vital functions, are dependent on ICT systems and on electrical power.

Contingency preparations are directed by the Government and via the Government Decision on Safeguarding the Security of Supply (539/2008), the aim being that Finns should be able to cope in different disruptive situations and emergency conditions affecting society. In 2006, the Government approved a Strategy for Securing the Functions Vital to Society (YETTS), which is used to mesh together the contin-

---

[13] http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm
[14] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience", Brussels 30 March 2009, COM/2009/0149 final.
[15] Global Risks 2008.
[16] Prof. Heikki Hämmäinen, Ensuring operation of information networks, Tiedosta journal, Finnish Information Society Development Centre, 9 March 2009. (In Finnish)
[17] Leppävuori, 2008.

gency preparations of the different administrative branches of government. Each ministry controls and monitors its own contingency preparations.

Contingency preparations by businesses are based on business principles, agreements made with customers, and risk management of their operations. The financial sector also has obligations set out by law to make contingency preparations for disruptions.

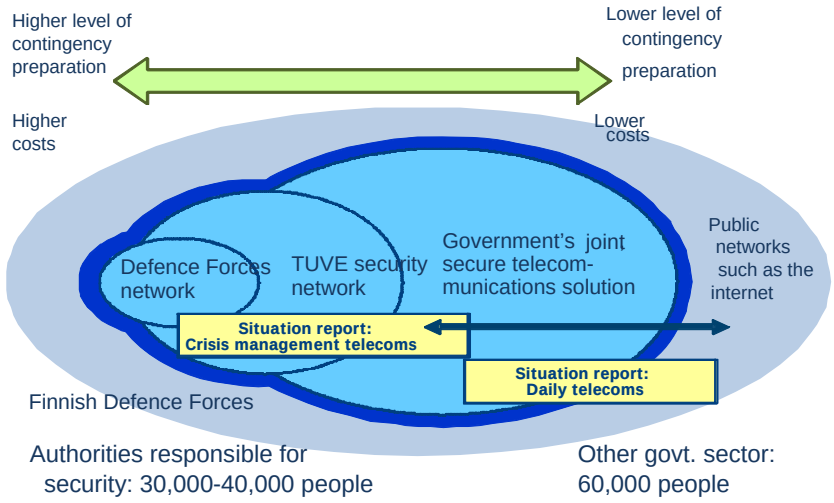
Non-governmental organisations (NGOs) have an important role in enhancing security at a practical level. Through their work they also add to society's resilience in the face of a crisis.

1.6.2 Contingency preparations against threats are made in normal circumstances

Even with large-scale contingency preparations it is not possible to foresee and prevent all threats. Unexpected and sudden events that also require leadership and information provision beyond normal arrangements are known as special situations. A special situation can arise during normal circumstances, disruptive situations or emergency conditions.

1.6.3 Situation report assembled via public networks

Figure 1.3 shows Finland's public sector telecommunications networks and their general level of preparedness. The Government security services unit puts together a national situation report using information from different ministries and other specified organisations. Public networks (Internet, mobile, corporate networks, other) are very important in the assembly of a daily situation report. The YKÄ work has a key role in this in developing the availability of critical ICT services.



Source: Ministry of Finance

Figure 1.3 Government telecommunications networks.

1.7 Aims of report

The aim of the YKÄ project has been to obtain a picture of the *usability and availability* of information infrastructure essential for securing the vital functions of society at all levels in society (central government, public administration, information

society in general) and in all security situations (normal circumstances, disruptive situations, emergency conditions). Solutions have also been sought for the problem situations identified, along with concrete proposals and measures, including indications of the parties responsible and the cost implications.

1.7.1 Analysis framework

With these aims in mind, this report defines a general operating framework for information infrastructure essential for securing the vital functions of society and which can be used for analysing critical information infrastructure. The framework can be used to determine the ICT functions and components that are critical to the underlying structure of vital functions, as well as the industry- and sector-specific critical ICT functions and components that overlay this.

The report analyses at a general level the critical nature and current status of information infrastructure, also in relation to contingency preparations, and considers whether usability and availability are supported sufficiently by the legislation. The YKÄ working group has conducted its work in close collaboration with other working groups charged with developing security projects within the public sector, and has consequently sought to avoid duplication of effort.

The report also looks at the adequacy of current measures for protecting critical infrastructure. The report presents a number of specific potential problem areas and vulnerabilities concerning critical information infrastructure, and outlines possible solutions and proposals for improvement. This also concerns the role of energy supply for telecommunications networks and the potential problems areas in this.

1.7.2 Usability and availability of critical infrastructures

The threats affecting vital functions and the usability and availability of information infrastructure are examined from two main perspectives, critical infrastructure protection (CIP) and critical information infrastructure protection (CIIP), at both the process and structural levels. CIP aims at securing continuity in business processes and structures in all critical infrastructures. CIIP aims at securing and optimising the usability and availability of business processes and structures in critical information infrastructure.

The analysis framework established in the report allows both CIP and CIIP needs to be examined at a general level and the impacts analysed in regard to the usability and availability of society's critical ICT functions and systems, and in regard to business.

1.7.3 YKÄ project in context

The importance and general aims of enhancing the **usability and availability** of information infrastructure essential for securing the vital functions of society (the YKÄ project) are specified in the **Ubiquitous Information Society Programme** run by the Ministry of Transport and Communications.

The YKÄ project has many different dimensions. The work of the project touches on a number of different public sector strategies, programmes and projects (Figure 1.4). Participation in the EU's CIP and CIIP work, and influencing the course of this work, is also an important element of the YKÄ project. New information society phenomena, such as online communities, are also taken into account.

Occupying a key role in the activities covered by the YKÄ project is the private sector and the users of its services (public administration, businesses, citizens), together with their agreements and development projects.

The YKÄ work has a close relationship with the VARE project on the government's ICT contingency preparations and with the Internal Security Programme. Both the YKÄ and VARE projects look at the same challenges and threats, from the perspectives of service providers and users. The service providers are mainly the same private sector operators. In the implementation of the Internal Security Programme, trust in information society services, accessibility of these services, and their usability and availability are of primary importance.

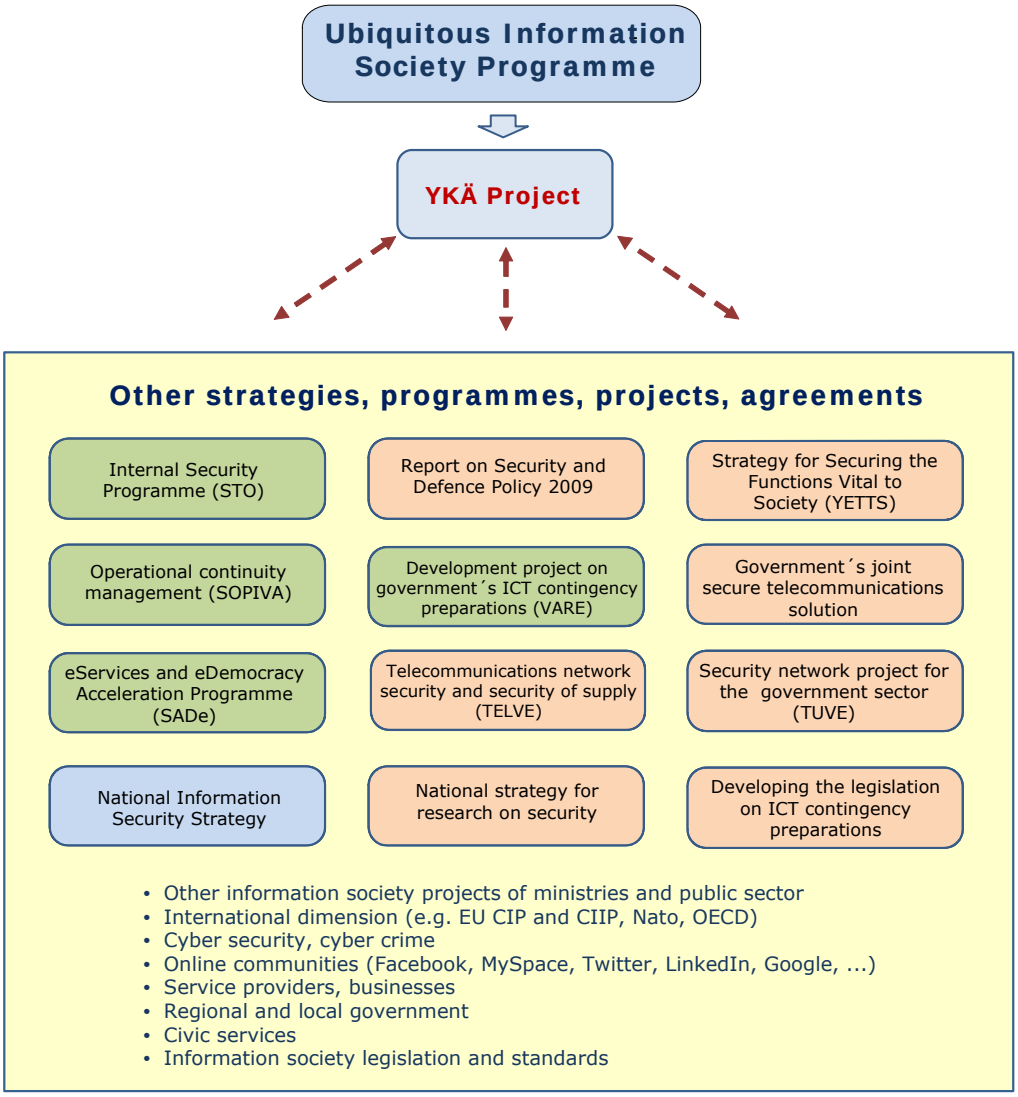


Figure 1.4 The YKÄ project and its wider context.

2 OPERATING ENVIRONMENT

2.1 General situation

2.1.1 Society's vital functions

The Strategy for Securing the Functions Vital to Society (YETTS)[18] specifies the following seven (7) functions as being vital to society: *management of government affairs; international activity; national military defence; internal security; functioning of the economy and infrastructure; the population's income security and capability to function; and psychological crisis tolerance.*

2.1.2 Critical sectors

Activities for ensuring the security of supply in Finland cover seven critical sectors (infrastructures) [19]:

- information society
- energy supply
- finance services
- transport and logistics
- health services
- critical industry and
- food supply.

These critical infrastructures are composed of structures and functions that are essential for the uninterrupted functioning of society. Critical infrastructures include both physical establishments and structures and electronic functions and services. Securing these infrastructures means identifying and securing the individual critical points while also constantly ensuring the operation of the entire entity.

2.1.3 Integrated contingency preparations

Finland has a contingency preparation system that forms an integral part of the information society and is based on stockpiling critical production inputs and contingency planning. All critical infrastructures and thus society's vital functions are reliant on ICT systems and on electrical power supply.

The importance of ICT in critical sectors is examined briefly in Appendix 1 in the light of a number of market and volume indicators.

Securing society's vital functions and maintaining and developing the security of supply both involve very close partnership between the public and private sectors. At the government level there are approximately 2,000 critical businesses, and these have a great many network partners. The partnership with the private sector is coordinated by the National Emergency Supply Agency.

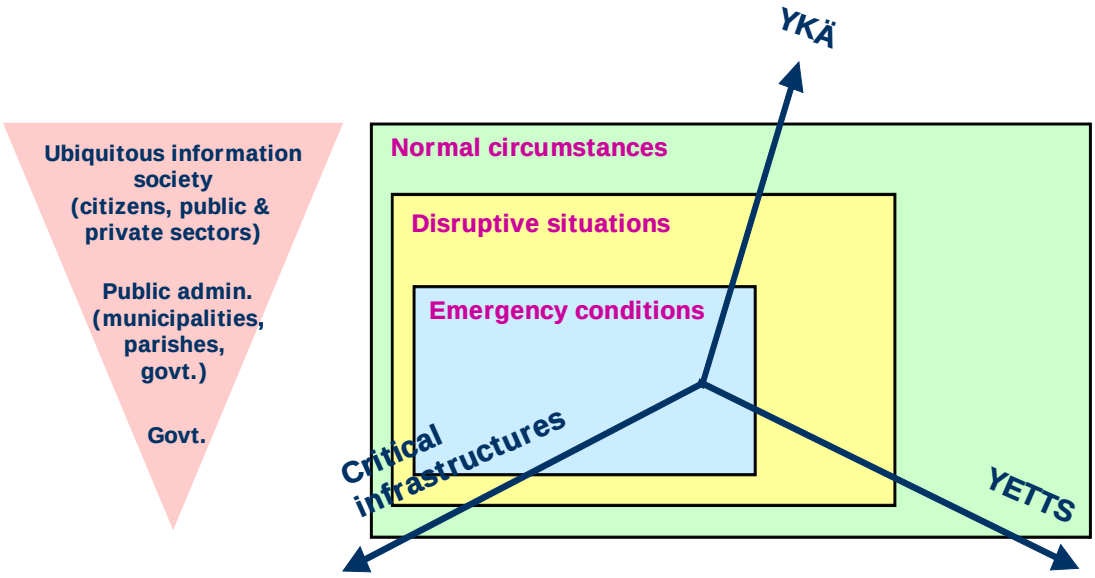
2.1.4 YKÄ project

Figure 2.1 shows the relationship between the YKÄ project ('Enhancing the usability and availability of information infrastructure essential for securing the vital func-

[18] Strategy for Securing the Functions Vital to Society, government resolution, 23 November 2006.
[19] http://www.huoltovarmuus.fi/.

tions of society') and YETTS (the Strategy for Securing the Functions Vital to Society), as well as critical sectors in the 'ubiquitous information society'.

The YKÄ work extends across all administrative branches (in the ICT sector) and covers the full spectrum from central government needs to those of businesses and citizens in an advanced information society. The YKÄ project also covers all security situations (normal circumstances, disruptive situations, emergency conditions).



YETTS	Critical sectors	YKÄ
• Management of government affairs • International activity • National military defence • Internal security • Functioning of the economy and infrastructure • The population's income security and capability to function • Psychological crisis tolerance	• Energy supply • ICT systems • Food supply • Health services • Banking and financial services • Transport and logistics • Critical industry	• More widespread adoption of information society technologies • Well-founded trust (Usability, availability, accessibility, service level, information security, ...) • Ensuring ICT operation • Critical information infrastructure (ICT/CI) • Time span • Role in contingency preparations

Figure 2.1 Role of the YKÄ project in relation to the Strategy for Securing the Functions Vital to Society (YETTS) and critical sectors in the 'ubiquitous information society'.

2.2 Public sector guidance mechanisms, programmes and projects relevant to the YKÄ project

Due to the multifaceted nature of the YKÄ project, reference is made to it and frameworks created for it in many public sector organisations, programmes and projects, ranging from the Government Report on Security and Defence Policy to information security strategies for the government and for citizens, and ICT standards.

2.2.1 Public sector guidance mechanisms

Public sector strategies, programmes and projects are guided by the Government Programme, legislation and legal praxis, standards and guidelines, operating licences, technical instructions and agreements and other obligations. The obligation of public authorities to make contingency preparations for emergency conditions is set out in the Emergency Powers Act.

The Government, state administrative authorities, independent state institutions governed by public law, other state authorities, state-owned enterprises, municipalities, joint municipal authorities and other groupings of municipalities all have an obligation to verify that their duties are managed as well as possible in different situations.

Some of the strategies, such as the Strategy for Securing the Functions Vital to Society (YETTS), serve mainly as guidance for public administration. YETTS was not designed with the private sector in mind and does not include financial and investment decisions or profit expectations. It also lacks guidance tools.

2.2.2 Strategies, programmes and projects

The YKÄ project takes into account the following strategies, programmes and projects. The Ubiquitous Information Society Programme is listed first because it establishes the needs and framework for the work covered by the YKÄ project.

- Ubiquitous Information Society Programme
- eServices and eDemocracy Acceleration Programme (SADe)
- National Information Security Strategy
- Strategy for Securing the Functions Vital to Society (YETTS)
- Internal Security Programme (STO)
- Development project on government ICT contingency preparations (VARE)
- Operational continuity management (SOPIVA)
- Telecommunications network security and security of supply (TELVE)
- Government's joint secure telecommunications solution
- Security network project for the government sector (TUVE)
- Government Report on Security and Defence Policy 2009
- Developing the legislation on ICT contingency preparations
- National strategy for research on security.

2.2.3 Organisations responsible

The work covered by the YKÄ project is being carried out by e.g.

- Finnish Communications Regulatory Authority (FICORA)
- Government IT Shared Service Centre
- National Emergency Supply Organisation (incl. the National Emergency Supply Agency)
- Government Information Security Management Board (VAHTI)
- Advisory Committee for Data Administration in Public Administration (JUHTA)
- Organisations with administrative responsibilities in this field (e.g. Financial Supervisory Authority)
- Ownership steering bodies (Ministry of Finance's ownership steering unit, named Solidium)
- Private sector.

2.2.4 Ministries

Even where responsibilities regarding implementation are delegated to other organisations, the statutory responsibilities designated to the different ministries concerning the YKÄ work remain intact. These responsibilities are set out in Appendix 2.

Appendix 2 contains a more extensive summary of strategies, programmes and projects together with the organisations responsible in each case. The guidance mechanisms are presented in more detail under each strategy or project. Appendix 3 contains a summary of national R&D activities in the YKÄ field, international CII and CIIP projects and the standards and requirements in the sector.

2.3 Protecting Europe's critical infrastructures

Finland has a long history of protecting its critical infrastructures and also has successful partnership models for this. This has allowed it to play an active role in the collaboration set up by the European Union concerning critical infrastructure protection. Finland has already gone a long way towards implementing the measures outlined in the EU's programme.

2.3.1 ECI

Critical infrastructures with cross-border impacts have been identified and designated as European critical infrastructures (ECIs). These ECIs were listed in a Green Paper (November 2005) presented by the Commission of the European Communities, and are shown in Appendix 2 with their associated products and services.

Since the ECIs extend across national boundaries, any survey of their weaknesses, vulnerabilities and security deficiencies should be based on a common, EU-wide methodology that would not only complement the national protection programmes already being implemented in Member States but would also bring added value to them.
This would also reinforce the ability of the EU's internal market to safeguard the profitability of business activities and create wealth on a continuous basis.

Figure 2.2 illustrates a commonly presented view of the different ECIs. As ICT systems are strategic components that form an integral part of the other critical infrastructures, the author has sought to illustrate this in the figure.

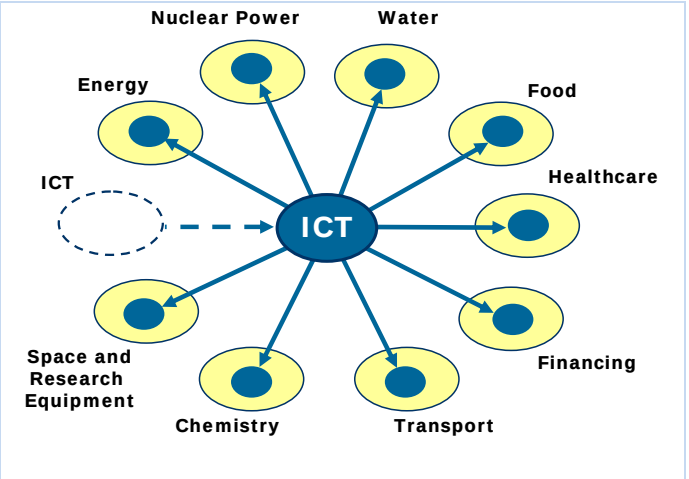


Figure 2.2
Critical infrastructures specified by the European Union.

2.3.2 ECI/ICT

ICT subsectors that are critical in an information society have been specified by the EU as follows: the Internet, fixed networks, mobile networks, radio and navigation systems, satellite systems and broadcasting systems. The 'layers' within the ICT subsectors are: environment, energy, hardware, software, networks, content, policies and practices, users and added value services.

2.3.3 CIIP policy initiative and EPCIP

In 2008 the European Union approved a policy initiative on critical information infrastructure protection (CIIP), which had long been in preparation. This CIIP policy initiative is being implemented as part of the broader European Programme for Critical Infrastructure Protection (EPCIP) and also in parallel with it. The EPCIP is being managed directly from the Directorate-General for Justice, Freedom and Security[20]. The Council of the European Union adopted the EPCIP in April 2007.

The EPCIP is examining ways in which critical infrastructure protection can be improved and is also providing support for this. Means of protection are needed especially in combating terrorism, but also for other reasons such as natural and technological disasters. In EU terminology, critical infrastructures are systems critical to society that have an operating impact covering at least two European states and whose efficient protection requires common and coordinated protection arrangements and cross-border collaboration.

2.3.4 Directive

A key element of the EPCIP is the Directive on the identification and designation of ECIs, issued in December 2008[21,22]. A further key element is the Critical Infrastructure Warning Information Network (CIWIN) [23].

Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection represents the first step towards defining and assessing ECIs. The Directive concentrates initially on the energy and transport sectors. It will be reviewed after three years, and the intention is to include the ICT sector in the next, revised directive.

2.4 International cyber initiatives

International cyber attacks against critical infrastructures in different parts of the world occur almost weekly and have given rise to a number of cyber initiatives. In spring 2008, NATO set up a Cooperative Cyber Defence Centre of Excellence in Estonia[24]. Numerous other cyber initiatives have emerged at different levels, too (e.g. the secret Cyber Initiative, USA[25]).

---

[20] http://ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm.
[21] Directive 2008/114/EC.
[22] http://register.consilium.europa.eu/pdf/fi/08/st16/st16862.fi08.pdf.
[23] COM(2008) 676 final.
[24] Helsingin Sanomat, 11 June 2008.
[25] http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html.

3 VITAL FUNCTIONS OF SOCIETY AND THREAT SCENARIOS

3.1 Functions

The Finnish Government puts forward necessary policy guidelines for securing society's vital functions[26] in its reports on security and defence policy, which are submitted to Parliament for approval. The practice of issuing these reports allows the Government and Parliament the opportunity to conduct a regular, wide-ranging and thorough debate on security issues. The reports assess developments in the security environment and determine Finland's operating strategy on this basis.

The vital functions are sets of functions essential to society that run across the different administrative branches of government and whose continuity must be secured at every moment (see Figure 3.1).

Society's vital functions are:

- management of government affairs
- international activity
- national military defence
- internal security
- functioning of the economy and infrastructure
- the population's income security and capability to function
- psychological crisis tolerance.

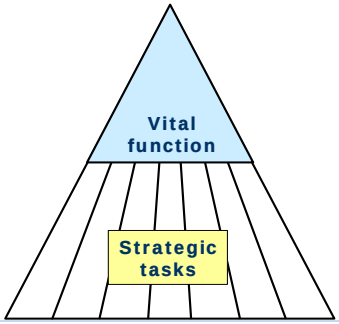


Figure 3.1 Society's vital functions are secured by focusing on strategic tasks.

For each function, a target state is outlined that sets the basis for defining the strategic tasks for which the ministries are responsible and the related maintenance and development tasks. The descriptions of functions and their target states and the development required for managing the strategic tasks take into account Finland's membership of the European Union, its work within the United Nations, its work in NATO's Partnership for Peace and in other international forums.

3.2 Security situations and threat scenarios

The security situations regarding society's vital functions and the various threats and threat scenarios affecting these are for the most part the same whether dealing with the public sector, the private sector or citizens in general. Differences are concerned mainly with whether the situation is in normal or emergency conditions or related to crisis management.

The YKÄ project deals with securing the usability and availability of information infrastructures and their energy supply in all circumstances.

[26] Strategy for Securing the Functions Vital to Society, government resolution, 23 November 2006.

3.2.1 Security situations

Society has to be able to secure vital functions in all circumstances. Contingency preparations emphasize the importance of making arrangements and taking measures in times of normal circumstances. In particular, electronic communications, telecommunications and energy supply systems needed for leadership and for controlling vital functions must be protected and secured during normal circumstances, ensuring that they can withstand the demands of different disruptive situations and emergency conditions.

The different security situations are specified as 'normal circumstances', 'disruptive situations' and 'emergency conditions', and 'special situations' can occur in any of these (Figure 3.2). The usability and availability of information infrastructure essential for society's vital functions are matters that concern all security situations, and this can start simply with the availability of the Internet and mobile networks.

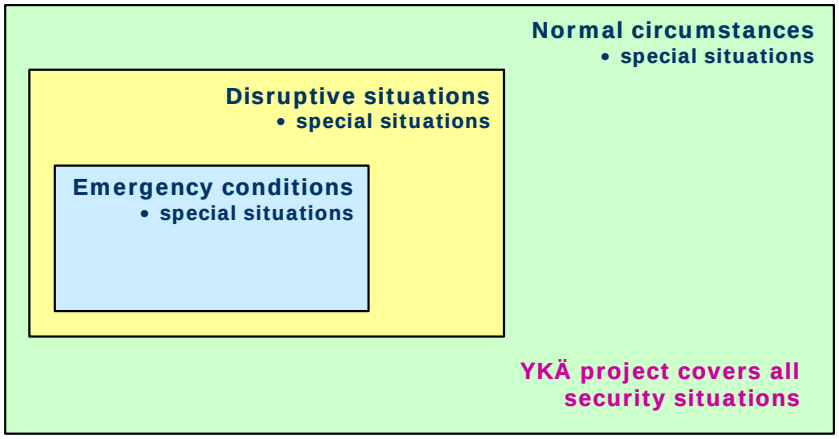


Figure 3.2 Security situations in society.

A more detailed description of the different security situations in society, the threat scenarios in regard to the Strategy for Securing the Functions Vital to Society (YETTS) and the special situations is given in Appendix 2.

3.2.2 Threat scenarios

A threat scenario is a general description of disruptions in the security environment that could endanger security in society, people's survival prospects or the nation's independence. Such situations could lie somewhere between threats affecting individuals and global threats. There are interdependencies between these levels, and so no clear boundaries can be defined between them.

The YETTS threat scenarios are:

- Disruption affecting electronic infrastructure
- Serious disruption affecting people's health and income security
- Serious disruption affecting operation of economy
- Major accidents, natural disasters and other accidents related to environmental conditions
- Environmental threats

- Terrorism and organised and other serious crime
- Threats related to population migrations
- Political, economic and military pressure
- Use of military force.

3.2.2.1 Seriousness of threats

A disruptive event may affect only an individual company or organisation internally or consumers in a very localised area. It may be an obvious operating malfunction, or it may have more extensive significance for society even in normal circumstances (of significance in terms of YKÄ or YETTS), or it may have an impact on the functioning of the state in disruptive situations and emergency conditions (YETTS). The impact will depend on the nature and extent of the event in question.

Figure 3.3 is a schematic illustration of the different levels of threat severity affecting ICT systems and energy supply and the impact of disruptions.

To safeguard the work of the YKÄ project it is important to identify the YKÄ threats and the disruptions causing them, which could have either very localised effects or a much broader impact, and in different security situations.

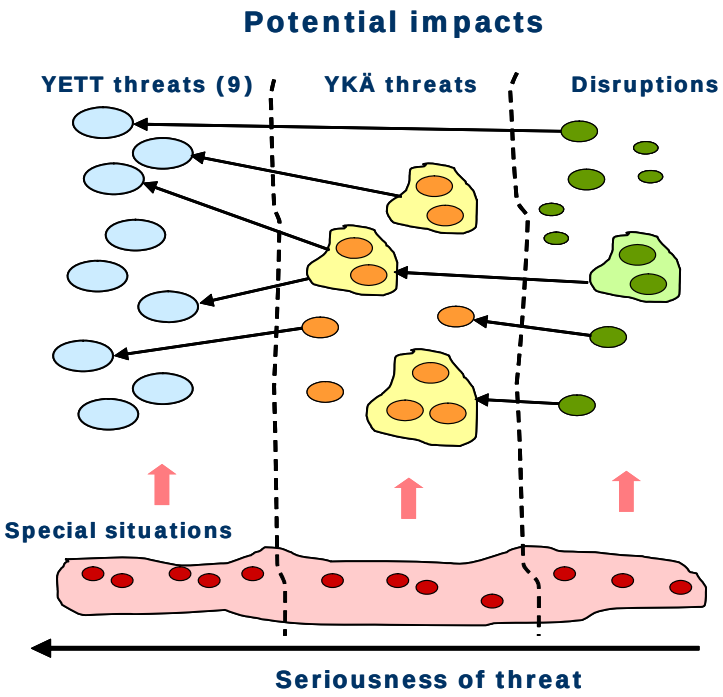


Figure 3.3 Threats and impacts at the YKÄ and YETTS levels caused by disruptive events occurring in information infrastructure and/or in energy supply.

Example: Kaminsky flaw

If there is a fault in the Internet infrastructure, all Internet traffic could be under threat. Spring 2008 saw just such a case, when a serious flaw was discovered in the Internet's DNS (Domain Name System) server system. This became known as the Kaminsky flaw [27]. The danger of DNS vulnerability for Internet users lies not simply in being directed to harmful websites. Attackers can also try to hijack

[27] Dan Kaminsky, Black Hat Security Conference, USA, August 2008.

e-mails. As this concerns traffic routing, the nature of the terminal used is unimportant (Windows, Linux, Macintosh, mobile phone), though each has its own information security problems.

The Kaminsky flaw had remained undetected in the Internet since the beginning, 25 years ago. This DNS vulnerability has still not been rectified in all DNS servers. According to the Finnish Communications Regulatory Authority (FICORA), one in ten DNS servers still remain vulnerable (January 2009). These unrepaired servers are everywhere: in the public and private sectors, with Internet operators and private individuals.

DNS vulnerability is a classic example of a major threat affecting vital functions of society. The Internet was not built to a 'carrier-grade' standard, unlike telephone networks or mobile networks, for instance. The Internet has always had to be patched when new vulnerabilities are found. It is probable that the Internet has numerous other serious holes.

3.2.3 Threat analysis

Table 3.1 presents a small part of the threat analysis performed in the VARE project[28], as an example of the type of information society impact that could arise from YETTS threats and related special situations.

The VARE project involved a more extensive analysis of the YETTS threat scenarios and related special situations and their impacts, concerning both the current situation (2008) and 2016, the end of the VARE action programme. This allows an assessment of the impacts of the measures.

The YETTS threat scenarios and related special situations and their significance for the government's ICT contingency preparations (VARE) are in practice in many respects the same as for the work under the YKÄ project on enhancing the *usability and availability* of information infrastructure essential for securing the vital functions of society. The service chains and service production of both central government and the information society at large are ultimately managed by the same private companies, who are also responsible for them.

[28] VARE Annex 2, threat analysis and scenarios, v05, 28 May 2008. Examples of the impact of special situations on ICT operation and of the role of VARE.

Table 3.1 Examples of the information society impact of special situations.

YETTS threat and related special situation		Event	Impact on usability and availability / functioning of information society
1. Disruption affecting electronic infrastructure			
Large-scale destruction or malfunction affecting public ICT systems.	A	Network and information system clocks working incorrectly.	Network Time Protocol (NTP) clock service used by information systems fails to work properly; e-mail send and receive times do not match; operation of certain event-management systems disrupted.
	B	Large-scale, long-duration power outages due to storm.	ICT systems switch to backup power, some of which does not work or is of too short duration; backup power does not cover all of user's equipment.
	C	Major ownership changes.	Functions moved abroad, discontinued and/or companies broken up.
	D	Fallen power lines.	Leads to localised problems in power distribution.
Large-scale malfunction of technical systems for electronic mass media.	A	Serious faults in transmission links for programme distribution.	Significant amount of public telecommunications network resources needed for mass media.
Major disruption in energy network.	A	Production at Loviisa power station shut down.	Large-scale disruption in energy distribution of a duration that exceeds the buffer from backup system.
	B	Continued disruption in operational monitoring of energy supply.	
	D	Damage at transformer station.	Local needs for backup power.
2. Serious disruption affecting people's health and income security			
Serious malfunction of social insurance service network.	A	Long-duration drop in usability/availability of service or basic registers as result of data corruption.	Weakened accessibility of basic data for payment functions.
3. Serious disruption affecting operation of economy			
Disruption affecting international and domestic payment systems.	A	Major bank's online functions closed due to serious information security vulnerabilities.	Purchasing problems as result of poor operation of invoicing and accounts payable and receivable.
	B	Serious workforce problem for key service provider.	Collapse in service level.
Significant disruption in financial markets.	A	Significant and long-duration drop in value of ICT shares on stock exchange, corporate actions and investment downturn.	Difficulties with investments, corporate actions.
Disruption in foreign trade.	A	Finland's SEPA functions closed due to information security breaches.	Difficulty purchasing materials required for spare parts and development work.
4. Major accidents, natural disasters and other accidents related to environmental conditions			
Nuclear accident in Finland or in neighbouring regions.	A		Immediate problems from electromagnetic pulse; restrictions affecting supply system flexibility; labour availability.
	C	Serious nuclear accident in region neighbouring on Finland.	Maintenance of Government decision-making and operation of security authorities.
Storms, floods or dam breaches causing evacuations or serious destruction.	A	Autumn storm in Helsinki region raises water level by 2.8 m.	Extensive water damage for both teleoperators and customer organisations in the Helsinki region following blockages in wastewater systems, causing damage to telecommunications and information infrastructure. Large-scale interruptions in service provision.
5. Environmental threats			
Rise in an area's concentrations of heavy metals or chemicals to beyond permitted limits for health.	A		Disruption to supply system due to flexibility restrictions.
6. Terrorism and organised and other serious crime			
Serious crimes or the threat of such against the state's highest leadership and key institutions or companies.	A	Criminal organisation threatens to injure top Government figures if its demands are not met.	Attack or aggressive reconnaissance against ICT companies.
7. Threats concerning population migrations			
Large-scale immigration.	A		Locally heightened need for data transfer.
	B		Vandalism, rioting.
8. Political, economic and military pressure			
Online transactions and financial transactions brought to a standstill.	A	Systematic and prolonged attack on the certification systems of Luottokunta, Finland's leading card payment service provider.	Problems obtaining backup resources and spare parts.
9. Use of military force			

A = special situation directly concerning ICT infrastructure
B = special situation that concerns essential support arrangements for ICT infrastructure, and weakens ICT usability/availability
C = special situation leading to significant special requirements regarding the operation and usability/availability of government ICT
D = special situation that does not give rise to significant disruptions for ICT, or the management of which leads to special requirements for only a specific administrative branch's ICT

4 DEFINING THE CRITICAL COMPONENTS OF INFORMATION INFRASTRUCTURE

4.1 Critical information infrastructure

4.1.1 ICT evolution, threats and vulnerabilities

Local, national and global information infrastructure provides data, telephone and video services to public and private users in complex systems comprised of a great variety of networks, electrical and electronic equipment, computers and software applications, themselves composed of many different technologies. Information society ICT systems and services are offered under free competition principles by network and service operators, system suppliers and integrators, and private service providers and suppliers, which range in size from international organisations to small local companies.

Information infrastructure is constantly changing and in turmoil on account of rapid technology development, new business requirements, changes in the business environment and regulations and guidance from the authorities.

This continuous evolution gives rise to new technologies, new applications and software, and new hardware and operating models in all the subsectors of the information infrastructure. These subsectors and components are interdependent, and as complex systems they are exposed to various vulnerabilities and threats.

4.1.2 Critical information infrastructure

From the YKÄ project's perspective, critical information infrastructure can be divided into critical communications systems (subsectors) and critical information systems and their component parts (ICT layers). This is illustrated in Figure 4.1[29,30]. Critical ICT and its components are presented in more detail in Appendix 1.

4.1.2.1 Critical communications systems

The European Commission lists the following critical communications systems (communications subsectors) in an information society:

- Internet
- Fixed networks (landline, wireless)
- Mobile networks
- Radio and navigation systems
- Satellite systems
- Broadcasting networks and services.

Within these, individual sectors may have their own critical communications systems (e.g. the VIRVE radio network for Finland's public authorities).

[29] Towards the definition of criteria for the ICT sector, Marcelo Macera, IPSC-JRC, February 2008.
[30] Adapted here (by report author) from 'The ARECI Study', Availability and Robustness of Electronic Communications Infrastructures, March 2007

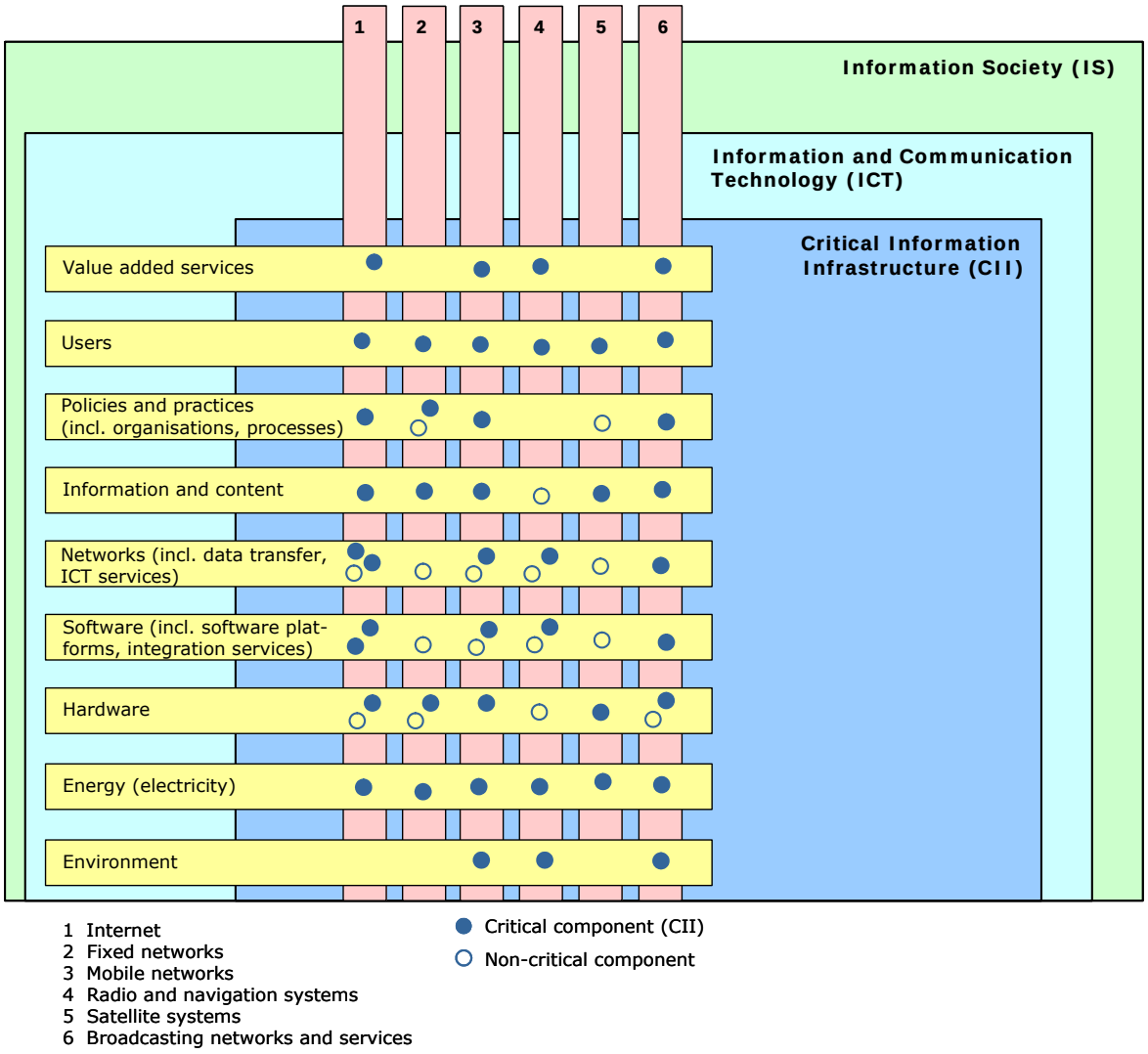


Figure 4.1 ICT layers and their critical/non-critical components as part of the critical information infrastructure (CII) and part of the information society (IS), with critical components identified at a general level.

4.1.2.2 Critical information systems

In an information society there will be a great many information systems of different kinds and at different levels. Each system, big or small, is critical for the activities of one group of users or another. A single definition of a critical information systems is therefore difficult.

The VAHTI working group has defined the key information systems as follows[31]:

- The main information systems are systems that produce or support functions that, if absent or using data that is erroneous or becomes disclosed, would lead to major economic or other losses for society. The functions can also be such that their absence or interruption would have a paralyzing impact on society or the operation of an organisation, or would weaken public safety/security.

  A key information system may be composed of a number of information systems that communicate with each other.

[31] Securing the government's key information systems, VAHTI 5/2004. (In Finnish)

In addition to key information systems used in normal circumstances, there are also key information systems for use only in emergency conditions.

From the YKÄ project's perspective, critical information systems include:
- Critical sectors' (see 2.1.1) own information systems
- Public sector registers

Within critical sectors are many kinds of information systems typical for each sector, such as the financial sector's data centres, customer service systems and the TUPAS certification service, or energy transmission control and monitoring systems (SCADA[32]), etc.

Public sector registers in Finland can be divided into
- General basic registers
  - Population Information System
  - Land Information System
  - Finnish Business Information System
- Administrative registers
- Local and regional registers
- Statistical systems (Statistics Finland)

The bodies centrally producing and maintaining data for the general basic registers are the Population Register Centre, the National Land Survey of Finland, the Ministry of Justice, Statistics Finland, the Tax Administration and the National Board of Patents and Registration. The basic register systems were created to serve society as a whole, with the data being as easily accessible as possible. Hundreds of millions of 'data units' are disclosed to different groups of users each year.[33]

Other public authorities such as the Tax Administration, the Social Insurance Institution of Finland, and the Ministry of Employment and the Economy collect data for various administrative registers used in, for example, taxation, determining basic pensions, labour market policy and social services work.

Local and regional public sector organisations use a wide range of information systems and registers. The data content is generally broader than that used centrally. Many local and regional authorities are also involved in maintaining basic registers.

Using the 'tunnistus.fi' joint identification service for the Tax Administration, the Social Insurance Institution and the Ministry of Employment and the Economy, a total of more than 700,000 identity checks were made during August 2009, for instance. This volume has been growing all the time. As a support service that pools resources and provides reliable personal and business identification for e-transactions, tunnistus.fi is a good example of a critical public sector service.

4.1.2.3 ICT layers

Each communications subsector can be divided into the following operationally differentiated ICT 'layers':
- Added value services (understood in the broad sense)
- Users
- Policies and practices

[32] SCADA (Supervisory Control And Data Acquisition).
[33] According to a conservative estimate, the number of data items disclosed to different user groups from basic registers in 2004, employing a variety of methods, totalled over 300 million. Source: Preliminary report on electronic registration of ownership of housing company shares, National Board of Patents and Registration publications 1/2004. (In Finnish)

- Information and content
- Networks
- Software and application platforms, system integration
- Hardware
- Energy
- Other infrastructure support and functioning.

Information infrastructure is also reliant on other critical infrastructures, especially energy (electricity).

5 CURRENT STATE OF CRITICAL INFORMATION INFRASTRUCTURE AND DEFINITION OF 'CRITICAL'

5.1 Current state

5.1.1 Strategic importance of Internet and mobile networks

The Internet and mobile networks have a central and growing role throughout society. Both are vital for the public sector, organisations, businesses and citizens. Before long, virtually all services in society will have transferred to the Internet.

The Internet also has a down side, however. It provides organised crime with a real-time, convenient and global marketing and sales/purchasing channel (drugs, human trafficking, terrorism). Information security attacks are commonplace and hundreds of different malware items emerge daily. Denial-of-service (DoS) attacks cause major inconvenience and losses for companies.

5.1.2 Internet: critical infrastructure

The Internet has become critical information infrastructure. The Internet refers here to the technical infrastructure together with services, protocols, connections and standards, which is built on and around Internet protocols (IPs). The Internet is defined via user experiences of the applications (data, audio, video) enabled by an Internet connection service (transmitted by operators). It therefore also includes the interconnection traffic between operators. Critical information infrastructure in Finland thus includes FICIX[34] and TREX[35].

Broadband access is a key feature of Internet use. The speed and accessibility of broadband also reflect, to a certain extent, the status of the information society in general. Without a sufficiently fast broadband it is not possible to use the Internet's thousands of services effectively. Neither can a sufficiently high-quality infrastructure be built without a fast broadband.

The Internet also plays a key role in the assembly of a national status report.

Serious risks and threats regarding the infrastructure and operation of the Internet are set out in more detail in Appendix 1.

[34] Beginning its operations in 1993, FICIX (Finnish Communication and Internet Exchange ry) is the biggest Internet exchange point in Finlan;, http://www.ficix.fi/.
[35] TREX (Tampere Region Exchange), the next generation internet exchange point, http://www.trex.fi/.

5.1.3 Mobile networks

5.1.3.1 Situation assessment

As critical infrastructure, Finland's mobile networks are for the most part of a high quality and the accessibility of services is moderate or better throughout the country, due to the competitive environment. In terms of the accessibility of services, there is still room for improvement in regard to certain sparsely populated areas.

5.1.3.2 Risks and development opportunities

Mobile networks have their own infrastructure risks (Appendix 1, not for publication, section 24(1)(8-9) of the Act on the Openness of Government Activities). One risk is the guarantee of access to a 1 Mbit/s broadband connection anywhere in Finland (in 2010) - this has been defined as a universal service. The wireless technology used is primarily either a mobile UMTS service or Digita's @450 service.

A second risk is associated with the Government's decision that a 100 Mbit/s broadband connection should be available almost everywhere in Finland by the end of 2015.

5.1.3.3 Contingency preparations for disruptive situations under normal circumstances

In Finland, contingency preparations for information infrastructure cover not only emergency conditions but also disruptions under normal circumstances, through sectoral legislation and with the aid of commercial service-level requirements.

5.1.3.4 Contingency preparations for emergency conditions

In addition to the general contingency preparations for emergency conditions concerning telecommunications infrastructure (section 9.2.6), consideration should also be given, in the case of mobile networks, to special contingency measures for emergency conditions (see 9.2.3).

5.1.4 Fixed networks

As critical infrastructure, Finland's fixed networks are of a high standard and access to network services is good. However, there is still considerable room for improvement in the fixed network in regard to future broadband needs, especially in sparsely populated areas. Certain preparations have already been made for this, as the Ministry of Transport and Communications already has broadband plans to build a fibre network by 2015 that would reach almost everyone. The Ministry is responsible for the programme's implementation, while the practical side is the responsibility of the Finnish Communications Regulatory Authority (FICORA)[36].

The vulnerabilities of a fixed network are set out in Appendix 1.

5.1.5 Public/private partnership

Critical infrastructure is for producing or supplying an essential service or product. Society's vital services, such as ICT services and energy supplies, are provided almost completely by means of private sector products and services. This applies to the ICT services of both the public and private sectors.

[36] http://www.ficora.fi/index/saadokset/ohjeet/laajakaista2015.html.

5.2 Desired state, definition of critical

5.2.1 Everything is interdependent

The vital functions of society, and especially critical infrastructures, are all dependent on ICT systems. The 'N-squared' formula applies (interdependencies Nx(N-1)/2), where N is the number of infrastructures. Everything is interdependent. In practice there is no communications network or service that is not critical for certain users.

Defining this criticality is very challenging. The following issues are important in relation to the definition and to the desired state:

- Is one thing more essential than another?
- Who determines the definition and using which criteria?
- To what extent can specifications be set by a third party, such as a public authority? One set of criteria has been defined in Regulation M54 (on Priority Rating, Redundancy, Power Supply and Physical Protection of Communications Networks and Services) of the Finnish Communications Regulatory Authority (FICORA).
- To what standard should usability and availability be developed?
- What reduction in usability and availability is permitted? To what extent can specifications be set by a third party, such as a public authority? A general definition is given in section 128 of the Communications Market Act. One more specific set of criteria has been defined in Regulation M58 (on the Quality and Universal Service of Communications Networks and Services).
- Can service level agreements be made between the subscriber and the (communications network/service) provider?
    - What about networks in which the subscribe-user relationship is not clear?
    - What if the subscriber does not understand himself/herself to be an implementer of a vital function?
    - What if the service provider's product range does not include a service level agreement for higher usability and availability?
    - Should requirements always be incorporated into agreements?

5.2.2 Usability and availability requirements for critical information infrastructure are case-specific

The usability and availability requirements for critical infrastructure or a component thereof may be more critical for one organisation than another (Figure 5.2). Online services and the Internet are critical for a hotel or travel company (organisation 1), for instance. For a housing construction company (organisation 2), on the other hand, the availability of fuel and mobile services may be of greater importance. In the financial sector (organisation 3), telecommunications networks and service centres will have a key role, requiring a high quality standard. The highest quality will be required of all components in the case of networks and services (e.g. TUVE) in the security sector (organisation 4).

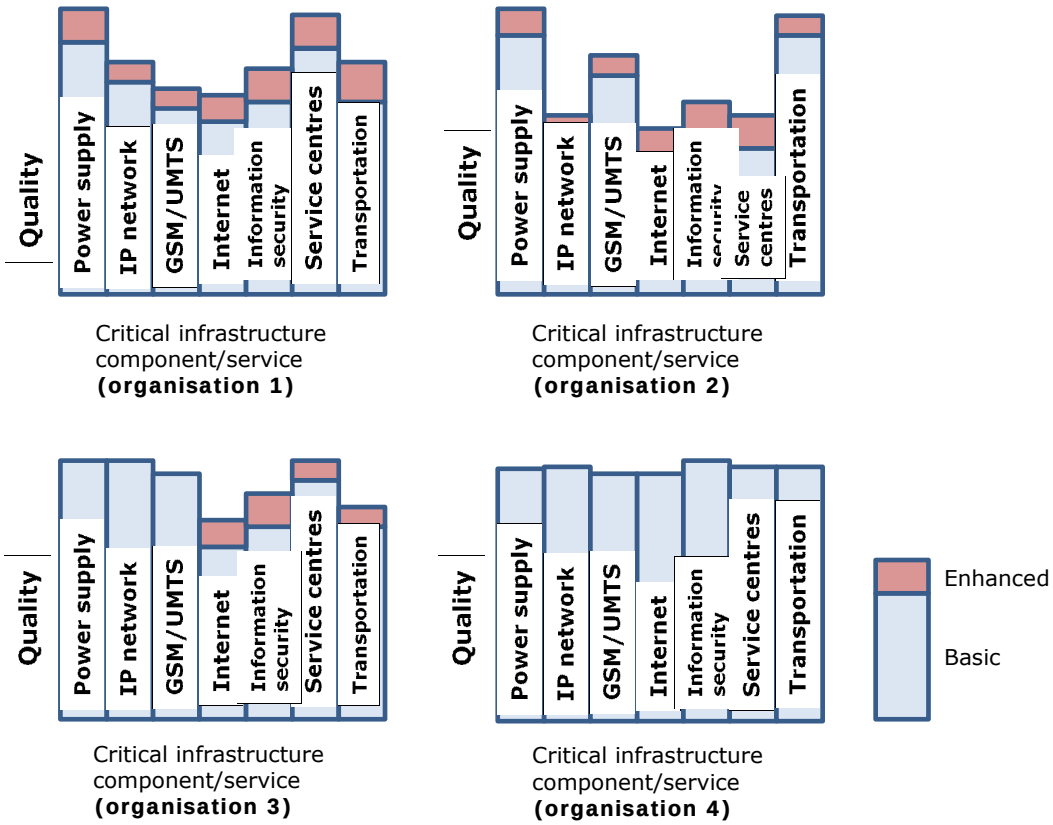


Figure 5.2 Basic and enhanced quality required in principal for critical infrastructure components of a business/other entity (by type of organisation).

Figure 5.2 also illustrates the principle that the basic quality offered via the quality criteria set by public authorities (e.g. FICORA M54/2008 for telecommunications networks; Electricity Market Act for power production) or via general competition is included in the agreed basic price for everyone everywhere, but that supplementary fees can be paid for obtaining enhanced quality.

5.3 Definition of usability and availability criteria

5.3.1 International perspective

The European Union has stated that because critical information infrastructures are global and closely interlinked, and because they are mutually dependent on other infrastructures, their information security and resilience cannot be guaranteed merely by national means without coordination. Resilience of critical information infrastructures is in itself a cross-border process, and in some cases a global one (Internet).[37]

[37] 2 April 2009 EU Commission: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" Impact Assessment (Part 1).

5.3.2 'Grey area' criteria

Figure 5.3 illustrates the different types of status for communications networks and services and the legislation applying in normal circumstances, disruptive situations and emergency conditions. The Finnish Communications Regulatory Authority (FICORA) has completed work on a Regulation on the maintenance of communications networks and services and procedures in the event of faults and disruptions[38]. Work is under way on legislation dealing with the 'grey area' (see 7.2.1).

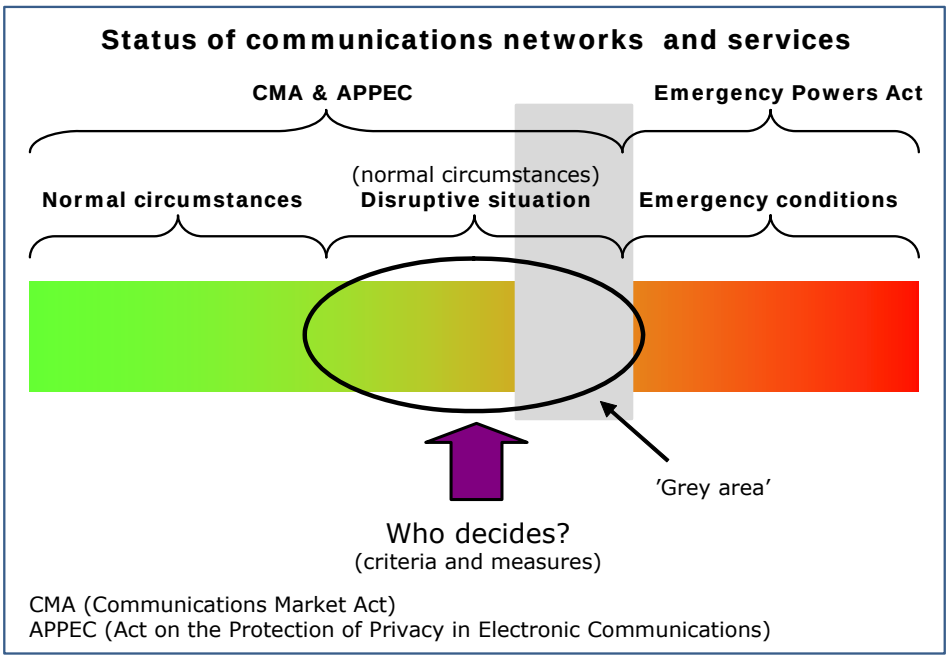


Figure 5.3 Determining the status of communications networks and services and deciding on criteria and measures.[39]

The measures are not simply a technical matter. The issue should be examined on a more comprehensive basis, giving consideration to processes, business models, service level agreements, ownership relations, etc. For ICT companies, contingency preparations require additional input over and above the normal range of activities. Contingency preparation requirements and measures ultimately culminate in additional costs. Are these costs to be paid for by the provider or the user of the critical information infrastructure, or by another party?

In April 2009, the European Commission issued a commentary stating that it is commonly perceived that market forces do not provide sufficient incentive for private operators to invest in critical information infrastructure protection to a level that governments would normally require[40].

[38] Regulation M57/2009 on the maintenance of communications networks and services and procedures in the event of faults and disruptions. (In Finnish)
[39] Seminar on the YKÄ project, 15 April 2009, Sami Kilkkilä, Finnish Communications Regulatory Authority (FICORA).
[40] European Commission statement: "In fact, it is a common perception that market forces do not provide sufficient incentives to private operators for investing to protect CIIs at the level that governments would normally demand – a market failure."

6 SECURING VITAL FUNCTIONS AND THEIR USABILITY AND AVAILABILITY

6.1 Motive: wider adoption of information society technologies

6.1.1 Guaranteeing trust

The aim of the Ubiquitous Information Society Programme is to achieve a wider adoption of information society technologies, which will boost productivity and competitiveness in the national economy and increase the satisfaction of people. The wider adoption of information society technologies can only occur if all the parties involved feel that there is sufficiently well-founded trust in the information society. All sides – public sector, businesses and citizens – have their own perspective in regard to trust.

The different perspectives on trust are given in Table 6.1. Improving the position of consumers requires a responsible approach from all concerned, including consumers themselves.

Table 6.1 Different perspectives regarding trust in services.

Attribute	Measure (example)
Online access (network accessibility)	24/7, 8am-4pm, 99.9%
Service level	Service response time
Privacy protection	See Table 4.2
Lawfulness of content	
Availability of services	24/7, 8am-4pm, 99.9%
Information security	Strong, weak

6.1.1.1 Usability and availability

One of the most important aspects in the wider adoption of information society technologies is guaranteeing the *usability and availability* of information infrastructure (Table 6.1).

NB. Usability and availability are defined in section 1 (see 1.1.1).

6.1.1.2 Privacy and threats against privacy

Measuring trust in the information society presents a challenge. Among the components given in Table 6.1, a second component alongside usability and availability is privacy protection, which is also dealt with in Table 6.2.

There are four groups of threats[41,42] against privacy: data collection, data processing, data transmission and invasion of privacy (Solove[39]). These are divided into sixteen subgroups. Privacy alone is a multidimensional concept in an information society.

[41] Solove, D. J. 2006: A Taxonomy of Privacy. University of Pennsylvania Law Review, vol. 154.
[42] Janne Lindqvist, Privacy protection in a networked society: Eyes open – Information society threats and opportunities, Parliament's Committee for the Future, publication 1/2008. (In Finnish)

Table 6.2 Threats against privacy[40].

Main group	Data collection	Data processing	Data transmission	Invasion of privacy
Subgroups	Surveillance	Combining data	Breach of trust	Intrusion
	Questioning	Identification	Disclosure	Harassment
		Not secure	Publication	
		Secondary uses	Widened accessibility	
		Exclusion	Blackmail	
			Theft	
			Misrepresentation	

6.1.2 Ensuring ICT operations

Trust is built by ensuring the operation of information infrastructure vital to society

- by investing in usability and availability (convenience) aspects (service level)
- through information security measures
- by tackling harmful and unlawful content
- by investing in CERT (Computer Emergency Response Team) activities
- by ensuring the operation of online banking
- through individual protection projects
- by making contingency preparations for cyber attacks and malware.

6.1.3 Identifying critical information infrastructure

Ensuring the operation of information infrastructure vital to society requires that it be identified and that the threats and risks be realistically surveyed and solutions outlined. This is especially important at the infrastructure level, where the impacts are extensive.

6.2 Functions and operators within critical information infrastructure are elements in a process

6.2.1 Usability and availability are made up of the usability and availability of service components

The specification of information infrastructure quality, and of its *usability and availability*, requires analysis of the infrastructure's components. This can be based on examining technical components of the product/service or examining the components as a process. Both approaches are needed. The process approach indicates what is done within the ICT components at different stages, and how this is done, and this focuses on business principles.

It is not possible through the YKÄ work to specify detailed indicators of the usability and availability of each layer and component in the critical information infrastructure. Usability and availability and the enhancement of these is part of the business of the company providing the product or service, and the objectives are defined on a case

by case basis in agreements between buyer and supplier (e.g. SOPIVA, Appendix 2, not for publication, section 24(1)(8-9) of the Act on the Openness of Government Activities), with their quality definitions (SLA[43]).

Table 6.3 uses examples to illustrate the critical components of ICT layers and the importance and vulnerability of these at a general level. In reality, for each ICT element the critical components and their vulnerability/importance are analysed on a customer/organisation-specific basis.

Table 6.3 Example of the most important critical components of information infrastructure and their importance and vulnerability.

No.	ICT layer	Critical component	Importance	Vulnerability
9	Added value services	Customer expertise	+++	+++
8	Users	Usability and availability	+++++	+++
7	Policies and practices	Agreement expertise	+++	+++
6	Information and content	Reliability	+++++	++++
5	Networks	Reliability	+++++	+++++
4	Software	Reliability	++++	+++
3	Hardware	Expertise	++++	++++
2	Energy	Reliable supply	+++	+++
1	Environmental factors	Transportation, payment	+++	+++

(the more plus-signs the more important/vulnerable)

6.2.2 Processes in business

In components of critical information infrastructure, individual functions and operators are considered elements in a process.

6.2.2.1 Processes and structures

The process definitions indicate that they are real-time operations concerned with how an organisation's people, technical systems and so on function in practice. Processes are thus normally an independent dimension of an organisation's structure.

A business process is a group of interrelated *tasks* and the *resources* for performing them, with which *business results* can be obtained. Appendix 1 examines a company's core processes in slightly more detail.

6.2.2.2 External operators – continuity management

Operators (organisations) that are external to the organisation in question also participate in process activities. For the government's critical ICT functions, this is agreed via the SOPIVA procedures and related requirements. Agreements made between purchaser and supplier can include e.g. service level agreements in which the service level and other matters concerning the quality of deliveries are agreed.

[43] SLA = Service Level Agreement.

The main aim of the SOPIVA recommendations is to get the organisation's (senior) management to determine the strategy and aims for continuity management of the organisation's operations, and to organise and allocate responsibility for matters concerning continuity management.

6.2.2.3 Challenges

Processes or process resources can be located globally in different parts of the network. The requirements for *trust* and, within this, for *usability and availability* in regard to critical information infrastructure can thus sometimes be very challenging. In operational networks there may even be hostile parties that use their own, often very effective, processes to exert influence in business communities in line with their vested interests. The new network models may even facilitate this type of development, although they undoubtedly also have their good side (e.g. cloud computing).

6.2.3 Usability and availability of a critical ICT solution at the planning stage

Planning is based on business activities and business processes. The system's requirements are determined by the business processes. The requirements may, for instance, be connected with usability and availability or information security. Thus the planning of usability and availability, for instance, is managed in close collaboration with management of business processes.

The public sector entity planning a secure and reliable information society with the aid of standards and statutes must have the same expertise as the party providing the services in order that technical agreement can be drawn up and understood.

> Trust in the information society – and within it enhancing the *usability and availability* of information infrastructure essential for securing the vital functions of society – can in practice occur only if usability and availability requirements are an integral part of the real operations of organisations, i.e. of their business processes and the management of these. This applies to all levels and all security situations.

6.2.4 YKÄ processes

In identifying critical information infrastructure, individual functions and operators are considered parts of a process. In charting threats and risks, it should be possible to take realistic account of their probabilities and of the interrelationships of risks and threats. The solutions outlined should focus on ensuring operating processes and on the most likely and most significant threats and risks. This is an especially challenging task.

Enhancing the *usability and availability* of information infrastructure essential for securing the vital functions of society (the YKÄ project) is itself a collection of business processes, or 'YKÄ processes'. The YKÄ processes are high-level tasks (definition, planning, publishing, management, government control mechanisms, supervision). The tasks, specifications and requirements are drawn from the strategies, programmes, projects and agreements of central and local government and the private sector (public/private partnership). The processes concern the critical ICT components identified (Figure 6.1).

The YKÄ processes are defined and managed via public sector steering mechanisms by designated organisations with specific responsibilities (Finnish Communications Regulatory Authority (FICORA), the National Emergency Supply Agency, the Government Information Security Management Board (VAHTI), the Advisory Committee for Data Administration in Public Administration (JUHTA), the Government IT Shared Service Centre (VIP), private sector).

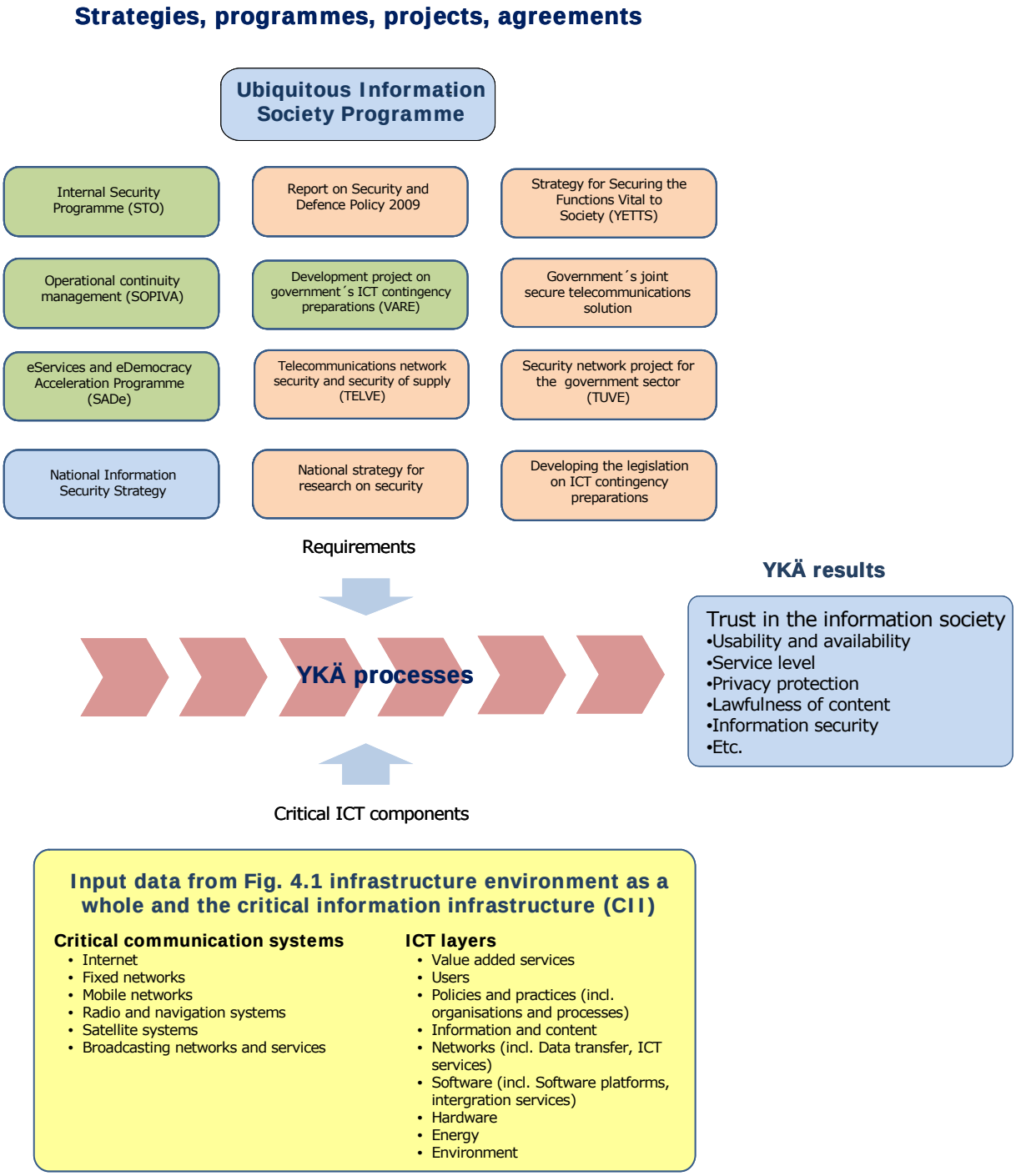


Figure 6.1 The wider adoption of information society technologies requires trust, which is built using high-quality YKÄ processes guided by the aims and requirements of the strategies, programmes and projects for the critical ICT components identified. The strategies, programmes and projects in the upper part of the figure are described in Appendix 2 (not for publication, section 24(1)(8-9) of the Act on the Openness of Government Activities).

6.3 Identity management – a new CII

6.3.1 Each critical infrastructure has its own identity management systems

Critical infrastructures are technical systems that must operate in all circumstances if society's vital functions and associated services are to be maintained. It is known that local, national and international networks (e.g. electrical, telecommunications and transportation networks) can endure only short breaks and disruptions without users noticing. Electronic transactions, payments, entry systems, etc. always require identity verification, whether or not the user is a person, device, network or service.

A key issue is how identity is to be verified in an information society in the event that other infrastructures (e.g. bank services, electricity supply) are unavailable. In an information society, there is a strong reliance on **information** rather than physical components or equipment, and this is a growing trend. Identification problems have been managed for decades using various means peculiar to the different critical infrastructures. Each of these infrastructures has its own 'keys', its own procedures, documentation or tests, before the service can be used.

6.3.2 Dozens of different identity verification methods

The banks have traditionally been at the forefront in developing identity verification. In addition the various credit and debit cards, 'citizen cards', Kela health insurance cards, etc. have functioned as identity cards independently of each other and without any standardisation. Many electronic identities are susceptible to identity theft. This is one of the biggest information security problems.

6.3.3 Information set free

The information society is moving towards an uneasy alliance with technology. A very wide variety of information is being transmitted via very complex systems and networks and dozens of different protocols, from a large array of terminal equipment and applications (PCs, servers, mobile phones, credit cards, bank and retailer applications, databases, etc.).

Moreover, many services and applications have been built in such a way that the data within them is not retained in the terminal for very long. Indeed, the idea is to be rid of the data as soon as possible, to avoid it getting into the wrong hands. The new phenomena to have emerged in the information society include various network communities (Facebook, MySpace, Bebo, LinkedIn, Google), which already feature the 'digital lives' of millions of users.

The above developments, which only scratch the surface, weaken the identity security and trust of users, and in turn add to the growth in cyber crime. Identity management has not evolved in the desired direction, not in Finland or anywhere else.

7 RELATIONSHIP BETWEEN USABILITY/AVAILABILITY OF INFORMATION INFRASTRUCTURE AND CONTINGENCY PREPARATIONS

7.1 Basis, current status and standards

7.1.1 Basis for contingency preparations

The general aim for Finland's security of supply is that this should be based on international markets and on national measures and resources. Contingency preparations are made to secure the infrastructure essential for the functioning of society and for the continuity of critical production under all circumstances.

A significant share of the country's security of supply relies on well-functioning markets and national and international companies and networks. In certain circumstances, systems that are dispersed across borders could also function as backup systems for each other. It is no longer possible to secure all of society's main functions using national means. For this reason, it is necessary to supplement and strengthen national security of supply by making use of EU membership and other cooperation in the field of international security of supply. However, contingency preparations for the most serious crises must always be made on the basis of national measures.

7.1.1.1 Businesses

For businesses, contingency preparations focus on the fundamentals for business operation, agreements made with customers, and risk management in these areas. To the extent that this is not sufficient for society at large, additional contingency preparation responsibilities are set out as obligations in the legislation. These statutory obligations for contingency preparations must not be allowed to disrupt the operation of the market or distort equitable competitive conditions. In this regard, particular attention must be given to both the Finnish and EU competition legislation.

Various companies and business organisations take part in contingency planning on a contractual basis through the National Emergency Supply Organisation's different sectors and pools. In the case of companies of key importance in emergency conditions which produce services for the public sector, for the security authorities and for other key companies, the aim is to guarantee their operating prerequisites in all security circumstances. With the increasing interdependence between the public and private sectors, obligations on both sides must be incorporated in service agreements.

In global markets the value chains of companies are spread across different countries and continents according to where the necessary functions can be produced at lowest cost. The consequence of this is that the fortunes of businesses and governments have become ever more differentiated from each other. The opportunities for national control are diminishing constantly.

7.1.1.2 Non-governmental organisations

In securing vital functions of society, non-governmental organisations (NGOs) based on voluntary activity also play a significant role alongside the government, authorities and businesses, both in the implementation of practical security and in enhancing crisis resilience. The inclusion of these NGOs is based on their own oper-

ating goals, and these must be taken into consideration when planning collaborative measures. In today's society, the role of individual people as operators in various networks is also of growing importance in contingency preparations and related information provision.

7.1.2 Standards

The standards for usability and availability of critical information infrastructure in regard to communications networks and services are in good shape and are constantly being supplemented and further developed. The Finnish Communications Regulatory Authority (FICORA) has introduced a comprehensive range of regulations and guidelines that also take into account the requirements for contingency preparations and set out various measures.

7.1.3 Contingency preparations and YKÄ

Enhancing the *usability and availability* of essential information infrastructure (the work of the YKÄ project) is clearly related to contingency preparations for securing society's vital functions (the YETTS work). Important common programme elements here are the government's VARE project, the Internal Security Programme, and the National Emergency Supply Organisation and its contingency plans and agreements (National Emergency Supply Agency, SOPIVA). The practical measures for the wider adoption of information society technologies and the government's ICT contingency preparations are based on services offered by the same private sector operators.

The YKÄ project is also clearly related to the contingency preparations of businesses and NGOs.

7.1.4 Challenge: information networks constantly underprepared?

The competitive pressures of the market economy felt by companies and exacerbated through networking appear to result in minimal contingency preparations in general and within information networks in particular, e.g. in terms of backup power, reserve equipment and staff backup. Today's information networks are tuned extremely efficiently, because the parties involved have a relatively high level of trust in the network and in each other. Competition appears to be keeping information networks in a constantly underprepared state. The incentives are not in place. Legislative provisions are needed.

Competition has also led to companies specialising further and thus to the enlargement of value networks and lengthening of value chains, which exacerbates the vulnerability of the system in crisis situations. No single participant can alone achieve a significant benefit from contingency preparations. Common strategies are needed.

The undoubted problem areas referred to above can be identified and resolved, but the complexity of the system means that it is impossible to foresee everything.

7.2 Adequacy of legislation for contingency preparations

7.2.1 Developing legislation on contingency preparations concerning the information infrastructure

On 1 November 2007, the Minister of Communications set up a working group to assess the need for regulatory amendments within the purview of the Ministry of Transport and Communications in regard to contingency preparations, taking into

account factors such as actions required under the Strategy for Securing the Functions Vital to Society (YETTS). In addition, the working group was asked to assess the need and potential for legislative means to strengthen the cooperation between telecommunications companies and companies responsible for energy distribution. The working group continued until the end of November 2009.

Telecommunications companies (network companies and communications services providers) are often able to manage and cover problematic disruptive situations by means of agreements. However, there are certain serious disruptive situations that cannot always be managed through mutual agreement between operators. The working group's aim is to identify the disruptive and other situations in society that do not fall under the concept of emergency conditions referred to in the Emergency Powers Act, but during which the government would need to support the interruption-free operation of the market.

Natural phenomena, especially disruptive situations affecting information security, disruptions to electricity grids and power distribution, problems obtaining spare parts, and market disruptions and other disruptions in telecommunications and online services can lead to serious situations in which the operation of functions vital to society can no longer be guaranteed. It must be possible to respond to such situations, and rapidly, too, with sufficient powers. Promoting cooperation between different operators through legislative means may help resilience in serious disruptive situations.

For this purpose, legislative powers are needed in order to ensure a more rapid switch to crisis management status and, once the situation has passed, a return to normal circumstances (Figure 7.1).

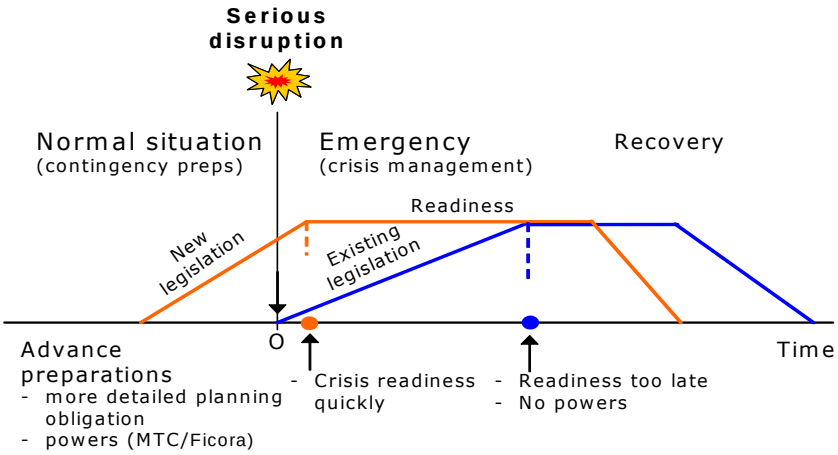


Figure 7.1 Contingency preparations improved through legislation.

7.2.2 Guidelines for contingency preparations

Society's vital functions have become more vulnerable than before, due to the widespread interdependence between ICT access and the availability of electricity. National services also rely increasingly on international networks and services (e.g. banking services). Society's vital functions are thus more vulnerable not only to national but also international cyber attacks.

This invites the question of which powers set out in contingency preparations should be invoked in major disasters.

8 ENERGY SUPPLY FOR TELECOMMUNICATIONS NETWORKS AND THE ADEQUACY OF PROTECTION

No information society can function without electrical power. Some terminal equipment can use batteries, however, and base stations have backup power for several hours. Traditional landline phones can also be used to make emergency calls even if there is a power outage in the home. These are a few examples of what is possible during a power outage.

The YKÄ project is thus directly concerned with power availability.

8.1 Finland's power grid

Finland's power system comprises the main grid, regional networks and distribution networks. Electrical energy in the main grid is transmitted from power production locations and from abroad to centres of consumption.

Most of the electricity consumed in Finland is transmitted via the main grid. Some of the power plants producing electricity are connected directly to the main grid, as are major consumers such as large factories. Power plants may also be connected to a regional or distribution network.

The electrified sections of the rail network take their traction power from the main grid, as does Helsinki Airport.

The regional and distribution networks transmit power within their own areas. Homes get their electricity from the distribution networks. Industry, the retail trade, services and agriculture get their power from the distribution network, regional network and the main grid according to the amount of energy used.

The main grid is mainly exposed to the elements. One tenth of the medium voltage grid and one third of the low voltage grids runs via underground cables. In the centres of towns and cities, in particular, the power lines are underground cables.

The aim is to have more underground cables for the low voltage grid, but doing so for the main grid would be very costly.

8.2 Importance of electricity

8.2.1 Power outages

Society's dependence on electricity has grown so great that disruptions in power distribution can paralyze daily functions completely. Water distribution, wastewater operations, fuel distribution, operation of shops and bank cash dispensers, telecommunications and heating all rely completely on electricity. They would come to a standstill in the event of a power outage due to stormy weather or a technical fault. The electricity dependence of a high-tech society presents risks that should be taken more carefully into account in contingency planning, in both the public and the private sector.

By official definition, a long-duration power outage is one that last more than three minutes[44]. In such cases, the supply of electricity does not get automatically reinstated after a short period. A long-duration power outage is also defined as one in which consumers are paid a fixed sum of compensation for a power outage lasting more than 12 hours. The fixed compensation sums are specified in the Electricity Market Act.

An individual fault in Finland's main grid, leading for instance to a power plant shutting down, is not sufficient to cause long-duration power outages for consumers. However, two such major faults or a fault appearing at a time of peak consumption and low production could even lead to a power outage affecting the entire country. If a fault in the main grid causes a nationwide power outage, this would last longest in the south of the country, as power would, in such circumstances, first be returned to northern Finland.[42]

8.3 Reserve power

8.3.1 Standards

Regulation M54/2008[45] of the Finnish Communications Regulatory Authority (FICORA) on 'Priority Rating, Redundancy, Power Supply and Physical Protection of Communications Networks and Services' includes regulations on the need for backup power for components of communications networks and services. Components of communications networks and services are rated on the basis of their importance in descending order from 1 to 5. The criteria for determining the priority ratings are described in the Regulation. The priority ratings concern phone services, broadband services, e-mail services, mass media services and other communication services.

For example, a component that affects communications services across a large geographical area (over 20,000 km^2) or a component that affects

a phone service covering ≥50,000 users, or
a broadband service covering ≥50,000 users, or
an e-mail service covering ≥200,000 users, or
a mass media service covering ≥100,000 users, or
another communication service covering ≥200,000 users,

is of class 2 importance, which requires backup accumulators for at least 6 hours (if the component of the communications network or service is connected to a power plant system in which the power backup is a fixed backup power plant, the accumulator's minimum duration is 3 hours)[43].

The minimum backup periods for backup accumulators are sufficient for the basic needs of the information society in normal circumstances. In Finland, too, there are, however, occasionally longer power outages caused by major storms, where 6 hour backups would not suffice.

Rectifying storm damage requires that, on top of everything else, field personnel are able to communicate using mobile connections. This represents a clear dependency relationship between power grids and mobile networks.

[44] Long-duration power outages and securing vital functions of society, Ministry of Defence, 28 May 2009. (In Finnish)
[45] Regulation M54/2008, Finnish Communications Regulatory Authority (FICORA).

8.4 Adequacy of today's protection systems

8.4.1 Overview

ICT systems are protected at a number of levels. Public authorities issue regulations (e.g. the Finnish Communications Regulatory Authority (FICORA) in telecommunications, and VAHTI in respect of information security for the government), and industry has its own regulations, as does the real estate sector (e.g. regarding cabling).

In addition, users have a wide range of practices for protecting themselves from, for instance, malware and for encrypting data being transmitted or contained in files on their computers.

Below is a discussion of the adequacy of protection systems in the government's vital information systems, the ICT services of municipalities and in communications systems.

8.4.2 Government information systems – situation 2008

The government's information security situation has been monitored systematically since 2000. Figure 8.1[46] presents the statistical trend for 2002-2008, drawn up on the basis of questionnaires. The figure does not show areas of information security where, in practice, almost 100% of agencies already operate in accordance with basic objectives. Such areas include, in the field of IT information security, tackling malware prior to e-mail distribution and in workstations, and, in the field of public sector information security, maintaining on at least a part-time basis an employee in charge of information security who reports to senior management.

[46] Government Information Security Management Board (VAHTI) report on operations for 2008, Vahti 1/2009, Ministry of Finance. (In Finnish)

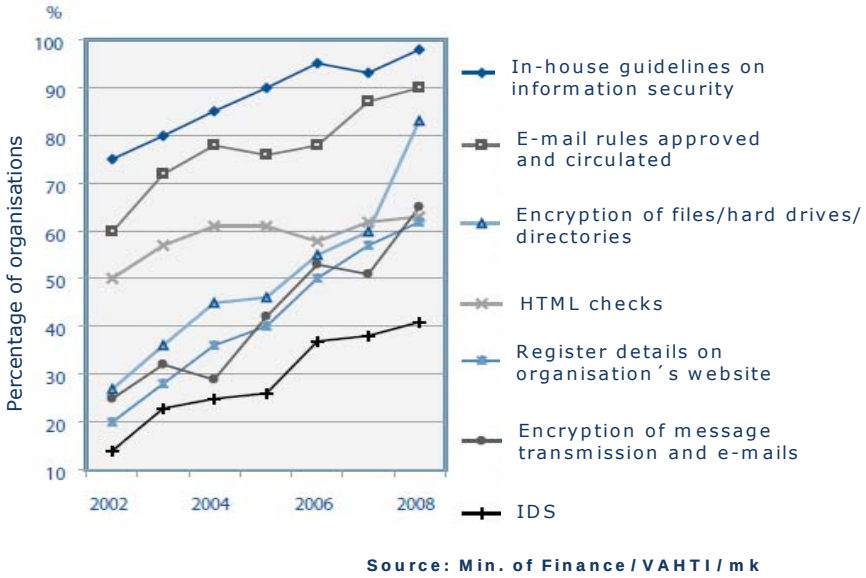


Figure 8.1 Trend in information security. The data was collected during 'government information security' theme days arranged annually in December by the Government Information Security Management Board (VAHTI).

The ministries and agencies have invested extensively in developing information security cooperation among information security organisations and different units, contingency preparations and data protection for non-conformity and disruptive situations and emergency conditions, and agency-level plans and guidelines. Protection from malware and information security attacks and other IT security development have been central to the continuous information security work carried out in every government organisation.

Figure 8.2 illustrates the trend in malware-induced denial-of-use situations, and the spread of information security attacks requiring special action[70]. Malware and information security attacks are an increasing problem. In 2008, about 16% of government organisations found themselves the target of an attack.

To manage the risks posed to operations and to ensure continuity, the government must be able in future to significantly further improve its contingency preparations for information security problems and its management of non-conformity situations, as well as its knowledge and management of different information system and network situations.

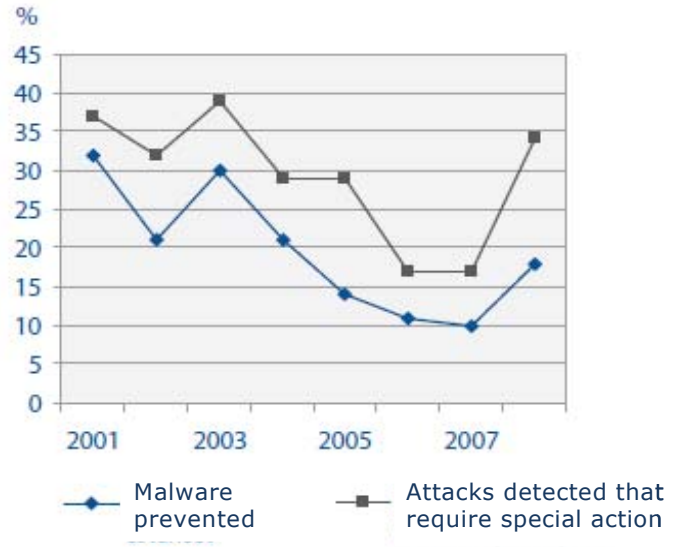


Figure 8.2 Impact of information security problems in government administration, 2001-2008.

The situation in regard to the adequacy of protection for the government's information systems is good and improving.

8.4.3 Private sector

The protection requirements for service providers are specified in agreements between service buyers and providers. The biggest private-sector providers of public-sector information services are Tietoenator, Logica and Fujitsu. Their protection procedures are of a high standard. There may be room for improvement in the protection systems of smaller service providers and service chains. These, too, are arranged through agreements, and the agreements are monitored.

8.4.4 Communications systems

The Finnish Communications Regulatory Authority (FICORA) is responsible for the protection standards for communications systems. The numerous protection regulations[47] are based on the Communications Market Act and the Act on the Protection of Privacy in Electronic Communications.

8.4.4.1 Regulation M54/2008[48]

FICORA Regulation M54/2008[43] applies to the priority rating of public communications networks and public authority networks and of the communications services provided in these networks, and to redundancy and reserve routes, power supply and securing power supply, and physical protection. The Regulation does not apply to the temporary provision of communications networks or services, or to temporary capacity, DVB-H network transmitters or radio operators whose licence specifies population coverage of less than 85%.

Components of communications networks and services are categorised on the basis of their importance in descending order from 1 to 5; an example was given above

[47] http://www.ficora.fi/index/saadokset/maaraykset/teletoiminta.html.
[48] Finnish Communications Regulatory Authority (FICORA) M54/2008.

in section 8.3.1 (see also Appendix 2, section 3.1.3.1, not for publication, section 24(1)(8-9) of the Act on the Openness of Government Activities).

Telecommunications companies must ensure that their premises for equipment used for public telecommunications meet the minimum requirements for physical protection. They must also ensure that components of communications networks or services left outside the priority rating are protected physically such that unauthorised persons cannot access them easily.

Regulation M54/2008 also contains requirements on the protection of transmission system components.

9 CONCLUSIONS AND PROPOSED MEASURES

9.1 Conclusions about current situation in general, and proposed measures

9.1.1 Telecommunications legislation, standards, structure, pricing

In terms of usability and availability, Finland's telecommunications legislation, statute monitoring, issuance of standards regarding information society issues, and the structure, protection and operation of networks and services are of a good standard internationally. Specifications, security classifications and other standards are of a high standard. Interconnections function well and are simple. The Finnish Communications Regulatory Authority (FICORA) actively monitors developments in the sector and develops standards to meet changes occurring in the sector.

Interconnections in the public telephone network are made under the reciprocal arrangements of operators. IP interconnections are arranged centrally among the operators in the sector. VoIP (Operational Voice over Internet Protocol) interconnection arrangements are still taking shape. Administration of identifiers is arranged extremely well for those cases where national powers are exercised. IP addresses and route databases are produced by a Regional Internet Registry (RIR) company (in Europe: RIPE NCC). The 'fi' root has been dispersed professionally. Within Finnish borders there are three root name servers. For E.164 numbers (telephone numbers), the mechanism is different and the national role greater.

The vulnerabilities of different networks are set out in Appendix 1.

9.1.1.1 Proposed measures

ICT business operations and markets, especially telecommunications networks and services, should only be subject to guidance and control to the extent essential for ensuring diverse and sufficient markets and services. The guidance mechanisms should comprise standards, operating licence conditions and funding. Competition will increase the alternatives, also in regard to usability and availability.

Infrastructure

The infrastructure network of cables (and radio frequencies) should be kept in good condition and should be a dense, flexible, up-to-date and evolving network. Searches for and minimisation of single points of failure (SPOFs) should be performed on a continuous basis. The necessary equipment and power shall be available.

This has cost implications for operators in the sector.

Telecommunications

One of the objectives for traffic (operation) is that the Ministry of Transport and Communications and the Finnish Communications Regulatory Authority (FICORA) should operate nationally and internationally in an active manner and with a strong mandate. This must be safeguarded at the CIIP level.

No cost implications.

End user

At the user level, it is important to secure the operation of the terminal device market, the operating system and system software markets, the encryption product market and the protective software market (anti-virus, IPS[49], etc.). Attention must be given to ensuring that high-risk combinations do not emerge on the terminal device or software markets and that there is no dependence on contact with a manufacture's online services beyond the reach of government regulation.

No cost implications.

Pricing

The pricing of telecommunications services in Finland should be at reasonable level or better. Has the often dramatic price competition of recent years been the reason why it has not proved possible to invest enough in service quality and accessibility (e.g. weak coverage in mobile networks) or in development? This issue has been the subject of public debate.

Ownership

For the state, IT ownership should rest with the Ministry of Finance. Telecommunications matters, including the Internet, should be within the purview of the Ministry of Transport and Communications and FICORA, and contingency preparations should be under the Ministry of Transport and Communications and the National Emergency Supply Agency (sectors and pools). Depending on the case and the situation at hand, it may also be necessary to call for general views at the government level. In practice, the focus will be on the motivations of commercial operators and on monitoring the outcome.

No cost implications.

Cooperation between parties

Cooperation between operators (telecommunications, energy) must be further increased, especially in investigating network and service disruptions and in rectifying faults, as well as in planning contingency preparations. This will improve the usability and availability of services.

Enhancing usability and availability will require greater expertise and training. Maintaining Finland's critical information infrastructure and drafting procurement and operating agreements of a high standard will require a strengthening of national expertise in normal circumstances. Improving the level of expertise will also require additional investment in R&D projects in this field within the public sector as well as in the owner organisations and those organisations with specific responsibilities.

There will be cost implications for different parties. It is not possible to estimate the scale of these.

[49] IPS (Intrusion Prevention System).

9.1.2 Protection of information infrastructure

9.1.2.1 Conclusions

Information infrastructure is protected at a number of levels. Public authorities issue regulations (e.g. FICORA in telecommunications, and VAHTI in respect of information security for the government), and industry has its own regulations, as does the real estate sector (e.g. regarding cabling).

In addition, users have a wide range of practices for protecting themselves from, for instance, malware and for encrypting data being transmitted or in files on their computers.

9.2 Critical communications systems

9.2.1 Usability and availability of critical information infrastructure – general conclusions

In the context of society's vital functions in Finland,

- *ensuring the usability and availability* of essential information infrastructure is, for the most part, in good shape in terms of administration, organisation, legislation and products/services.
- There is room for improvement in the *usability and availability* of information systems and services. The information system and information service sectors do not, however, feature comprehensive standards-based regulatory mechanisms such as those in the electronic communications field.
- The *usability and availability* of information infrastructure is planned, implemented and managed as part of business processes. Purely technical solutions and standards are not sufficient.
- In Finland, the contingency preparations for information infrastructure cover not only emergency conditions but also disruptions under normal circumstances, through sectoral legislation and with the aid of commercial service-level requirements.
- The joint operation of contingency preparations between the public and private sectors functions well and the division of costs is also well established.

In addition to traditional telecommunications, information society networks include traffic from various new sources too, such as the entertainment industry and pay-to-access services. Guidance for these is based on different needs than for ICT functions (e.g. filtering, obligation to store). As a consequence, the usability and availability requirements for networks and services can be conflicting (quality classification, pricing).

9.2.2 Fixed networks

9.2.2.1 Conclusions

As critical infrastructure, Finland's fixed networks are of a high quality and the accessibility of online services is good. However, there is still considerable room for improvement in the fixed network in terms of future broadband needs, especially in sparsely populated areas. Certain preparations have already been made for this, as the Ministry of Transport and Communications already has broadband plans to build a fibre network by 2015 that would reach almost everyone. The practical guidelines for the programme are the responsibility of the Finnish Communications Regulatory Authority (FICORA).

9.2.3 Mobile networks

9.2.3.1 Conclusions

As critical infrastructure, Finland's mobile networks are for the most part of a high quality, and accessibility is moderate or better throughout the country, due to the competitive environment. In terms of the accessibility of services, there is still room for improvement, especially in regard to certain sparsely populated areas (but also in certain parts of the Helsinki region).

9.2.3.2 Proposed measures

In addition to the general contingency preparations for telecommunications infrastructure in emergency conditions, the following special measures should also be considered in regard to mobile networks:

- introduction of a 'privileged customer' facility
- a shared SIM facility (personal SIM card would work in any Finnish network that still operates after a user's network crashes).

Cost implications not assessed.

9.2.4 Internet

9.2.4.1 Situation assessment and general measures[50]

It is not possible to give a detailed list or to know of all the essential services for society over a time perspective covering many years (compare development over past 15 years). Everyone needs the Internet for something, and society needs all services and networks for something.

The Internet has become a critical infrastructure. Services for businesses and citizens via the Internet have become vital. The elements of the Internet located in Finland and the services available in Finland are among the building blocks of the country's social fabric.

9.2.4.2 Proposed measures

The functioning of the Internet as a neutral, evolving and critical data transfer platform must be secured with the aid of international collaboration, regulation and technical solutions, to ensure that it serves society at large in an adequate and reliable manner, as follows:

- by taking into consideration that, for both trunk traffic and terminal devices, the different networks should link together into a single, sufficiently meshed communications infrastructure which, unseen to users, utilises a different protocol or different networks for data transmission
- by ensuring that communications secrecy on the Internet is secured
- by ensuring that Finland has a continuing and active role in the international administration and development of the Internet (Internet Cooperation for Assigned Names and Numbers (ICANN))
- by launching separate reporting on protection of the Internet.

The public sector must reserve sufficient resources for these tasks.

[50] Seminar on the YKÄ project, 15 April 2009. Internet working group conclusions.

9.2.4.3 Risks and development opportunities

Table 9.1 gives examples of threat scenarios that can appear on the Internet and how these can be tackled fully or partially, and the organisations responsible.

Table 9.1 Internet threat scenarios and means for tackling and preventing them.

Threat	Means for tackling / preventing	Organisations responsible

International databases or operational (data) security systems could fail	• services emulated in Finland, and
	  • either own national (information) security systems created, or
	  • national back-up systems created in cooperation with organisations in the sector.
		• CERT-FI
		• operators
		• FICIX

Internet DNS server data could be falsified en masse, or entire servers falsified.	• introduce a DNSSEC system for critical points as applicable, and • ENUM[51] (or DNSxxx)	• FICIX • operators • Finnish Communications Regulatory Authority (FICORA)
IP addresses registered in Finland could be hijacked either intentionally or unintentionally.	• establish a national warning system, and • agree via EU cooperation on impact minimisation in the event of a threat materialising	• CERT-FI • Ministry of Transport and Communications (MTC)
Other measures for improving the Internet's usability, availability, reliability and international accessibility		
Clocking of new telecommunications networks, and NTP (Network Time Protocol) distribution (caesium or GPS clock).		• FICIX
Guidance on telecommunications companies' use of route reflectors, and consideration of a RouteServer option for interconnections.		• FICORA • operators
Securing Finnish representation and continuum in global Internet administration (ICANN[52], IGF[53] and IANA[54]).		• MTC/FICORA • Ministry for Foreign Affairs (MFA)
The United States is preparing legislation on cyber security. It looks like the US President may not, after all, be given the right to cut the Internet connection of any organisation or service[55]. The first draft of the law indicated that the President would be able to disconnect any information system or network critical for the Federal Government or the United States.		• Legislative developments must be monitored at both national and EU level • MTC • MFA

Contingency preparations for disruptive situations under normal circumstances

In normal circumstances there are various disruptive situations that could emerge on the Internet and for which it must be possible to make contingency preparations. These are presented in Table 9.2. Finland could, for example, be the target of a disruption from outside its borders (e.g. a DDoS[56] attack). This is a very serious threat scenario. Finland could also be a base for the launch of a disruption (e.g. a DDoS attack or an IP hijack).

[51] ENUM (from **E**.164 **NU**mber **M**apping). ENUM is a technology, in which ENUM identifers based on the Internet's DNS server system are formed from traditional telephone numbers (on the E.164 standard). This allows a variety of communications services to be directed to the number (such as Internet phone calls and e-mail). Although ENUM supports various services such as instant messaging and e-mail, its most important use is in directing VoIP calls (http://www.ficora.fi/index/palvelut/palvelutaiheittain/enum/mikaenumon.html).
[52] ICANN (Internet Corporation for Assigned Names and Numbers). See Appendix 2.
[53] IGF (Internet Governance Forum). See Appendix 2
[54] IANA (Internet Assigned Numbers Authority). See Appendix 2.
[55] TIVI.fi, 1 September 2009. http://www.tietoviikko.fi/kaikki_uutiset/article323975.ece?s=l&wtm=tietoviikko/-01092009.
[56] DDoS (Distributed Denial of Service). A simultaneous attack from several sources against a certain system.

Table 9.2 Contingency preparations for disruptive situations on the Internet under normal circumstances.

Disruptive situation	Means for tackling / preventing	Organisations responsible
Cooperation among telecommunications companies paralyzed (e.g. result of corporate acquisition).	• Securing emergency funding • Taking over a company's operating activities • Arranging operations through temporary solutions.	• National Emergency Supply Agency • Ministry of Transport and Communications (MTC) • Finnish Communications Regulatory Authority (FICORA)

Finland could, for example, be the target of a disruption from outside its borders (e.g. a DDoS attack).	• By giving preference to traffic that is internal to the country, e.g.
	  • by introducing white-listed mail servers, DNS servers and a 'privileged customer' facility.
	  • The 'privileged customer' facility should be standardised nationally.
		• MTC
		• FICORA
		• Operators

Finland could also be a base for the launch of an international disruption (e.g. a DDoS attack or an IP hijack), in which case the threat could be that • Finland is isolated from other countries, and • possibly even a shutdown of national infrastructure.	• Aim to avoid directing society's protective actions (filtering, telesurveillance) at critical elements. • Protective actions should be implemented separately from them.	• MTC • FICORA • Operators

9.2.5 Broadband quality

9.2.5.1 Conclusions

Finland's broadband quality (broadband quality score (BQS)) has in recent years slipped behind the broadband services offered by other developed countries. This is illustrated by the results of an extensive survey shown in Figure 9.1. The BQS measures both the downlink and uplink speeds and the latency (delay) weighted by different traffic profiles, both currently and also in accordance with application scenarios for the future.

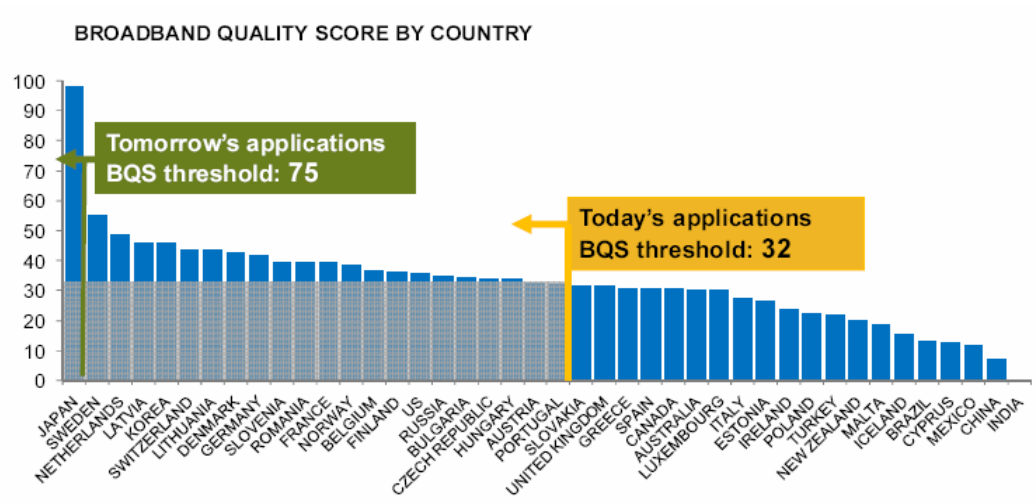


Figure 9.1 Broadband quality score (BQS) in different countries.[57]

[57] Broadband Quality Score – A global study of broadband quality, September 2008 (sponsored by Cisco).

The BQS correlates with the pervasiveness of ICT products and services, the knowledge economy and Internet use. The density of the fibre network and the extent to which cable networks have been updated are also factors raising the BQS score.

The Finnish Communications Regulatory Authority (FICORA) has published a new Regulation M58 on the quality of communications networks and services.

9.2.5.2 Proposed measures

Investment in fibre infrastructure

If Finland's information society is to return to the level where it belongs on account of the experience gained and the economic and technological expertise, and to ensure greater trust in the Internet's role as critical infrastructure, Finland should invest further in broadband access, increasing penetration and focusing on quality. At the infrastructure level this means greater investment in fibre connections.

Improved broadband access will promote the wider adoption of information society technologies, and this will be in line with the YKÄ objectives. The achievement of this will be furthered by the Government's broadband strategy.

The cost implications are great and focus mainly on network investment.

9.2.6 General contingency preparations for emergency conditions

An emergency situation affecting ICT services may arise for instance from a major market disruption or the realisation of a serious external threat. In such circumstances, the accessibility of telecommunications services could be diminished in part or in full (see Table 9.3).

Table 9.3 Contingency preparations for emergency conditions.

Emergency conditions	Action	Organisations responsible
Cooperation among telecommunications companies could be paralyzed as a result of market disruptions • bankruptcies • lack of attention to resources.	• Agreeing a takeover of the operations of telecommunications companies by the government or some other party agreed by the government.	• Ministry of Finance (MF) • Ministry of Transport and Communications (MTC)
Telecommunications companies' operations could become paralyzed • e.g. military strikes.	• Transfer to official systems.	• MF • MTC

9.2.7 Other general challenges and measures

9.2.7.1 Emergency powers legislation – guidance for contingency preparations

Should emergency powers be invoked already during major disasters rather than only in emergency conditions (see 7.2)?

9.2.7.2 Adapting services in line with developments at EU level

Attention must be paid to ensuring that the development of service structures at EU level and the measures to secure vital functions domestically are in harmony with each other and mutually compatible. One example is the way in which the payment system has developed in the financial sector; another is the development of shared structures among different operators (e.g. energy, telecommunications). Further development should be facilitated by exporting good solutions from Finland to the EU, in addition to Finland adopting solutions from the EU.

9.2.7.3 Manageability of networked business activities

Almost all service provision in an information society is managed by the private sector. The immediate partners of service providers can be managed through agreements. Service structures relying on chains of relationships, changes occurring in these relationships, and the responsibilities involved are the most challenging to manage and supervise.

9.2.7.4 Collaboration between political decision-making, bill drafting and business interests

The information society has numerous joint projects in which political decision-making, bill drafting and business interests are represented. These projects have not always produced the best possible results. For example, could the aim of numerous coexisting e-identification systems become a new threat to the continuity of service provision? See sections 6.3 and 9.6.

Moreover, do small and medium-sized companies even have the resources to maintain and manage countless parallel identification technologies and information security technologies?

Collaboration between the different parties must be strengthened and the needs and opportunities of users (companies, consumers) to benefit from decisions and solutions should be investigated further.

9.3 Issues of ownership policy and industrial policy

9.3.1 Changing situation – growing challenges

Information infrastructure has quickly become the most strategic critical infrastructure, together with energy supply. This is acknowledged internationally in all areas of society, and applies as much to volumes as to significance, for instance in regard to productivity in society.

Finland is among the world's safest countries. It is not subject to any immediate threat of a conflict. The world is shrinking, however. Globalisation, economic swings and future threat scenarios involving networks have led to attempts to use national resources to ensure critical ICT functions.

As a consequence of international cooperation, new operating models have been formed from complex value networks. An organisation's operating processes may be partially or wholly located outside the country's borders, making it more difficult to control the security and reliability of operations.

9.3.2 Threat: market disruptions

A characteristic of recent developments in ICT services has been the globalisation of supply and the outsourcing of functions, possible side-effects of which could cause serious market disruptions and problems for the accessibility of ICT services.

The market does not always encourage private operators to invest in the protection of critical information infrastructure to a standard required for society's contingency preparations. This was also concluded by the European Commission.

The **usability and availability** of ICT services cannot be guaranteed in all cases, and this will affect society's contingency preparations. An ICT company and a critical subcontractor company serving it could, for instance, dismiss a high proportion of their staff resources, discontinue offering certain services or go bankrupt.

Today's tough competitive environment leaves few spare resources for a company, and this could weaken its risk-bearing capacity and thus make the company's operations more vulnerable to various threats in a crisis situation.

9.3.3 Working group's findings

There was lively discussion in the working group on the subjects of ownership and supervision of critical information infrastructure and its components.

9.3.3.1 Measures

The securing of information assets and data vital to society, and the accessibility of these, must be guaranteed in all security situations. To prevent data leaks and denial-of-service attacks, for example, it would be good if information assets were widely dispersed. Management of information infrastructure critical to the functioning of society must be arranged in such a way that influence can be brought to bear through national statutes and decisions.

Society must help establish a protection body for critical information infrastructure for situations in which the market does not offer sufficient incentive for private operators to invest in protecting such infrastructure to a standard required for contingency preparation in society at large.

9.3.4 National Emergency Supply Organisation

9.3.4.1 Background

The National Emergency Supply Agency's balance sheet shows approximately EUR 1.2 billion[58]. Most of the funds are committed to warehouse materials. The largest product group by far is liquid fuels, comprising 80% of the Agency's assets. Other major product groups are grain and seed grain, medication materials and various industrial materials.

Security of supply in regard to the functioning of the information society is coordinated by the National Emergency Supply Agency's infrastructure department, information society cluster and the pools within it. In addition, the information society cluster has its own regional organisation, a regional pool consisting of 'TIVA' committees concerned with contingency preparations for information systems. The

[58] http://www.huoltovarmuus.fi/organisaatio/talous-ja-lainsaadanto/huoltovarmuuden-rahoitus/.

Agency's information society cluster is of strategic importance from the YKÄ perspective.

In regard to maintaining the security of supply, ICT activities and logistics have a growing strategic role. Furthermore, the role of the information society in ensuring vital functions of society in normal circumstances has expanded and is of growing significance.

9.3.4.2 Proposal of the working group

The role of the National Emergency Supply Organisation should be further strengthened and expanded in regard to ICT.

Cost implications not assessed.

9.3.5 Expansion of budget for security of supply

9.3.5.1 Problem and models

Securing critical information infrastructure for vital systems beyond the normal level in order to facilitate the wider adoption of information society technologies will require additional investment from ICT operators. Developing the work on critical information infrastructure protection (CIIP) will also require additional investment.

In April 2009, the European Commission issued a commentary stating that it is commonly perceived that market forces do not necessarily provide sufficient incentive for private operators to invest in CIIP to a level required for society's contingency preparations.

There are two main alternatives regarding CIIP funding:

- a separate CIIP budget, in which the government's share is e.g. 50% and that of telecommunications companies altogether 50%.
- telecommunications companies collect 'CIIP cents' directly from buyers and transfer these to the CIIP budget.

In both models telecommunications companies are set obligations and principles concerning who pays if it becomes necessary to make key investments in CIIP in excess of the normal level.

The first of the two models is in use in Sweden. The second principle is the same as today's 'emergency supply charge' collected in conjunction with energy taxes. The emergency supply fund is growing through energy use, but funds are allocated to e.g. medicines and ICT structures.

A further question surrounds the role of networks and service providers that are important to society (mass media, funding, retail,...) in the collection of CIIP funding and in paying for investments.

The turnover of telecommunications companies in 2008, for example, was a total of EUR 4,262.6 million[59]. If 0.6% of this were collected for contingency preparations, this would mean an additional sum of about EUR 25 million on the present contingency preparation budget.

[59] http://www.stat.fi/til/tvie/2008/tvie_2008_2009-06-09_tau_011_fi.html.

The level of funding should be adjusted to meet overall demand, and should be targeted in accordance with the needs of critical infrastructure, as outlined in the Government decision.

Demand and supply should nevertheless in themselves guarantee companies an appropriate level of continuity management. If needs are greater than this, public authorities would pay this through budget funds.

9.3.5.2 Working group's findings

The working group has discussed funding of the new challenges for contingency preparations.

9.4 Further development of the YKÄ work

9.4.1 Guaranteeing the continuity of the YKÄ process

Responsibilities in regard to the YKÄ work on enhancing the *usability and availability* of information infrastructure essential for securing the vital functions of society are currently allocated within the public sector to the different ministries and organisations, and to a range of projects. Within the framework of the YKÄ project now being concluded, the future of this work is being examined at senior level in the Ministry of Transport and Communications. The YKÄ work demands continuity and needs to be further developed in regard to business processes and the practices agreed on the basis of these (see section 6.2.4). The working group found that

- there are no shortcuts to the YKÄ objectives, as all the required action must be taken with care
- the YKÄ project should be guided and monitored actively to ensure that undesirable practices do not get established unintentionally
- the strategy and guidelines of the YKÄ project should be controlled and monitored centrally on account of the intricacies involved, but implementation of the measures would be dispersed.

An important element of the YKÄ project is the international CII and CIIP dimension, mainly associated with the European Union. These activities require continuous monitoring and a well-justified rationale set out by the public sector.

9.4.1.1 Proposals of the working group

The working group feels that it is important to further develop the work of the YKÄ project and to consider the forms that this could take. It is proposed that the ownership of this preparatory work should lie with the National Emergency Supply Organisation's information society cluster. The preparatory work should also include R&D activities in the YKÄ field.

Sufficient resources must be allocated for developing the YKÄ project.

9.5 Measures related to services and technology

9.5.1 Establishing a disruptive events register

9.5.1.1 Background

Critical infrastructures (CIs) are interdependent in many ways, and rely especially on ICT and energy supply. A number of international studies have sought to model these interdependencies. However, these studies are mainly theoretical and, almost without exception, lack real practical data. A register of disruptive events is needed that would be based on practical observations.

Such a register could operate by, for example, each CI sector listing the disruptive events occurring its own field, rated in an agreed manner, and figures would then compiled centrally on an automatic basis in a manner determined on the basis of modelling.

The register could be used in

1. *identifying critical CI components (e.g. ICT, energy)*
   a) critical component identification
   b) investigating the **real** origin and importance of disruptive events, and the cascading of disruptions from one CI to a second and third
   c) modelling and forecasting.
2. *developing quality*
   a) planning and allocation of ICT resources and organisation for usability and availability/contingency preparations
   b) supervision of ICT system service level agreements
   c) formulation of a status report (e.g. energy, ICT).

9.5.1.2 Proposals of the working group

A separate investigation should be made concerning the establishment of a disruptive events register as described above. The owner of the project would be the National Emergency Supply Organisation/information society cluster.

The estimated cost of the project is **EUR 400,000** annually.

9.6 Other proposed measures

9.6.1 Identity management

The value and verification of identities should constitute a critical infrastructure of its own. This should also be raised to the CII level in the European Union.

There must be a functioning, reliable, simple and sufficiently widely accepted identity recognition procedure in use within the information society.

9.6.1.1 Proposals of the working group

The working group proposes that identity management should form a separate concept in the field of critical infrastructure. To develop this concept further, attention should be focused on whether it can be linked up as part of some existing and sufficiently broad identity management development project.

The public sector must reserve sufficient resources for this.