POST & TELESTYRELSEN

DATE
4 July 2006

REPORT NUMBER
PTS-ER-2006:12
ISSN 1650-9862

FILE REFERENCE
06-3280

Strategy to improve Internet security in Sweden

Foreword

The National Post and Telecom Agency (PTS) has been assigned by the Government to submit proposals on a strategy to improve Internet security in Sweden. This report is PTS's proposal.

Today, the Internet is a tool and forum for most of us, both in working and everyday life. A characteristic feature of such an everyday infrastructure as the Internet has become may be that we take it and its functions for granted. It is noticed only when there are problems. It can be compared to our roads – we hardly think about them being there as long as they are whole and lead us to where we want to go. If, however, there are potholes in the carriageway or when roads are closed, forcing us to choose another route, we react.

The Internet is a more invisible infrastructure, where normally we do not even see the physical part of the infrastructure. The logical part of the Internet, such as, for example, a functional domain name system, is even more abstract to us as users of the Internet. However, it is just as important to achieve preparedness in order to be able to deal with any potholes in the infrastructure of the Internet, both the physical and the logical, as it is to continuously maintain our roads and other vital public infrastructures. The report 'Strategy to improve Internet security in Sweden' is directed at these issues.

Security issues concerning the Internet are a complex area – as is clearly shown by this report. Not only do they relate to issues of vulnerability and protection of the complex physical and logical levels of the infrastructure, but they also raise issues regarding the responsibility of the government, the operators and Internet users. This strategy points out the importance of addressing these issues now to ensure that the proposed vision, expressed in this report, becomes a reality – that in ten years the Internet will be secure, rapid and have high accessibility for everyone in Sweden.

This report was prepared by the following staff at PTS: Helena Bäckström, Frida Nilsson (Project Administrator), Kajsa Ritzén Frisell, Lars Hedensjö, Christoffer Karsberg (Project Manager), Anders Rafting, Björn Scharin (Acting Project Manager), Roland Svahn and Eric Wedin.

Stockholm, July 2006

Katarina Kämpe
Acting Director-General

Contents

Appendices

Summary

The National Post and Telecom Agency (PTS) has been assigned by the Government to submit proposals on a strategy to improve Internet security in Sweden. The aim of the strategy is to facilitate and clarify future work to secure Internet infrastructure. The strategy is directed at those parts of the infrastructure that are unique to the Internet. The point of departure for security within the Internet infrastructure is the providers' responsibility for networks and services on the basis of market requirements. Public commitment is based on there being demands that the market cannot satisfy. PTS is the sector authority for electronic communications, which also includes the Internet.

PTS's proposed vision is that in ten years' time, the Internet will be secure, rapid and have high accessibility for everyone in Sweden.

The goal of a strategy to improve Internet security in Sweden is to secure critical functions in the Internet infrastructure, which, if they were not maintained, would cause substantial disruption or interruption and in this way impede or prevent the use of the Internet for large groups of individual users or vital public businesses, authorities or organisations.

Trends and threat profiles:

- Society is becoming increasingly dependent on the Internet
- Society is becoming increasingly vulnerable to IT attacks
- Vulnerabilities in protocols and programs are increasingly being discovered
- Laws, legal proceedings and policies do not keep in pace with developments and globalisation
- Convergence in networks, terminals and services is continuing to increase
- Inadequate security in user environments constitutes an ever-increasing risk
- The competence gap is widening in pace with increased complexity
- Developments in the market involve increased internationalisation
- More wireless networks and services

Strategic positions adopted:

- The physical infrastructure of the Internet should be protected against accidents, disruption, wiretapping and manipulation of information during transmission
- Resistance to disruption in the domain name system should be increased
- Resistance to disruption to the exchange of traffic between Internet operators should be increased
- Users and buyers should be trained and informed to enhance security awareness
- The assumption of responsibility for user security should increase among Internet operators and the providers of software and equipment

- National awareness of Internet infrastructure should be promoted. This should be done in a broader context regarding information security. The comprehensive approach and coordination of research should be improved
- Swedish participation in international fora should be increased. This should be done in collaboration between the private and public sector
- Crisis management regarding the Internet infrastructure should be improved

The action plan comprises a number of measures within the framework of the strategic positions adopted, showing the allocation of responsibility, level of importance, timeframe and estimated cost for the respective measure.

The management plan lays down the administrative rules concerning how the strategic positions adopted and the action plan should be attended to. For example, the management plan contains guidelines regarding how often the action plan should be updated and which party is responsible for this.

1 PTS has been assigned by the Government to submit proposals on a strategy to improve Internet security in Sweden

PTS has been assigned by the Government to submit proposals on a strategy to improve Internet security in Sweden.

The aim of the strategy is to facilitate and clarify future work to secure the infrastructure of the Internet.

The strategy is directed at those parts of the infrastructure that are unique to the Internet as well as information, the situations relating to responsibilities, the development of knowledge, international work and crisis management.

The strategy has been prepared on the basis of the orientation of the IT Bill, previous surveys, trend analysis exercises, literature reviews and contacts with trendsetting people within the area.

The report describes the preconditions for the strategy, the current situation, proposals for a vision and objectives, trends and threat profiles, strategic positions adopted, measures including, among other things, division of responsibility, and also the management of the strategy.

1.1 The formal assignment from the Government

The National Post and Telecom Agency (PTS) has by its Terms of Reference for the budget year 2006[1] been given the following assignment by the Government:

"PTS shall provide proposals for a strategy to improve Internet security in Sweden in accordance with the orientation of the Government Bill 'From an IT policy for society to a policy for the IT society' (Government Bill 2004/05:175). This proposal shall also contain proposals for an action plan, division of responsibility and the management of the strategy. The proposal shall be reported to the Government (Ministry of Industry, Employment and Communications) no later than 31 July 2006."

1.2 The aim of the strategy is to facilitate and clarify future work to secure the infrastructure of the Internet

The aim of the strategy to improve Internet security in Sweden is to facilitate and clarify future work to secure the infrastructure of the Internet.

The Government has concluded[2] that the structure of the Internet is basically robust and has great opportunities of being able to function even under severe conditions and in the event of disruptions to telecommunications. Although the

[1] Terms of Reference for the budget year 2006 regarding the National Post and Telecom Agency, etc. within area of expenditure 22, Communications, and area of expenditure 6, Defence, and emergency preparedness against vulnerability (Riksdag Communications 2005/06:81 and 2005/06:82)

[2] In the Government Bill 'From an IT policy for society to a policy for the IT society', Government Bill 2004/05:175

Internet is basically a robust electronic communications system, it is not possible to resolve the security problems that apply to the Internet once and for all. It is therefore important to conduct long-term work in order to monitor, promote and, where appropriate, influence this security work.

1.3 Scope and delimitation of the strategy

A proposed strategy has been drawn up that describes the overall long-term approach to improve the Internet security in Sweden. The orientation of the strategy is in line with the Government Bill 'From an IT policy for society to a policy for the IT society' (Government Bill 2004/05:175). This means, among other things, that the strategy is directed at the physical and logical infrastructure.

The strategy is directed at those parts of the infrastructure that lie outside the 'transmission level', see Figure 1, and those parts of the infrastructure that are unique to the Internet, for example exchange points for Internet traffic and servers in the domain name system.

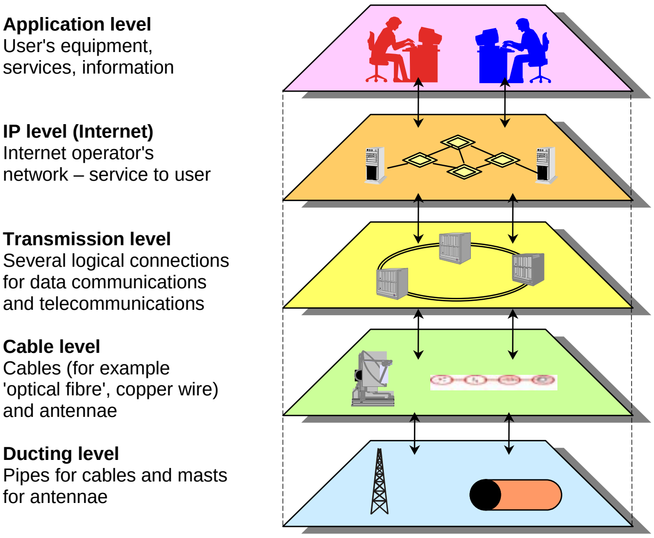
Application level
User's equipment, services, information
IP level (Internet)
Internet operator's network – service to user
Transmission level
Several logical connections for data communications and telecommunications
Cable level
Cables (for example 'optical fibre', copper wire) and antennae
Ducting level
Pipes for cables and masts for antennae

Figure 1: The levels of the Internet infrastructure[3]

PTS's strategy 'Robust electronic communications' deals with the overall infrastructure for electronic communications.[4] As the Internet also makes use of the infrastructure at the underlying levels, for example mobile masts and backbone networks, work within the framework of the robust electronic communications strategy that is conducted at these levels also affects the Swedish part of the Internet. The robust electronic communications strategy also takes into consideration the importance of robust time, among other things for frequencies in communication networks, traceability and realtime services such as IP-based telephony and IPTV.

[3] The IT Policy Strategy Group's working group for IT infrastructure and broadband, illustrations of the IT infrastructure.

[4] Strategy for robust electronic communications for the yers 2006 to 2008, National Post and Telecom Agency, 2006 (PTS-ER-2006:19)

According to the orientation of the IT Bill, this strategy also relates to information, development of knowledge and international work. In this context, 'information' means informing users so that they do not expose themselves to unnecessary risks and protect their environments so that they do not constitute a threat to the infrastructure of the Internet. However, the strategy does not cover measures that must be implemented by users to secure information that is transmitted via the Internet through, for example, encryption, secure identification, or measures to combat disruptive operations that do not constitute a direct threat to the Internet infrastructure.

In conjunction with the production of the strategy, PTS has identified a need for two further important areas in addition to those stated in the IT Bill: the responsibility for end-user security (see Section 5.4) and crisis management (see Section 5.7). These areas have been assessed to be of strategic importance for achieving the objective of the strategy (see Section 3.2).

'In Sweden' means that the strategy itself is limited to cover the nation. The Government has stated that this involves creating an information-base for and implementing measures that are feasible in Sweden. However, the strategy should be oriented towards taking into account international work. The Internet in Sweden is also dependent on several functions that are located abroad. Taken overall, the term 'in Sweden' may be said to constitute a restriction on the opportunities of Swedish stakeholders to react to and influence the area, taking into consideration the international situation.

1.4 Definition of the Internet and the Internet infrastructure

The Internet is a global, worldwide, logical network that has been established through the physical and logical linking of a large number of networks that are owned and managed by various private and government stakeholders. The lower levels of the network infrastructure hierarchy, for example fibre, copper, radio and transmission and which are used for Internet traffic, are also used in most cases for traffic for other applications, for example, fixed and mobile telephony, virtual private networks and various IP-based qualitative services. As networks and network equipment used for the Internet in this manner are shared with other services with guaranteed accessibility and quality according to contracts, the resources for the transmission of Internet traffic from termination point to termination point are variable and unpredictable.

All computers linked to the Internet are able to communicate with all other computers on the Internet by all using the IETF standard Internet Protocol (IP) for relay of traffic. IP technology means that the relayed traffic is split up into packets. The packets' route through the network (routing) is managed by special equipment, 'routers', and is based on a number of different criteria. For traffic *within* one operator's network, a routing decision is made on the basis of technical parameters, such as distance, delay and capacity. However, traffic exchanged *between* operators' networks, which occurs within public or private exchange points, is controlled by decisions based on the operator’s policy. A policy for the exchange of traffic with another operator may contain preferences for a particular route on the basis of a business contract, the type of traffic, load distribution, etc. External routing, that is to say the exchange of traffic between operators, is conducted in 'border routers' or 'border gateways', located at the extremity of the networks, and is effected in accordance with a global IETF standard, the Border Gateway Protocol (BGP).

A very important function within the infrastructure of the Internet is the domain name system (DNS). All computers on the Internet are identified with the aid of a unique IP address, which is used to relay packets on the Internet to the correct computer. For the sake of readability, an IP address is expressed as strings of numbers separated by full stops. The DNS translates these to a more user-friendly form, for example www.pts.se, so that you do not have to remember complex combinations of figures. These 'domain names' are easy to write and memorise when, for example, you want to link up to websites or send electronic mail.

1.5 Method to prepare the strategy

The IT Bill is the point of departure for the preparation of this strategy together with PTS's previous investigations[5] in the field and the knowledge that has been accumulated in conjunction with these assignments. PTS has also taken into account the Government Bill regarding 'Cooperation in crisis – for a more secure society'. PTS has supplemented the information-base with a review of the relevant literature in the field. During the initial phase, trend analysis work was conducted with the futures analysis business Kairos Future to identify trends and threats against the infrastructure of the Internet. Informal consultation with a number of trend-setting people in the field has taken place regarding visions, goals, trends and strategic positions adopted.

1.6 Reading instructions – structure of the strategy

The proposed strategy contained in this report basically comprises two parts: the strategic positions adopted (Chapter 5) and the action plan (Chapter 6). These two parts are linked by a management plan (Chapter 7), an administrative document which, among other things, regulates how the strategy should be practically managed.

Chapter 2 describes the investigations that have preceded this report, the allocation of public and private commitments, the international work and the structure of the current system of rules within this field.

Chapter 3 describes PTS's proposal for a vision for the Internet and objectives for the infrastructure of the Internet from a security perspective.

Chapter 4 deals with the trends and threat profiles that can be distinguished by PTS relating to the infrastructure of the Internet.

Chapter 5 presents the strategic positions adopted, that is to say how PTS considers that Sweden should work in the long-term in order to secure the infrastructure of the Internet.

[5] Internet in Sweden – Is it robust? (PTS-ER-2003:1), Den Internationella förvaltningen av Internet (The international management of the Internet) (PTS-ER-2003:23), Secure TLDs - Top Level Domains (PTS-ER-2004:19), Swedish strategy to secure the Internet infrastructure (PTS-ER-2005:7)

Chapter 6 presents PTS's proposals for an action plan, comprising a number of measures within the framework of the strategic positions adopted. This chapter opens with a summary of the measures with an allocation of responsibility, level of importance, timeframes and estimated cost for the respective measure. The action plan has a shorter life cycle than the strategic positions adopted and will consequently be updated more regularly.

Chapter 7 contains the management plan, which lists the administrative rules about how the strategic positions adopted and the action plan should be attended to. For example, the management plan contains guidelines about how often the action plan should be updated and who is responsible for this.

Appendix 1 contains explanations of abbreviations and terms.

Appendix 2 describes the international and Swedish organisations that are relevant to the work to improve Internet security.

Appendix 3 contains a discussion about the operators' responsibility for the security of their services.

Appendix 4 contains PTS's proposals to update the contact list of the CIIP Directory.[6]

[6] The CIIP Directory is a globally-recognised contact list for various security functions in various countries, which is managed by the UK authority responsible for network security, the National Infrastructure Security Co-ordination Centre (NISCC).

2 Preconditions and current situation

The Riksdag (Swedish Parliament) and Government have been considering the Internet and security within IT policy for a long time. The 'IT Bill' of 2004 proposed that the policy goal for the information society should be a sustainable society for all. Sub-objective three of three comprises accessibility and security and guides this report.

The success of the Internet results to a large extent from the initiatives and work of private organisations to develop functions for the Internet. The point of departure for security within the Internet infrastructure is the providers' responsibility for networks and services on the basis of market requirements. Public commitment is based on there being market imperfections that cannot be satisfied by the market.

As a sector authority, PTS is responsible for electronic communications, including the infrastructure of the Internet in Sweden.

2.1 The Riksdag and Government have for a long time emphasised IT issues where the Internet and security have been dealt with as part of the IT Policy

IT affects all sectors of society, and the core of the policy for the information society is those issues with a more general and cross-border significance.

What we now call the policy for the information society was often referred to in the early 1990s as the data policy. Government Bill 1984/85:220, 'Data policy', dealt with computer technology in working life, technical developments, education and personal privacy. The main orientation of Government Bill 1995/96:125, 'Measures to broaden and develop the utilisation of information technology', was education, the legal system and the provision of information resources to society. In the work with the predecessor to the current Government 'IT Bill' (Government Bill 1999/2000:86) 'An information society for all', the Government formulated the IT policy objective to be that Sweden should be the first country with an information society for all. Confidence, accessibility and competence in the use of IT were to be given priority.

Following the Government Bill 'An information society for all', an evaluation of the IT policy pursued over the years has been conducted by, among others, the National Financial Management Authority (ESV). This shows, where this applies to the IT infrastructure, that Sweden has come a long way in its work to establish a properly functioning IT infrastructure to cover the entire country. It also shows that Government initiatives have contributed to a good foundation for enterpreneurship in sparsely populated areas as well as in other regions.

It was proposed in the Government Bill 'From an IT policy for society to a policy for the IT society' (Government Bill 2004/05:175) that the objective of the policy for an information society should be a sustainable information society for all. The Riksdag approved the Government Bill on 25 January 2006. Prioritised tasks, or sub-objectives, include quality, sustainable growth, and accessibility and security.

The sub-objective 'quality' means that IT should contribute to an improved quality of life and to improving and simplifying everyday life for people and businesses. The sub-objective 'sustainable growth' means that IT should be used to promote sustainable growth. The sub-objective 'accessibility and security' involves making an effective and secure physical IT infrastructure with high transmission capacity available in all parts of the country, among other things to provide people with access to interactive public e-services.

Examples of initiatives that have been taken on the part of the Government are also referred to in the Bill. Among other things, preconditions were created for electronic communications between authorities and citizens, criminality and disreputable operations were combated, initiatives were effected to enhance information security, e.g. RAKEL, and for the provision of information resources, and the development of broadband was also promoted. Where this applies to RAKEL, for example, which is a radiocommunication network for, among others, the police, rescue and ambulance services, it is of importance for information security as it creates the preconditions for alternative communication routes.

In the Bill 'Cooperation in crisis – for a more secure society' (Government Bill 2005/06:133), the Government reported on its strategy for the security of society. This strategy aims to form a framework for society's overall work to improve security. The Government reported on, among other things, how the structure for crisis management should be improved by proposing that one authority should be given the multisectoral responsibility for crisis management. The Government Bill also explained the Government's view on an advanced strategy in the field of information security and a national programme for security research. The various interim reports of the 'Information Security Inquiry' have been taken into account in this connection.

PTS has previously conducted investigations regarding the security of the Internet infrastructure. The inquiry 'Internet in Sweden – is it robust?' tested how well the Internet works independently of functions abroad. Practical trials were conducted in conjunction with this inquiry regarding the important parts of the DNS for Sweden and a national exchange point for Internet traffic. The inquiry 'The international management of the Internet' describes how the management of the most important common resources is effected. The inquiry 'Secure TLDs - Top Level Domains' contains a survey of the functions in the operation and the administration that are important for good DNS security. The 'Swedish strategy to secure the Internet infrastructure' forms the basis of a large part of the orientation of the IT Bill as regards the security of the Internet infrastructure. In addition to these inquiries, which were conducted by PTS on the assignment of the Government, PTS has tested the name server operators' use of DNSSEC and has conducted a preliminary study with simulations of vulnerabilities in traffic exchange on the Internet.

Sweden's IT Incident Centre at PTS, Sitic, continuously monitors and publishes information about vulnerabilities in protocols and programs that are of importance to Internet infrastructure and its users. Sitic has also implemented a distributed intrusion detection system that publishes up-to-date information about attack attempts directly on Sitic's website. Sitic reacts to incidents on the basis of the information available, for example information about preventive measures is published. In addition to this, Sitic has implemented a distributed system 'The state of the Internet, to survey problems with the links between the major

Swedish Internet operators. These results have been published on Sitic's website. In order to further improve the operative activity, international contacts have been extended and improved, which facilitates more effective intervention in the event of an incident.

2.2 Public commitment

The general reasons that are referred to for public commitments within the various fields normally originate from economic theories regarding the Government's role in the social economy. The financial justification for public commitments is based to a large extent on the basis that there are a number of imperfections in the market that must be corrected through public stakeholder initiatives. These involve needs that the market cannot satisfy for various reasons. The armed forces, police and rescue services represent typical examples of collective utilities.

The point of departure for public commitment is that individuals, i.e. both private persons and businesses, have a fundamental responsibility to protect life and property and to implement preventive measures. This means that harmful effects may be reduced if certain fundamental security measures have already been taken by the party who is responsible for the operation. This means, in its turn, that it is important to encourage all stakeholders in society to implement the security measures that are possible and to exercise supervision of compliance with applicable provisions within the area.

Crisis management at a social level basically has the same character as the operations above and is dealt with more extensively in both 'Vulnerability and security in a new era' (Swedish Official Government Reports – SOU 2001:41, p. 76) and partly in Government Bill 2005/06:133. It is stated in these documents, among other things, that public involvement should, in the first instance, relate to those crisis situations where only the public bodies or those municipalities affected are able to assume the overall responsibility to manage, coordinate and prioritise the measures that need to be implemented in order to counter the crisis. However, this does not mean that public bodies should themselves take on a general financial responsibility for all of the measures that may be required in order to counter this kind of crisis situation.

The Government's commitment as regards the infrastructure of the Internet is based on the current overall IT policy objective that Sweden should be a sustainable information society for all. As a basis for this, there is a policy for the information society and this is effected through governmental responsibility for certain infrastructure, for the coordination of public resources and services, for legislation and also through support for development and new approaches.

The point of departure regarding security within the Internet infrastructure is that it is the service provider (the operator) who is in charge of the electronic communications that is responsible for his network and the quality of the service. This is done on the basis of the requirements imposed by the market, see Section 2.3.

The sub-objective that guides this report is in the first instance 'accessibility and security' (contained in Government Bill 2004/05:175), primarily as regards the objectives for the IT infrastructure.

The Government Bill emphasises the importance of facilitating new technology by maintaining technology neutrality as far as this is possible, in order to promote competition between the various kinds of networks and by attempting to make the existing infrastructure accessible to all (which has also represented a precondition for government support for the development of broadband networks). Openness and interoperability are also mentioned as being important so that access to services is not impeded by technical or commercial lock-ins or exclusions. Furthermore, information security, among other things regarding the function security of the Internet, is referred to as an important social issue as well as the Internet being organised and managed in a functional and reliable way and the security of the network being carefully monitored.

PTS is the sector authority for electronic communications, which also includes the Internet. It is PTS's vision that everyone in Sweden should have access to efficient, affordable and secure communications. PTS has a supervisory responsibility according to the Electronic Communications Act (2003:389 – EkomL). The point of departure for PTS's work with quality and security within electronic communications is to promote competition within the market, the procurement of security-enhancing measures, coordination between the government and industry, and also regulation and supervision.

Through The Electronic Communications Act, PTS can impose requirements on the Internet operators that their operations should satisfy reasonable requirements for good function and technical security. PTS can also work to make it easier for the consumer to obtain information about the quality of services. The work of PTS aims to make it easier for the user to make rational choices.

An Act on national top-level domains for Sweden on the Internet entered into force on 1 July 2006. The aim of the Act is to ensure that, through insight and supervision, the Government has the opportunity to ensure the efficient and secure administration of the top-level domain for Sweden. PTS is the supervisory authority under the Act. The management of risks linked to the Internet's functionality lies outside Sweden's control to a greater extent than is the case for other infrastructures. Nor is any individual country or organisation responsible for the security of the Internet, and this imposes demands on international coordination. Government influence does not inevitably ensure that the Internet is more reliable, but it may explain what responsibility rests upon those administering a top-level domain and can if necessary create a legal basis for being able to implement measures in the area.

In accordance with the above, PTS is procuring measures to enhance security and has recently published its Strategy for robust electronic communications for the years 2006 to 2008 (PTS-ER-2006:19).

In general, activities are implemented to manage the issues that have been identified as important within the various policy areas in the IT Bill. The Ministry of Justice has conducted a review regarding the system of rules that surround offences taking place in IT environments or with IT aids. The Swedish Emergency Management Agency (SEMA) is responsible for the development of RAKEL.

2.3 Private commitment

There are historic reasons for the private sector's large part in the work with the development, management and security of the Internet. In fact it was the American armed forces that started the development of a network for data traffic during the 1960s and 1970s, at that time in the first instance as an internal research project, but gradually the civil American authorities assumed the responsibility for supporting this research. Operators who were previously only engaged in offering fixed telephony and leased lines have been afforded greatly increased business opportunities through the Internet and there are currently tens of thousands of Internet operators around the world.

The success of the Internet depends to a great extent on the initiatives of private organisations for the development and standardisation of functions for the Internet. In 1998, the US Government transferred the management and the security protection of the Internet's critical intellectual resources, such as IP addresses and domain names, to the civil organisation ICANN. Blocks of IP addresses are allocated to five regional Internet registries, 'Regional Internet Registries' (RIR) by the organisation IANA, which, on the assignment of ICANN, looks after the operative aspects of their activities. The RIRs are private organisations funded by the membership fees of RIR customers, i.e. operators and large businesses. The blocks of IP addresses allocated by each RIR are then allocated in their turn to Local Internet Registries (LIR), which normally comprise the Internet operators. Then, these LIRs allocate addresses to the users and distributors of Internet communications. The RIRs are active within many areas regarding the implementation of new technology and they are endeavouring to establish good relations with industry. A significant part of the RIRs' operations involves disseminating knowledge about how traffic exchange between the Internet operators should be conducted in a robust and secure way. This is done, among other things, by arranging regular conferences and courses.

A considerable part of the responsibility for the security of the Internet infrastructure lies with the Internet operators who, within the framework of commercial feasilibility in a market that is subject to competition, implement measures to protect their respective parts of the infrastructure against disruptive or destructive incidents. Competition is a driving force for operators to maintain good preparedness to rectify disruptions and faults that arise. Since the telecom market was deregulated in 1992, Sweden has acquired a competitive market where security is a competition factor together with price and quality. It is thereby the individual operator who assumes the responsibility in their network, in the contract in relation to the end-user, for good functionality and technical security, together with the responsibility for network sustainability and accessibility. Rights and obligations, including function and security, are primarily regulated by contracts concluded between the end-user and the operator.

End-users are also responsible for the security of their environments and their behaviour on the Internet, and it is clear that one of the major threats to the infrastructure of the Internet is the inadequate security of end-user equipment and the capacity of this equipment to withstand attacks and intrusions together with inadequate security awareness on the part of users. This weak security means that end-user equipment can be exploited as a platform in coordinated attacks against the arbitrary functions of the infrastructure, for example the DNS or a service server for telephony.

Network equipment suppliers have recently made increased efforts to introduce security mechanisms, as have the dominant suppliers of software for end-user equipment.

Various private organisations play a very important role in society with regard to research, development and standardisation work on security and security related to the Internet and its infrastructure. Other organisations function as discussion fora and disseminators of knowledge by, for example, arranging courses and seminars. A large contribution is made here regarding the exchange and dissemination of information about security enhancement methods and tools to both producers and consumers of Internet services.

Appendix 2 includes a more comprehensive description of the organisations that play an important role in the work with the security of the Internet infrastructure.

2.4 International work for Internet infrastructure security

The function of the Internet lies outside national control to a greater extent than is the case for other infrastructures, and the responsibility is divided between many different stakeholders, both national and international.

The US Government has traditionally played a signficant role in the organisation and management of the Internet. During the latter part of the 1990s, this management started to be transferred from the US Government to ICANN. There are a number of advisory committees linked to ICANN in which industry and the public can participate. Sweden is active within the international advisory committee, the Governmental Advisory Committee (GAC). This committee has been assigned to support ICANN with advice on a number of issues relating to government affairs, in particular where the policy of ICANN could have implications for national laws or international treaties or agreements.

At a global level, there is cooperation on IT policy measures and positions to be adopted as a follow-up of the UN World Summit on the Information Society (WSIS).[7] The overall objective is to bridge the digital divide, and the single largest issue relates to the management of the Internet, primarily the management of certain of the Internet's critical resources, DNS and IP numbers. The management of these parts is critical from a security perspective and Sweden is actively working to ensure that the prevailing system shall not be jeopardised but is internationalised in the long term. Work is being carried out within the framework of several different international organisations and coordination is normally conducted through the EU. The Internet Governance Forum (IGF), where all stakeholders involved in the management of the Internet have an opportunity to discuss, among other things, global security-related issues, was born as a result of the work of WSIS.

Sweden is also active within the framework of the work conducted by the OECD as regards the production of reports with follow-ups and analyses of development within, among other things, the area of IT.

[7] The UN World Summit on the Information Society was conducted in two stages. The first was held in Geneva in 2003 and the second in Tunis in 2005. The implementation and follow-up of measures of importance for, among other things, the infrastructure of the Internet is in progress.

Several Swedes are participating in the international standardisation work. Work is primarily being conducted within the private sector through the Internet Engineering Task Force (IETF).

In 2004, the European Network and Information Security Agency (ENISA), which works with issues of network security and information security within the EU, was established. ENISA works, among other things, within the following areas:

- Risk analysis and risk management
- Monitoring standardisation
- Encouraging and initiating cooperation between incident management functions[8]
- Producing and encouraging the use of recommendations[9]
- Awareness enhancing measures

A Communications Committee, COCOM, and a European group of regulatory authorities, ERG, have been established within the EU to ensure that the system of rules for electronic communications will function as intended. Their aim, among other things, is to encourage cooperation and collaboration between the countries and the EU Commission. The EU Commission also has a high level advisory group, the High Level Group on Internet Governance (HLIG), with one representative from every Member State, which prepares EU positions regarding current issues concerning the global management of the Internet.

Article 23 of the Directive on universal services[10] imposes a requirement that the fixed telephony network is accessible in the event of a catastrophic network collapse. There is also an opportunity for Member States to implement further measures to protect public order and security in accordance with the Framework Directive.[11] Set against the background that the Swedish regulation should, among other things, be interpreted against the provisions in the applicable Directive, it may be of interest to study how a selection of other Member States has chosen to implement the provisions of the EU. One such comparative study[12] shows that most Member States have implemented Article 23 in some form regarding network integrity and also the provisions relating to good function and technical security. Finland in particular has more extensive technical regulations in the form of requirements regarding, among other things, maintenance, performance and electricity supply. Others require a risk and vulnerability analysis to be implemented by those operators affected. In certain cases, there are requirements for operators to inform users about the quality of the service.

[8] That is to say the Computer Emergency Response Team (CERT)

[9] Referred to as 'Best Practice'

[10] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services

[11] Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services

[12] Utredning and länderinformation rörande driftavbrott (Survey and country information concerning operational interruption and requirements for good technical function and security, etc.)

The 'i2010[13] – A European Information Society for growth and employment' is the initiative that replaces the former strategic orientation eEurope 2005. This initiative is the first to push through the renewed Lisbon Strategy. Security is an important part of the i2010 Initiative. The EU Commission has produced a communication[14] on a European strategy for a secure information society within the framework of i2010, which aims to update the 2001 Communication on Networks and Information Security. There are three areas of focus in order to counter security threats against the information society in Europe: specific security measures, the regulation of electronic communications and combatting IT crime. The forthcoming communication, the Strategy, involves a joint effort using all three of these focuses.

As regards national strategies, few countries have produced a corresponding strategy to the strategy that is presently proposed. However, there are a number of countries that have produced security strategies, which, among other things, include the area of the Internet, for example the Netherlands,[15] Canada,[16] Norway[17] and the USA.[18] There are also countries that have worked with these issues in conjunction with their e-government strategies, for example New Zealand.[19] The New Zealand strategy has been produced as a risk analysis where the various threats have been analysed together with the impact that they may have, among other things, directed at the infrastructure and confidence in the Internet. In the American strategy, emphasis has been placed on five prioritised areas: national incident management, national risk management, awareness enhancement measures, security of public administration and national and international cooperation. This strategy mentions, among other things, the need for security in BGP and DNS in conjunction with the infrastructure of the Internet.

2.5 System of rules relevant to Internet infrastructure

Chapter 1, Section 1 of The Electronic Communications Act states that the objective of the Act is, among other things, that private individuals, legal entities and authorities should have access to secure and efficient electronic communications. Secure communications means that communications should be operationally secure.

[13] COM(2005) 229 final, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the regions 'i2010 – A European Information Society for growth and employment'.

[14] COM(2006) 251 Communication from the Commission to the Council, The European Parliament, The European Economic and Social Committee and the Committee of the regions – A Strategy for a Secure Information Society – "Dialogue, partnership and empowerment"

[15] A safer Internet for all, KWINT (Kwetsbaarheid op Internet) an initiative of Ministry of Economic Affairs (NL), 2004

[16] Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection

[17] National strategy for information security – challenges, priorities and measures, Ministry of Defence, Ministry of Trade and Industry and Ministry of Justice and the Police (Norway), 2003

[18] The National Strategy to Secure Cyberspace, Department of Homeland Security (USA), 2003

[19] Trust and Security on the Internet - Keeping the Internet safe for e-government in New Zealand, November 2004

The supervisory authority may, according to Chapter 1, Section 8 of The Electronic Communications Act, issue regulations for the peacetime planning of the needs of the Total Defence for electronic communications. This right to issue regulations only applies to the need of the Total Defence for peacetime planning for situations of war, and not any general planning of stable and sustainable infrastructure solutions, even if these can of course generate synergy effects for peacetime planning.

According to Chapter 1, Section 9 of The Electronic Communications Act, the supervisory authority may order a party that provides electronic communications networks or electronic communications services that are of particular importance from the public perspective to take into account in a particular way the needs of the Total Defence for electronic communications during times of alert. This obligation thereby only applies to networks and services that are of particular importance and requires a decision by the supervisory authority. As this obligation should take into account the needs of the Total Defence, it may be difficult to implement more general measures under this provision to improve the infrastructure or stability among several networks or services. These obligations only arise when a decision or regulation has been issued.

Society's increased use and dependence on electronic communications reduce the tolerance for interruption and disruption. Chapter 5, Section 6 a of The Electronic Communications Act states that fundamental requirements are imposed on good function and technical security and on sustainability and accessibility in the event of extraordinary events during peacetime concerning all kinds of electronic communications. This provision deals with a fundamental level of operational security, a certain minimum of guaranteed security and covers all providers of public communication networks or public communications services. This provision has been made to ensure that users should be able to rely on communications functioning at a basic level.

The increased use of the Internet for critical social functions makes it increasingly important that the addressing system, the domain name system, which is used to translate domain names into IP addresses, is robust. On 1 July 2006, the National Top-level Domains for Sweden on the Internet Act (2006:24) entered into force. The Act provides the supervisory authority with the opportunity for insight and supervision regarding the administrator who controls the Swedish national top-level domain, .se. The scope of this supervision covers various areas, including monitoring that the operation is managed in a secure and efficient way and that databases that are fundamental to the operation are transferred to the supervisory authority. The Act does not cover the possibility of the supervisory authority replacing the administrator of the Swedish national top-level domain, but rather provides powers to order compliance with the authority's supervisory decision, backed up by a default fine.

3 Vision and goals for improved Internet security in Sweden

PTS's proposed vision is that in ten years the Internet will be secure, rapid and have high accessibility for everyone in Sweden.

The goal of a strategy to improve the security of the Internet in Sweden is to secure critical functions in the Internet infrastructure which, if they were not maintained, would cause substantial disruption or interruption and in this way impede or prevent Internet use for large groups of individual users or for vital public businesses, authorities or organisations.

3.1 The vision is that in ten years the Internet will be secure, rapid and have high accessibility

PTS's proposed vision is that in ten years the Internet will be secure, rapid and have high accessibility for everyone in Sweden.

The Internet contributes to the promotion of democracy, sustainable economic growth, increased competition and the consumers' position in the Swedish market. A secure, rapid and accessible Internet simplifies everyday life and improves the quality of life for citizens. Important everyday tasks that previously required a great deal of citizens' time can now be efficiently conducted over the Internet: communications with authorities, financial transactions, global, social and economic contacts and the purchase of goods and services. The Internet is used as a carrier for a long list of services such as telephony, web, radio and television. Individuals feel confident that Internet-based services and legal, financial and social interactions function securely and rapidly. Security is an obvious quality that is incorporated into communications networks, software and equipment, which makes the user's environment and communications secure.

3.2 The goal is to secure critical functions within the Internet infrastructure

The goal of a strategy to improve the security of the Internet in Sweden is to secure critical functions in the Internet infrastructure that, if not maintained, would cause substantial disruption or interruption and in this way impede or prevent the use of the Internet for large groups of individual users or for vital public businesses, authorities or organisations.

4 Trends and threat profiles affecting the infrastructure of the Internet

Trends and threat profiles:

- Society is becoming increasingly dependent on the Internet.
- Society is becoming increasingly vulnerable to IT attacks.
- The discovery of vulnerabilities in protocols and programs is increasing.
- Laws, legal proceedings and policies do not keep pace with developments in technology and globalisation.
- Convergence in networks, terminals and services is continuing to increase.
- Inadequate security in user environments constitutes an ever-increasing risk.
- The competence gap is widening in pace with the increase in complexity.
- Developments in the market involve increased internationalisation.
- More wireless networks and services.

This chapter describes a number of trends that PTS has identified through trend analysis work. The chapter does not describe what is aimed for, but is a description of possible developmental tendencies.

4.1 Society is becoming increasingly dependent on the Internet

Society is on the whole completely dependent on secure and functional communications over the Internet. The Internet is critical for industry and is an important driving force for the growth of Sweden. Many businesses base their entire operations on the Internet, not least within the financial sector, and the Internet is used, among other things, as infrastructure for controlling processes within industry. The public sector has also taken great strides towards greater use of the Internet and thereby also increased dependency on the Internet, among other things with substantial investments in automated self-services. A large proportion of the payments made by the public are conducted through bank services that are arranged via the Internet, with a strong concentration during the last five days of every month. For a large number of Swedes, the Internet comprises an important channel for both information and communication. With increasingly rapid Internet connections for households, the use of services requiring broadband is increasing and thereby the total quantity of traffic on the Internet is increasing rapidly.

This increased dependency has led to an increase in the number of governments that are interested in the international administration of the Internet, including the administration of the critical functions of the Internet.

4.2 Society is becoming increasingly vulnerable to IT attacks

As society becomes increasingly dependent on IT generally and the Internet in particular, it becomes increasingly interesting for organised criminality to attack society through systematic technical attacks instead of via more traditional means.

These attacks are no longer conducted only by individual hackers wishing to test their skills, but also by more organised groups whose aim is financial gain or who have ideological motives. This may result in demands for increased technical robustness and more stringent legislation and similarly increased demands on risk and vulnerability analyses. It may also result in increased demands by society for police surveillance and intelligence services.

4.3 The discovery of vulnerabilities in protocols and programs is increasing

There is an increasing interest in vulnerabilities. Increasing numbers of vulnerabilities have been discovered in pace with the creation and use of more protocols and programs. Certain vulnerabilities create more of a threat than others, depending upon which protocol or program has the vulnerability and also the kind of vulnerability involved. As a result of the exploitation of vulnerabilities, more people are demanding protocols and programs that are more secure.

Vulnerabilities can be created on different occasions and be of varying kinds, which in its turn can result in various forms of exploitation. Vulnerabilities can be created by the definition of how a protocol should function or when various programs introduce support for managing a protocol. Vulnerabilities can also be created in programs without deriving from the management of a protocol.

4.4 Laws, legal proceedings and policies do not keep pace with developments in technology and globalisation

Laws and legal proceedings often have a tendency to get out of step with rapid technological development and increased globalisation. Increased globalisation also imposes increased demands on the harmonisation and adaptation of the Swedish system of rules.

Legislation in Sweden does not necessarily mean that the measures implemented have such a great effect, as the Internet is borderless. Issues of jurisdiction and enforcement are of great importance in this context. Increasing globalisation in combination with the inadequate coordination of laws and policies can result in insecurity. This results in the user becoming increasingly dependent upon information about the quality of services in order to be able to make well-informed choices.

4.5 Convergence of networks, terminals and services is continuing to increase

A clear trend today is that services such as telephony, radio and television are converging to an increasing extent towards using the same physical infrastructure with traffic based on IP. Convergence is taking place within the infrastructure, services and user equipment. Converging physical networks reduce alternative traffic routes and can thereby increase vulnerability, for which reason certain categories of users should evaluate the risks and vulnerabilities that may exist and, for example, ask what would happen if the only route out does not function and consider having alternative traffic routes as a supplement.

Businesses and authorities who wish to have greater accessibility and security are welcoming the offers of the operators and are paying for technical measures that operators are making within the infrastructure in order to achieve increased security and accessibility. If an increasing proportion of resources within the infrastructure is used for profitable prioritised traffic, there is a risk that accessibility and quality will deteriorate for other users. Inadequate network neutrality can therefore be perceived as a threat by users who rely on their traffic not being discriminated against.

The Internet currently has a large number of users, and the most popular applications are e-mail, searching for and gathering information and interactive e-services like booking travel, Internet banking, file sharing and interactive games. A further application, which is advancing, is the making of calls over the Internet. As the use of voice communication (corresponding to traditional telephony), which uses the Internet for part of the transmission, is spreading primarily among private individuals, and is also substituting fixed telephony, this also further increases dependency on a functional Internet as disruptions and interruptions to the telephony service could constitute a threat to life and health for individual users. Telephony is making increasing use of critical resources within the infrastructure of the Internet, such as DNS and exchange points.

4.6 Inadequate security in user environments constitutes an ever-increasing risk

One of the greatest problems on the Internet today is inadequate security in the environments of individual Internet users. Computers that are insufficiently protected can be taken over and remotely controlled without the user's knowledge and thereby can be exploited as platforms for overload and disruptive attacks against, among other things, critical parts of the Internet infrastructure. This not only means a risk to the integrity or property of the individual user, but also to the general function of the Internet. A denial of service attack against critical parts of the Internet infrastructure can have consequences for users of the Internet throughout the world. This imposes demands that all Internet users assume a greater responsibility for their own behaviour on the Internet and security in their own environment. However, currently existing security problems are complex, and it is often necessary for users to have extensive understanding and knowledge in order for them to be able to act securely on the Internet and secure their own environment.

Another group of users are those organisations offering services via the Internet, for example Internet banks and other financial institutions, and who administer their own network connected to the Internet. Many problems can arise that may lead to the organisation becoming isolated from the Internet, which can have great consequences for society. An organisation that administers is own network in the form of its own AS (autonomous system) needs, for example, a good knowledge of BGP (Border Gateway Protocol) so that it does not by mistake create major problems for many other Internet users.

A third group of users are public administrations who are large users of the Internet. Public administration uses the Internet as a channel to automatically provide and gather information to and from central registers and systems. E-mail and web services are used as an essential communication medium between citizens and authorities in Sweden and internationally. As a major purchaser of various products and services for Internet use, the Government has a great opportunity to influence the market in conjunction with procurement procedures as regards the security of hardware, software and services. Security services are first offered when demand becomes so great that it justifies the suppliers' additional costs for development and implementation. Therefore, the Government, as well as the municipalities and county councils, also assumes an important role in this context. In order to be able to make full use of this strong position, it is necessary that the Government improves the competence of Government procurement officers and imposers of specifications as regards Internet security.

4.7 The competence gap is widening in pace with the increase in complexity

Dependence on the Internet is constantly increasing and, as a consequence of this, society is becoming increasingly susceptible to IT attacks. The development towards increased convergence and the use of new technologies with increasing intelligence within the terminals mean that users' terminals constitute higher risk and a risk that the competence gap will widen in pace with this complexity. The increased complexity of networks, services and user terminals means that only a few people have a clear overall picture.

One development that can entail a risk of increased complexity is the migration to IPv6. It is probable that the previous version, IPv4, will coexist with IPv6 within the foreseeable future by means of complex solutions. IPv6 has achieved great dissemination in certain parts of the world, for example in Japan, South Korea and India. In Sweden, IPv6 has only been used on a small scale so far, but it is likely that it will achieve increased use in the future.

The increased complexity is a consequence of increased functionality and security. This not only applies to the Internet, but in principle to all further developments. One example, in addition to IPv6, is Secure DNS, where the function increases not only security, but also complexity owing to key administration, etc.

4.8 Developments in the market involve increased internationalisation

The monitoring of the operation and the management of serious faults and disruptions to the network require staff with high skills that are available around the clock. For reasons of cost and efficiency, operators are endeavouring to automate and centralise the operations and the monitoring. As borders are becoming increasingly open, this means that many international operators may to a greater extent locate their operational centres abroad, but also conversely that they wish to locate central nodes, important for other countries, in Sweden.

Centralisation and remote control of traffic makes local, regional and international electronic communications increasingly dependent on functional links to a few nodes, nodes that are sometimes placed outside the borders of Sweden.

4.9 More wireless networks and services

Connection to the Internet nowadays also includes wireless forms of connection. These connections can be made both by local wireless networks and by mobile telephony networks. Wireless networks comprise both commercial services and open access points and can provide new opportunities for anonymity on the network. Wireless technologies are also increasingly becoming a supplement to the operators' backbone networks.

The development of technology has resulted in a number of wireless standards that offer the consumer mobile communications, a greater geographical mobility and an opportunity to be constantly connected via terminals of various kinds such as, among other things, laptop computers, mobile telephones and handheld computers, etc.

This trend means that new services are being developed, for example positioning, increased mobility and flexibility, and access to several connection technologies and an increasing number of options. The risks that can accompany increased wireless use, in comparison to fixed networks, include the sensitivity of communications to disruption and greater opportunities for wiretapping if the traffic is unprotected. The anonymity made possible by wireless networks is attractive to those who wish to attack services or the network.

5 The adoption of strategic positions to increase the security of the Internet infrastructure

Strategic positions adopted:

- The physical infrastructure of the Internet should be protected against accidents, disruption, wiretapping and manipulation of information during transmission.
- Resistance to disruption in the domain name system should be increased.
- Resistance to disruption to the exchange of traffic between Internet operators should be increased.
- Users and buyers should be trained and informed to enhance security awareness.
- The assumption of responsibility for user security should increase among Internet operators and providers of software and equipment.
- The national development of knowledge regarding the Internet infrastructure should be promoted. This should be done in a broader context regarding information security. The comprehensive approach and coordination of research should be developed.
- Swedish participation in international fora should be enhanced. This should be done in collaboration between the private and public sector.
- Crisis management regarding the Internet infrastructure should be developed.

5.1 Protect the Internet's physical infrastructure

The physical infrastructure of the Internet should be protected against accidents, disruption, wiretapping and manipulation of information during transmission.

It is very important to secure physical transmission (in networks, exchange points and other equipment) so that it functions continuously in accordance with operator requirements. Furthermore, measures must be taken against accidents, mistakes and against unauthorised people having the opportunity to disrupt functions within the infrastructure as well as wiretapping or altering information during transmission. Equipment for services that are important to society on the Internet should be physically protected against disruption and interruption.

The number of weak points must be minimised through analysis and measures in conjunction with rollout and development. There should, to the greatest extent possible, be redundancy for equipment and connections as the opportunities to protect the various parts of the network against accidents and physical attack are limited.

5.2 Protect the Internet's logical infrastructure

The logical infrastructure of the Internet comprises, among other things, a large number of protocols and programs. Many vulnerabilities have been identified within these and more will be discovered in the future. One ambition for a more secure Internet should be concentrated on identifying which protocols and programs are critical for the Internet's function. The protocols that this strategy focuses on are the protocols for the domain name system and traffic exchange between operators.

5.2.1 Increase resistance to disruption in the domain name system

Resistance to disruption in the domain name system should be increased.

An international hierarchy, the domain name system (DNS), is used for addressing on the Internet. Use of the Internet is made difficult or impossible without access to DNS.

DNS is the world's most distributed database, where the various parties look after their own part of the database. This local administration eases work to keep the database up-to-date at the same time as control functions are required to ensure that information that is entered is correct. It is relatively easy to falsify information and this can result in users ending up on the wrong website or e-mail being sent to the wrong destination. Nor can satisfactory DNS services be maintained in the event of overload of DNS that is caused by a party presenting the query submitting, with a malicious intent, repeated enquiries to DNS in large numbers. There are other ways in which the DNS service can be attacked, for example by attacking the name servers' connection to the Internet, or attacks can also be made against the name servers themselves. If the attack is aimed at knocking out the name servers’ capacity to answer enquiries, the attacker must knock out all capacity to achieve complete success. It is therefore important that the name servers for a zone have surplus capacity to be able to resist attacks, at the same time as there is a need to be able to actively filter out attacks of this kind. A party presenting a query to the Internet's Domain Name System (DNS) should be able to verify where the information comes from and that the information has not been altered en route.

5.2.2 Increase resistance to disruption to the exchange of traffic between Internet operators

Resistance to disruption to the exchange of traffic between Internet operators should be increased.

The very feature that makes the Internet the global network that it is, is that traffic can move between the networks of different operators. Large quantities of traffic exchange between various operators may mean that Internet traffic can be wrongly directed through a malicious action or mistake so that users do not reach the website they are looking for or e-mail does not arrive. There are weaknesses and vulnerabilities in the protocols that are used for traffic exchange, which can be exploited for attacks. Even if the protocols themselves are not attacked, denial of service attacks can have severe consequences, for example by overloading the router's process capacity, memory or connections so that the function is completely or partially disabled.

Moreover, there is some risk that false routers are connected at the operators' borders, and can act so that traffic is relayed to the wrong destination. There is currently considered to be only a relatively slight probability of a threat against border routers being carried out, but this may be expected to increase. In certain cases, the consequences can be very severe and can result in the Internet becoming more or less inaccessible. This area is complex and few have the competence to maliciously disrupt traffic between operators. However, mistakes and insiders can cause extensive disruptions. In order to counteract disruption to the exchange of traffic, Sweden should, above all else, work to ensure that improved recommendations are drawn up that optimise the use of existing solutions and, in the longer term, promote the introduction of methods for governing traffic exchange between the operators that make traceability possible.

An organisation, for example a business that communicates via the Internet through the technology of the Border Gateway Protocol, needs to have access to special competence to avoid inadequacies in management causing disruption to accessibility to the Internet for themselves and others.

5.3 Information for users and buyers to enhance security awareness

Users and buyers should be trained and informed to enhance security awareness.

Everyone who uses the Internet in some way is a part of the Internet and thereby influences security on the Internet. Internet users in Sweden are a very large and heterogeneous group including everyone from the home user to major companies or public authorities. In order to achieve a more secure Internet and to avoid Internet users unknowingly becoming a threat to Internet infrastructure, the knowledge and attitudes of users towards security on the Internet must be improved.

The security awareness of users will not play a decisive role for the infrastructure's security in the longer term. Security for the infrastructure should as far as possible be an integral part of the system and services, but it is necessary during a transitional period that individual Internet users also become security-conscious users.

In order to ensure a good level of protection, it is also important that major companies and public authorities have appropriate procurement skills, which is crucial so that the organisation, in its contractual situation with, for instance, operators, knows what requirements should be imposed. In order to promote a more secure Internet in Sweden, it is particularly important that the government is well-informed as a buyer, when determining specifications, and user of programs and equipment for Internet services.

5.4 Enhance assumption of responsibility for user security

The assumption of responsibility for user security should increase among Internet operators and providers of software and equipment.

The responsibility for security is divided between several different stakeholders, and users also of course have a responsibility for security in their environment and their behaviour on the Internet. However, it may be questioned why such a large part of the security responsibility currently lies with the users. Set against the background of the development in progress on the Internet and the nature of the Internet, with increasing processor power and intelligence in the terminals, Internet operators and providers of software and equipment should be given both a greater opportunity and a greater obligation to implement measures in various ways so as to limit the extensive risks for the user in the services and products that they supply.

It would be desirable to regulate obligations as little as possible and for development to be primarily conducted on a voluntary basis.

5.5 Promote national development of knowledge

The national development of knowledge regarding the Internet infrastructure should be promoted. This should be done in a broader context regarding information security. The comprehensive approach and coordination of research should be developed.

The increasing dependence of society on the Internet imposes demands for increased security. These demands mean that more resources are necessary for research about security on the Internet. The research that is currently in progress in Sweden within the field of information security is mainly focussed on academia or stakeholders in close cooperation with universities and colleges. Collaboration between business and the university world is conducted through, among other things, joint projects. There are also a number of good examples of research that is being conducted by industry with the aid of grants from organisations.

The funding of information security research in Sweden is spread over a number of different financiers, including public authorities, foundations, businesses and foreign stakeholders.

5.6 Further enhance Swedish participation in international work

Swedish participation in international fora should be enhanced. This should be done in collaboration between the private and public sector.

Owing to the borderless structure of the Internet, Internet security work is primarily conducted in the international arena within the framework of several different bodies, among others IETF, ICANN, CENTR, ETSI, UN, ITU, EU and OECD. The WSIS process has contributed by enhancing our knowledge and interest in policy issues, security issues and international standardisation, not least within developing countries. As regards standardisation, these bodies currently only represent the public interest to a limited extent.

Parts that are of substantial importance for the function of the Internet lie to a great extent outside Sweden's control, and work with standardisation and policy issues is divided among several different stakeholders, both nationally and internationally. Collaboration is required if security work relating to the Internet is to be successful and to achieve converged electronic communications in the long term where technology and the legal system function efficiently regardless of the service and national borders. In this way, a more secure Internet will be achieved in Sweden and Sweden will contribute to a more secure Internet from a global perspective as well as deal with IT incidents that arise without unacceptable disruption to society.

5.7 Develop crisis management regarding the Internet infrastructure

Crisis management regarding the Internet infrastructure should be developed.

Stakeholders who work with the Internet infrastructure have in most cases some form of crisis management routines for this infrastructure and the functions that are owned and managed by the respective stakeholder. However, there are no comprehensive, compiled and coordinated routines for mitigating the consequences in the event of serious disruption.

It is worth emphasising that the development of the capacity for crisis management should not be affected at the expense of preventive work with robustness which, by it being conducted, reduces the risk of crises and reduces interruption times in conjunction with the disruptions that nonetheless arise. However, there is reason to coordinate planning regarding how very extensive crises should be dealt with.

6 Action plan to implement the strategic positions adopted

PTS has prepared a draft action plan in order to realise the strategy that has been produced within the Government assignment 'Strategy to improve Internet security in Sweden'. This action plan comprises a number of measures within the framework of the strategic positions adopted.

The action plan is introduced with a summary of the measures showing the allocation of responsibility, level of importance, timeframe and estimated cost for the respective measure. Thereafter, a description of the respective measure is provided.

This chapter presents PTS's draft action plan with a number of measures within the framework of the strategic positions adopted, as described in Chapter 5.

The summary shown below shows all of the measures that are reported in this chapter.

The party responsible states the stakeholder(s) responsible for the measure in question being implemented and performed in the manner intended.

The *level of importance* states whether a measure is ongoing, planned or proposed. If it is proposed, it is weighted as important or very important. The precondition for the implementation of a proposed measure may be a decision at government level. The measures that PTS is prepared to implement involve a separate assignment and, when appropriate, funding may be required to implement the measure.

The *timeframe* states the period within which a measure is planned to be implemented: within one year, two years, three years or four years. Otherwise, it is expressed as continuous.

C*osts* state the estimated cost of the proposed measures, that is to say those that are not ongoing or planned. The estimation of cost has been made within the following intervals:

Low:	Below SEK 500 000
Medium:	SEK 500 000 – 1 500 000
High:	Above SEK 1 500 000

Costs for continuous measures are estimated on an annual basis.

Measure	Party responsible	Level of importance	Timeframe	Costs
6.1 Measures to protect the Internet's physical and logical infrastructure				
Produce recommendations to providers of content services for increased accessibility	PTS	Planned	< 2 years	-

Measure	Party responsible	Level of importance	Timeframe	Costs
Promote the use of DNSSEC in name servers	PTS	Planned	< 2 years	-
Produce recommendations for more secure traffic exchange between Internet operators	PTS	Ongoing	< 2 years	-
6.2 Measures for information to users				
Provide information about vulnerabilities	PTS/Sitic	Ongoing	Continuous	-
Develop advice for ordering Internet services	II Foundation	Ongoing	< 2 years	-
Coordinate and intensify information initiatives towards users	PTS	Very important	Continuous	High
Educate trainee teachers in Internet security	Universities and colleges	Important	< 2 years	High
Further develop PTS's website for Internet security	PTS	Important	< 2 years	Medium
6.3 Measures to enhance the assumption of responsibility for user security				
Work with specified requirements for good function and technical security	PTS	Ongoing	< 1 year	-
Follow up the Internet operators' functional capacity	PTS	Planned	< 2 years, thereafter continuous	-
Provide the Internet operators with a legal possibility of impeding the dissemination of harmful traffic	Government	Very important	< 2 years	Low
Investigate the requirements for increased responsibility for providers of software and equipment	Government	Very important	< 3 years	High
6.4 Measures to promote the improvement of knowledge				
Inform stakeholders about the financing sources available	Relevant authorities	Important	Continuous	Low
Work to ensure that funds are allocated within the framework of the EU's research programmes relating to the Internet infrastructure	Government	Important	Continuous	Low

Measure	Party responsible	Level of importance	Timeframe	Costs
6.5 Measures to enhance Swedish participation in international work				
Increase Swedish coordination and participation in international fora	PTS	Very important	Continuous	High
Clarify Swedish distribution of responsibility in conjunction with international contacts concerning security of the Internet infrastructure	Government	Very important	< 1 year	Low
Further develop operative international networks for incident management	PTS/Sitic	Ongoing	Continuous	-
Continued active participation in review of EU directives	Government	Ongoing	< 2 years	-
Increase participation in standardisation work	PTS	Important	Continuous	High
6.6 Measures to improve capacity for crisis management				
Increase exchange of experience, follow-up and learn from major disruptions	PTS/Sitic	Ongoing	Continuous	-
Produce a coordinated continuity plan for the Internet infrastructure in Sweden	PTS	Very important	< 4 years	High
Investigate alternative forms of communication for operations managers during crises	PTS	Important	< 4 years	Medium
Investigate alternative information channels from Sitic to users concerning the status of the Internet in conjunction with disruptions to the Internet	PTS/Sitic	Planned	< 2 years	-

6.1 Measures to protect the Internet's physical and logical infrastructure

This section describes the measures that affect those parts of the infrastructure that are unique to the Internet. Measures to protect the electronic communications infrastructure are in the main primarily dealt with by PTS's strategy Robust electronic communications – Strategy for the years 2006 to 2008.

6.1.1 Produce recommendations to providers of content services for increased accessibility

The providers of vital public services, for example Internet banking services and e-government services, should ensure that the breakdown of an individual cable does not result in the services becoming inaccessible to the surrounding world, for example by using duplicate Internet connections that are physically separate. A domain name holder should implement measures to enhance accessibility to name servers that refer to addresses on the Internet that should be reachable by the surrounding world, for example web servers and e-mail servers. Examples of such measures are that the domain name holder should always have at least two domain name servers for his domain, preferably with different operators.

PTS has previously participated in the production of the Swedish Urban Network Association's recommendations on robust nodes and robust networks. PTS also intends to conduct work to produce recommendations on, for example, the location of web servers in physically protected environments, secure traffic exchange for those with autonomous systems (AS) for duplicate Internet connections, routines to deal with operational disruptions, the management of denial of service attacks, and increased security when managing domain name servers.

6.1.2 Promote the use of DNSSEC in name servers

DNS information that is transferred using the current technical solutions cannot be guaranteed to be either correct or genuine, that is to say, can be said with certainty to come from an intended source. This can be ensured by using DNSSEC. After almost ten years of work producing a standardised solution for a more secure DNS, the Internet Engineering Task Force (IETF) has been able to approve DNSSEC as a standard,[20] paving the way for the introduction and the initiation of DNSSEC.

PTS will promote the opportunities for users to increase the security of the DNS service in various ways by supporting DNSSEC in name servers. In order to stimulate the introduction and use of DNSSEC, PTS intends to arrange seminars for Internet operators and those domain name holders with high security requirements. PTS also intends to inform the public about what DNSSEC protects against and, on the basis of the experience that PTS gains from the tests conducted, to provide easily accessible instructions about the measures and steps that an organisation must implement for the use to get started.

6.1.3 Produce recommendations for more secure traffic exchange between Internet operators

The fundamental weakness in traffic exchange between Internet operators is attributable to the inability to get a guarantee regarding who originally advertised a certain route through the network for a particular address area. As a consequence of this, neither the authenticity nor the correctness of the routing information can be checked. The IETF has worked for a number of years within a Routing Protocols Security Working Group to produce cryptographic methods to resolve these problems, though without yet being able to propose any standard. Even if a

[20] RFC 4033, 4034 and 4035

standard had existed by this time, there would be problems with a new standard as security would still be weak as long as it was not introduced by all operators. No one wants to be the first with an introduction and resistance is significant, as a security method of this kind involves increased complexity and an increased loading on routers and connections. Internet operators are commercial organisations where this kind of security is not yet part of their business plan and, in addition to this, will require increased financial and staff resources.

In order to conclude the advice and instructions, 'Best Common Practices', PTS is investigating vulnerabilities in the Internet border routing system in Sweden (the interdomain routing system) oriented towards physical experiments and simulations of attacks against the routing system. By analysing the results of these studies, a measurable profile of the consequences can be obtained as well as a basis for the assessment of impact on functions that are important to society. Our ambition is that the results shall contribute to clarifying the extent to which security problems can be resolved through the application of enhanced and updated 'Best Common Practices' in the operation.

6.2 Measures for information to users

6.2.1 Information about vulnerabilities

It is important for users of programs and protocols to monitor vulnerabilities of the programs and protocols that they are using. Vulnerabilities that affect their own systems can be more rapidly avoided if they are detected at an early stage. Sitic will continue to monitor and publish vulnerabilities that are important for organisations in society. Good planning and the well thought-out management of computer resources can sometimes, without the need for program corrections, reduce the risk of someone exploiting a vulnerability. Sitic will continue to publish preventive advice and demonstrate good examples in the preventive work. In addition to this, a public tool for searching and sorting vulnerability information will be published on Sitic's website. In this way, those interested in technical matters can be given a simple means of access to several sources within the area of vulnerability.

6.2.2 Develop advice for ordering Internet services

It is essential for large businesses and authorities to have appropriate procurement skills, as it is crucial for the organisation to know what requirements to impose in contractual relationships with, for instance, operators. PTS is prepared to contribute to the work that was started by the II Foundation on the modernisation and adaptation of the Recommendations that were produced by the IT Commission's 'General specification of Internet service'. The intention of the specification is to provide support to buyers when specifying requirements in conjunction with procurement and when drawing up service level agreements between service providers and their customers. The Government should also use the Recommendation to ensure that secure Internet services are available for public administration.

6.2.3 Coordinate and intensify information initiatives towards users

The Government should appoint a coordinating function for information initiatives on Internet security directed at households, schools, small and medium-sized businesses and organisations, etc. Young people are large consumers of the Internet and are inclined to take risks with downloading, etc., when surfing. Therefore, information work directed at youngsters about secure behaviour on the Internet is important to achieve a more secure Internet. PTS is prepared to assume a coordinating role and to intensify its information work. PTS also intends to support various initiatives in the future to enhance security awareness, such as, for example, the Surfa Lugnt (Surf Securely) campaign.[21]

6.2.4 Educate trainee teachers in Internet security

The awareness of users about and their attitudes towards security on the Internet must be improved in order to achieve a more secure Internet. In order to be able to reach users at an early stage, security aspects should constitute a natural part of education-related Internet use. This imposes requirements on the teachers who conduct educational activities, for which reason training as regards security on the Internet should form part of teacher college training courses, for example in a manner corresponding to the work of the Knowledge Foundation[22] on IT in teacher college training courses. PTS considers that this is important and anticipates that it will contribute to improving Internet security.

6.2.5 Further develop PTS's website for Internet security

PTS's website for Internet security contains information adapted for target groups about security on the Internet for households, small and medium-sized business and organisations, and also small and medium-size authorities.[23]

The website has a section called 'For the workplace', which is directed at small and medium-sized businesses, authorities and organisations. It contains more advanced information about, for example, system configuration and remote connections.

In order for the website to be an up-to-date source of information and contribute to the target group becoming more security-conscious and better buyers, it is important for the content to be developed in this respect and for it to be kept up-to-date on the basis of the target group's needs.

PTS will also implement, when the occasion arises, marketing of the website as a whole with the aid of editorial publicity, but has identified a need to supplement this with advertising campaigns on bought channels, primarily on the Internet.

6.3 Measures to enhance the assumption of responsibility for user security

6.3.1 Work with specified requirements for good function and technical security

PTS can impose requirements on Internet operators for their operations to satisfy reasonable requrements on good functionality and technical security by applying

[21] See http://www.surfalugnt.se

[22] IT in Schools (ITIS) and the Knowledge Foundation initiative for IT in teacher college training courses (10 June 2005)

[23] See http://www.pts.se/internetsakerhet

current legislation, for example Chapter 5, Section 6 a of the Electronic Communications Act (2003:389), and verification of compliance with the act.

PTS is also working to make it easier for users to get information about service quality. A well-informed user has greater opportunities to make conscious and soundly-based choices. Information about service quality is an important way to ensure that the consumer and other end-users have a greater opportunity to optimise their choice of operator, not only on the basis of price but also on the basis of the quality aspects.

6.3.2 Follow up the Internet operators' functional capacity

It is important that the functional capacity of Internet operators is actually maintained, thereby creating confidence in the Internet as a communication system. The suppliers who are responsible for operation of the infrastructure and the operators who provide services on the network have the primary responsibility of protecting the network against disruptive attacks. If competition in the market functions properly, quality requirements will in the first instance be defined by the interaction between the market stakeholders. If users are demanding certain qualities, such as reliability and security for the services that they request, services that are characterised by security and reliability can become a means of competing. PTS will monitor developments and the functional capacity that the Internet operators actually have.

6.3.3 Provide the Internet operators with a legal possibility of impeding the dissemination of harmful traffic

Internet operators should be given a legal opportunity to implement emergency measures, such as filtering electronic messages that jeopardise the system or the function of the network, such as denial of service attacks. Internet operators have, as The Electronic Communications Act is worded today, limited opportunities to implement emergency measures in respect of a customer's communication without their consent, for example in a situation where he has been adversely affected by Trojans or other programs that send mass e-mails or participate in the overload of web services. The same circumstances apply in cases where the customer is exposed to corresponding attacks himself. Such a legal opportunity should be combined with an information requirement about the measures that are implemented. The detailed proposed change of The Electronic Communications Act, which was submitted in PTS-ER 2005:7, Swedish strategy to secure the Internet infrastructure, is still valid (see Appendix 1 of PTS-ER 2005:7 under the heading 'Filtering issues').

A discussion concerning the operators' responsibility for security in their services is contained in Appendix 3.

6.3.4 Investigate the requirements for increased responsibility for providers of software and equipment

Taking into consideration ongoing developments with increasing processor power and intelligence in terminal equipment, together with the increased use of broadband for Internet connections, providers of software and equipment should, in addition to the Internet operators, be given a greater opportunity and obligation to limit the extensive risks for the user in the services and products that they supply. It is necessary to investigate further the preconditions for such opportunities and obligations. It is proposed that the Government, or the party appointed by the Government, should investigate the responsibility of software and equipment manufacturers for user security on the Internet. This survey should be conducted with participants from the sector.

6.4 Measures to promote the improvement of knowledge

6.4.1 Inform stakeholders about the financing sources available

The authorities that are involved should inform and encourage important research projects to seek money from the various funding sources available, for example, Vinnova, the Knowledge Foundation and the II Foundation. Furthermore, the relevant authorities should improve their information about the possibilities of applying for funding via the EU research programmes in the field.

6.4.2 Work to ensure that funds are allocated within the framework of the EU's research programmes relating to the Internet infrastructure

The Government should, in conjunction with the orientation discussions for how funds from the EU research programmes (primarily IST and ESRP)[24] should be allocated, prioritise and point out the importance of security in the Internet infrastructure and work to ensure that funds are allocated for these purposes to a greater extent than today.

6.5 Measures to enhance Swedish participation in international work

6.5.1 Increase Swedish coordination and participation in international fora

Swedish participation in international fora that are working with Internet security needs to be intensified, taking into consideration the borderlessness of the Internet and the functions that lie outside national control. The Government should appoint a coordinating function to ensure that joint guidelines are prepared for Swedish positions on issues that are of strategic importance for the security of the Internet, which should apply both nationally and internationally. This coordination responsibility should include consideration being taken to the work of the relevant organisations on Internet-related issues and to jointly discuss with the relevant stakeholders current issues in this international work. PTS should assume this role as the authority responsible for the electronic communications sector. PTS is prepared to coordinate Swedish participation and increase its participation in international fora, for example ENISA, FIRST, ICANN/GAC, Internet Governance Forum (IGF), OECD and ITU.

6.5.2 Clarify Swedish distribution of responsibility in conjunction with international contacts concerning security of the Internet infrastructure

More intense international cooperation regarding 'CIIP' (Critical Information Infrastructure Protection) is in progress with Swedish participation. Work is in progress within the International Watch & Warning Network (IWWN) and within other fora. Officers responsible for policy at ministry level are taking part in this

[24] Information Society Technologies and European Security Research Programme

international cooperation. Sweden does not currently have any representation at a corresponding level on policy matters. An international coordination document, known as the CIIP Directory, that includes the contact details of national bodies dealing with the CIIP, represents an important document for use in these contexts. The Government should indicate which stakeholders should constitute the international contact points for policy issues and other subject and expert areas. See PTS's proposal, contained in Appendix 4.

6.5.3 Further develop operative international networks for incident management

PTS intends to continue to further develop an operative international network through Sitic. Preconditions will be improved to effectively monitor vulnerabilities and active threats and to stop attacks through these international fora. Opportunities to continue to improve the security of the logical infrastructure will be increased through national and international forms of cooperation[25] for incident management functions (CERT).

6.5.4 Continue active participation in review of EU directives

Sweden is actively participating in the review of the EU Directives that form the basis of The Electronic Communications Act. It is important that the Government emphasises in this review work the matters considered to be of urgency in order to ensure that the work to secure the Internet infrastructure progresses.

6.5.5 Increase participation in standardisation work

International standards are gaining increasing importance for national growth. Harmonisation in respect of technical security requirements and operative security levels is a constantly ongoing and important process. Standardisation is naturally being pursued by the private sector in the first instance. The public sector is participating to a limited extent, which may mean that the public interest is not always sufficiently represented. PTS is prepared to increase its participation in this process at a comprehansive level.

6.6 Measures to improve capacity for crisis management

Collaboration between the various stakeholders, both from the public and private sector, is a fundamental precondition for functional crisis management. Collaboration must be prepared before a crisis arises to enable effective crisis management to be implemented.

[25] Important CERT cooperations include, among others,. FIRST (Forum of Incident Response and Security Teams), TF-CSIRT (Task Force - Collaboration of Security Incident Response Teams), EGC (European Government CERTs) and NCF (Nordiskt CERT - forum). Other organisations and forms of cooperation that are important to security work include ENISA (European Network Information Security Agency) and IWWN (International Watch and Warning).

6.6.1 Increase exchange of experience, follow-up and learn from major disruptions

An investigation of a major disruption is initially dealt with by the or those organisations that have been adversely affected. There may be a need for extra resources in conjunction with such a study in order to be able to interpret the course of events. Sitic has the capacity to contribute in the follow-up and also has an extensive network of contacts, which could possibly bring the person investigating the matter into contact with additional valuable people or information to further clarify the course of events.

An investigation of a disruption is often also valuable for others besides the organisation that has been adversely affected. Important experience from the disruption that is documented in the follow-up should be communicated to other organisations, primarily to those dealing with the same kind of IT environment. Sitic offers a function to exchange information regarding incidents. An important aspect of this function is that the party making the report and the organisation that has been adversely affected remain anonymous and that no information is passed on that could lead to the party making the report or the organisation that has been adversely affected being traced. According to a survey in the Hidden Statistics Inquiry,[26] which was conducted in 2005, it transpired that two out of three organisations were unaware of Sitic. In order to facilitate the reporting of incidents by organisations to Sitic, awareness of Sitic needs to increase. Sitic will continue to follow up major disruptions.

6.6.2 Produce a coordinated continuity plan for the Internet infrastructure in Sweden

The coordination of the Swedish reponse in the event of serious disruptions to the functions of the Internet should be improved. Crisis management should be conducted as a collaboration between the public sector, private sector and other organisations.

A continuity plan exists to reduce the damage that has been caused by interruptions. This continuity plan ensures that external resources can be allocated in conjunction with extensive disruptions. The cause of a disruption can, for example, be the result of a natural disaster, accident, equipment fault or malicious disruptions.

A 'principle of responsibility' applies in the event of crises in Sweden. The principle of responsibility means that the party who is normally responsible for a particular function in society also has this responsibility in the event of a crisis. The principle applies to both the public and the private sector.

This measure aims to produce a coordinated plan for serious events affecting the Internet. The intention of the plan is to cover major disruptions, i.e. disasters, that affect several stakeholders simultaneously. As the authority responsible for the sector, PTS is prepared to lead this activity. The stakeholders of most interest for this activity are major owners of the infrastructure and organisations that manage important logistic services. PTS has good experience of exercises within the sector

[26] Mörkertalsundersökningen 2005 – Svenska organisationer om IT-säkerhetsincidenter (Hidden statistics inquiry 2005 – Swedish organisations on IT security incidents) (File reference 05-9152/59)

and is prepared to test the plan together with the relevant stakeholders when the plan is approved.

6.6.3 Investigate alternative forms of communication for operations managers during crises

The parties maintaining the important parts of the Internet infrastructure need to have the opportunity, in the event of major disruptions or crises, to communicate regarding the disruption or crisis on a channel other than the channel adversely affected by the disruption so that they can jointly deal with the situation. PTS is prepared to investigate whether there is such a need.

6.6.4 Investigate alternative information channels from Sitic to users concerning the status of the Internet in conjunction with disruptions to the Internet

It may be necessary, in the event of a major interruption or disturbance within the infrastructure of the Internet, to provide users with information about the situation on a channel other than the one that has bee adversely affected by the disruption, for example the Internet. Sitic is currently continually providing information about security-related problems on the Internet, primarily via the Internet and in exceptional cases, depending upon the situation, via journalists and the media. PTS intends to investigate the need for information about disruptions or crises via channels other than the Internet, for example via radio or text television.

7 Plan for management of the strategy

The management plan prescribes the administrative rules concerning how the strategic positions adopted and the action plan should be managed. For example, the management plan contains guidelines about how often the action plan should be updated and who is responsible for this.

7.1 Aim of the management plan

PTS's draft management plan aims to prescribe the administrative rules concerning how the strategy, i.e. the strategic positions adopted and the action plan, should be revised and administered with the aim of keeping the strategy up-to-date.

The strategic positions adopted are probably relatively long-term, but may need to be updated in pace with developments.

The action plan comprises concrete measures within the framework of the strategic positions adopted and will function as a living document that may be amended when prioritisations are made or where specific areas need to be illustrated. The action plan shall be continuously followed up.

7.2 Decision makers, periodicity and implementation

Changes to the strategic positions adopted should be decided by the government. The strategic positions adopted are updated according to perceived needs and it is proposed that this is done through a special assignment by the Government to PTS.

The updating of the action plan is decided by PTS and is conducted by PTS every other year.

7.3 Feedback reports

The status of the implementation of the measures contained in the action plan is reported to the Government annually in conjunction with PTS's annual report.

Literature

A safer Internet for all, KWINT (Kwetsbaarheid op Internet) an initiative of Ministry of Economic Affairs (NL), 2004

Act (2002:833) on Exceptional Circumstances in Peacetime in Municipalities and County Councils

The Civil Defence Act (1994:1720)

COM(2005) 229 final, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the regions 'i2010 – A European Information Society for growth and employment'.

COM(2006) 251 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the regions – A Strategy for a Secure Information Society – 'Dialogue, partnership and empowerment'

Committee of Inquiry Terms of reference 2006:36 - Förbättrad samordning av utvecklingen av standarder och grundfunktioner inom IT-området (Improved coordination of the development of standards and basic functions within the field of IT)

Den internationella förvaltningen av Internet – vilka organisatoriska alternativ finns (The international management of the Internet – What organisational alternatives are there), National Post and Telecom Agency, 2003 (PTS-ER-2003:23)

Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services

Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services

Förordningen om åtgärder för fredstida krishantering och höjd beredskap (2002:472). (Measures for Peacetime Crises Management and Times of Alert Ordinance)

General specification of Internet service, the ICT Commission, 2000

Government Bill 1984/85:220 on Data Policy

Government Bill 1995/96:125 Measures to broaden and develop the utilisation of information technology

Government Bill 1999/2000:86 An information society for all.

Government Bill 2001/02:10 Continued Renewal of the Total Defence

Government Bill 2001/02:158 Samhällets säkerhet och beredskap (The security and emergency preparedness of society)

Government Bill 2002/03:110 The Electronic Communications, etc. Act

Government Bill 2004/05:175 From an IT policy for society to a policy for the information society.

Government Bill 2005/06:133 Cooperation in crisis – for a more secure society.

Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection

Internet in Sweden – is it robust? – Internets uppbyggnad och användning, Internets beroenden av funktioner utomlands (The structure and use of the Internet and the Internet's dependence on functions abroad), National Post and Telecom Agency, 2003 (PTS-ER-2003:1)

Internet-Draft Generic Threats to Routing Protocols A. Barbir, S. Murphy, Y. Yang, 2004

Ministry Publications Series 1994:53 Motiv för offentliga åtaganden (Reasons for general government commitments)

Ministry Publications Series 2006:1 A strategy for Sweden's security

Mörkertalsundersökningen 2005 – Svenska organisationer om IT-säkerhetsincidenter (Hidden Statistics Inquiry – Swedish organisations on IT security incidents), National Post and Telecom Agency, 2005 (File reference 05-9152/59)

National strategy for information security – challenges, priorities and measures, Ministry of Defence, Ministry of Trade and Industry and Ministry of Justice and the Police (Norway), 2003

The National Strategy to Secure Cyberspace, Department of Homeland Security (USA), 2003

RFC 1771 A Border Gateway Protocol 4, Y. Rehkter, 1995.

RFC 3833 Threat Analysis of the Domain Name System (DNS), D. Atkins, R Autein, 2004

RFC 4033 DNS Security Introduction and Requirements, R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, 2005

RFC 4034 Resource Records for the DNS Security Extensions, R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, 2005

RFC 4035 Protocol Modifications for the DNS Security Extensions, R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, 2005

RFC 4271 A Border Gateway Protocol 4, Y. Rehkter, T. Li, S. Hares, 2006.

Robust networks– recommendations – laying robust networks. Ducting, cables and connection points. The Swedish Urban Network Association (*Svenska stadsnätföreningen*), 2005.

Robust nodes – recommendations – Design of physical security for nodes in open neutral broadband networks, The Swedish Urban Network Association (*Svenska stadsnätföreningen*), 2004

Secure Operation of Top Level Domains – What functions are vital to ensure a high degree of security in the domain name system, National Post and Telecom Agency, 2004 (PTS-ER-2004:19)

Security Information to Internet Users – final report, National Post and Telecom Agency, 2005 (PTS-ER-2005:33)

Strategy for robust electronic communications for the years 2006 to 2008, National Post and Telecom Agency, 2006 (PTS-ER-2006:19)

Swedish Official Government Reports – SOU 2001:41 Vulnerability and security in a new era

Swedish Official Government Reports – SOU 2003:27 Informationssäkerhetsutredningen – delrapport 1 om signalskydd (Information security Inquiry – Preliminary report 1 on signal protection)

Swedish Official Government Reports – SOU 2003:59 Toppdomän för Sverige (Top-level domains for Sweden)

Swedish Official Government Reports – SOU 2004:32 Informationssäkerhet i Sverige och internationellt – en översikt (Information security in Sweden and internationally – an overview)

Swedish Official Government Reports – SOU 2005:42 Secure information

Swedish Official Government Reports – SOU 2005:71 Information security policy – organisational consequences

Swedish strategy to secure the Internet infrastructure, National Post and Telecom Agency, 2005 (PTS-ER-2005:7)

Terms of Reference for the budget year 2006 regarding the National Post and Telecom Agency, etc. within area of expenditure 22, Communications, and area of expenditure 6, Defence, and emergency preparedness against vulnerability (Riksdag Communications 2005/06:81 and 2005/06:82)

Top-level domains for Sweden on the Internet Act (2006:24)

Trust and Security on the Internet - Keeping the Internet safe for e-government in New Zealand, November 2004

Utredning och länderinformation rörande driftavbrott (Survey and country information concerning operational interruption and requirements for good technical function and security, etc.), Survey by Bird & Bird Advokat HB on the assignment of the National Post and Telecom Agency, 2005

Vilket informationsbehov har Internetanvändare vid störningar i Internettrafiken? (What information needs do Internet users have in the event of disruptions to Internet traffic?), National Post and Telecom Agency, 2003 (PTS-ER-2003:34)

Appendix 1 – Abbreviations and concepts

ARN National Board for Consumer Complaints (*Allmänna reklamationsnämnden*)

AS Autonomous systems

BGP Border Gateway Protocol

CERT Computer Emergency Response Team: An international generic term for organisations dealing with and preventing the occurrence of IT incidents in the form of security problems. They are usually found, for example, within organisations with large IT environments, at Internet operators or within the government to deal with IT incidents at a national level.

CIIP Critical Information Infrastructure Protection. Equipment, technical systems and communication routes that may be deemed critical for the functioning of society.

CIIP Directory The aim of the CIIP Directory is that it should constitute a reference document with national contacts within the CIIP area. This document was initiated at the G8 'CIIP Experts Conference' in March 2003 and is administered by the British National Infrastructure Security Co-ordination Centre, NISCC. The CIIP Directory currently contains government contact points for 18 countries.

DNS Domain Name System

DNSCHECK DNSCHECK is a tool that has been produced by the II Foundation to enable a domain name holder to check whether his .se domain is correctly configured.

DNSSEC The IETF standard DNS Security Extensions (DNSSEC) provides the user with the possibility of cryptographically verifying whether the DNS lookup is correct and in this way be able to detect and avert an attack.

Domain A level in the domain name hierarchy.

Domain name A name that corresponds to an IP address, for example pts.se.

DoS attack Denial of Service attack: An attack that impedes accessibility, usually executed through intentional overloading.

EGC European Government CERTs, an informal group comprising European sister organisations, whose aim is to develop efficient collaboration within the area of information security.

ENISA European Network and Information Security Agency.

ESPR ESPR (European Security Research Programme) is a European research programme within the framework of the seventh framework programme oriented towards security research.

ETSI European Telecommunications Standards Institute. ETSI is an independent not-for-profit organisation. ETSI is responsible for information and telecommunications standardisations within Europe.

FIRST Forum of Incident Response and Security Teams (FIRST) is an international forum for CSIRTs who jointly deal with IT security incidents and encourage preventative measures within this area.

FM-CERT The Swedish Armed Forces Computer Emergency Response Team.

FMV Defence Materiel Administration (*Försvarets materielverk*)

FMV CSEC An operational branch within the Defence Material Administration, the Swedish Certification Body for IT Security.

FRA National Defence Radio Establishment (*Försvarets radioanstalt*)

GAC Governmental Advisory Committee: An advisory body to ICANN with national representatives who contribute with their respective countries' view on DNS.

ICANN Internet Corporation for Assigned names and Numbers: Is responsible, among other things, for policies concerning the allocation of IP numbers and domain names.

IETF Internet Engineering Task Force: International standardisation body for the internet protocols.

IP (Internet Protocol) communications protocol that deals with the addressing, routing and transmission of IP packets on the Internet on what is known as the network level.

IP address Numerical address for a computer or other equipment in an IP network. This address is normally written as four whole numbers separated by full stops (for example 123.45.67.8)

IPv4 Internet Protocol, version 4 (32-bit IP addresses).

IPv6 Internet Protocol, version 6 (128-bit IP addresses).

IST Information Society Technologies. The EU's framework programme for research and technical development regulates how the IST should prioritise its research activities. The aim in this area is for the European general public to gain access to the services of the information society.

ITU International Telecommunications Union: A collaborating body within the UN for telecommunications issues.

IWWN International Watch and Warning (IWWN) comprises 17 Member States and aims to improve international coordination of common interests within the area of Watch & Warning.

KBM Swedish Emergency Management Agency (*Krisberedskapsmyndigheten*)

KK-stiftelsen The Knowledge Foundation (*Stiftelsen för kunskaps and kompetensutveckling*)

NCF Nordic CERT Forum (NCF) is a regional forum for government and academic CSIRTs in the Nordic countries.

OECD Organisation for Economic Co-operation and Development is a collaborating body for developed western industrial countries. The OECD was formed in 1960 with the aim of promoting economic development and growth in the Member States.

Pharming Pharming is an advanced form of phishing. A perpetrator can arbitrarily redirect a visitor from one website to another by manipulating the translation between the IP address and the domain name.

Phishing A kind of spam mail that aims to gather sensitive information from Internet users.

RAKEL Radiocommunications for Effective Management (*Radiokommunikation för effektiv ledning*)

RPS National Police Board (*Rikspolisstyrelsen*)

Sitic Sweden's IT incident centre (Sitic) is an independent organisation that supports society in the event of threats to IT security. Sitic is part of the National Post and Telecom Agency (PTS). Sitic assesses and provides information on an ongoing basis about threats to IT security that risk affecting authorities, county councils, municipalities and businesses. Sitic provides a function for information exchange in respect of IT incidents between organisations in society and disseminates information to society about new problems that can disrupt IT systems. Sitic also provides information and advice about preventive measures and compiles and issues statistics as a basis for continual improvements in preventive work.

SLA (Service Level Agreement) a service guarantee in the form of an agreement where, for example, a business providing an Internet service undertakes to maintain a certain quality of its service with an obligation to pay compensation if the service provider does not satisfy the contractual requirements.

Spam Spam is the same as junk mail; undesired e-mail messages.

SOTI The area of cooperation 'technical infrastructure'; an area of collaboration for authorities within, among other things, electronic communications, power and water supplies for the planning and coordination of emergency preparedness measures.

S-BGP The sender of BGP information can be validated through the Secure Border Gateway Protocol (S-BGP), produced by BBN Technologies (i.e. there is no standard), at the same time as unauthorised changes of information cannot be made without being detected.

S-BIT The coordination office for crime-related IT incidents; coordination function between the National Criminal Police and the Swedish Security Service (SÄPO).

TF-CSIRT Task Force – Collaboration of Security Incident Response Teams. TF-CSIRT endeavours to promote cooperation between CSIRTs (Computer Security Incident Response Teams) in Europe. Its main objectives involve creating a forum for the exchange of experiences and knowledge, establishing pilot services for European CSIRTs and establishing new CSIRTs. TF-CSIRT has been established to support cooperation between CSIRTs in Europe.

Top-level domain Level in the DNS hierarchy that lies immediately below the highest level, that is to say root.

WSIS World Summit on the Information Society

Appendix 2 – Organisations that are relevant to Internet security

The following section first describes the most important international organisations that, in their work to administer, develop and standardise the Internet, allocate a large proportion of their resources to security work. Thereafter follows a description of those Swedish organisations of importance for Internet-related security work.

International organisations

ICANN

In 1998, a white paper from the USA government established a private foundation called the Internet Corporation for Assigned Names and Numbers, (ICANN) in order to meet the worldwide demand for a civil organisation to administer the names and addresses, etc. of the Internet. ICANN is a private sector, non-profit corporation based in Los Angeles. Its role is to be responsible for the administration and security of the domain name system (DNS), the allocation of address space in the Internet Protocol, the coordination of new parameters for the Internet Protocol as well as being responsible for the Internet's root server system. A number of advisory committees help ICANN by providing it with information. The most important of these committees are the Governmental Advisory Committee (GAC), whose members are government representatives, the Security and Stability Advisory Committee (SSAC), where experts work with security issues concerning DNS and routing, and the Root Server System Advisory Committee (RSSAC) that works with security regarding DNS root servers. The committees themselves are not entitled to represent ICANN. The members of ICANN's board are elected by the various support groups and advisory committees. The ICANN board consists of 15 voting members, including the organisation's president, and six observers, non-voting 'liaisons'.

ISOC

The Internet Society (ISOC) is an international organisation working to enhance the availability and utility of the Internet. ISOC, which was founded in 1992, is a non-profit society formally based in the USA. In pace with the development of the Society, national sub-branches, 'Chapters', have been established in many countries. ISOC-SE is the Swedish sub-branch. ISOC's goals are a stable and flexible expansion of the Internet, access to the Internet for everyone, open, unrestricted and ethical use of the Internet and increased knowledge about the Internet among decision makers, in industry, within organisations and among individuals. ISOC is working both with the technologies of the Internet and with its effects on society. Development of the Internet architecture and the technical standards for the network forms an important part of this technical work. ISOC is, among other things, the organisation home for the groups responsible for the development of Internet standards, for example IETF. ISOC also attends to research and training, as well as the worldwide dissemination of information. ISOC makes a special contribution by supporting the spread of the Internet in developing countries, among other things through training and other support projects. The board of ISOC comprises people from all over the world. Many of them have made great contributions to the development of the Internet and Internet technology.

IETF

Standardised methods and protocols are a prerequisite for functioning communications over the Internet. Traditionally, the Internet Engineering Task Force (IETF) has carried out the work to produce these, which has been described as a process of drawing up joint documents rather than building up an organisation[27]. Among other things, the IETF arranges discussions about the various issues concerning the Internet and has been organised so that all interested parties can participate in the work of the organisation. Standardisation documents for the Internet – 'RFCs' (Request for Comments) – are drawn up by working groups. These working groups are primarily in the form of mailing lists and can be joined by anybody. Each mailing list has its own rules and aim, which are laid down when the group is set up. RFCs vary in importance as shown by their designation in the document, such as 'full standard', 'best current practice', 'experimental' or 'informational'. There are approxiately 400 RFCs.

The IETF has been publishing various standards in different subjects since the end of the 1960s and the documents cover a large number of issues. Among others, there are RFCs dealing with the use of domain names, server operations and recommendations in respect of operational security. The group is disbanded when the aim of the group is achieved, which often means the publication of an RFC. The IETF also arranges conferences where participants meet face to face. However, decisions made on these occasions are not more important than those made on the mailing lists, in fact rather the opposite. Decisions are made by a 'rough consensus', that is to say practically all participants on the mailing list should give their consent or at least not oppose a decision. The IETF has a secretariat with employees who primarily arrange conferences and maintain a register of 'Internet Drafts', that is to say proposals for RFCs.

IAB

The Internet Architecture Board (IAB) is ISOC's advisory body for technical issues. The IAB has been commissioned to attend to the overall development of the Internet and is not unlike a coordinator for the various rather autonomous groups and processes aiming to maintain and develop the Internet's technical systems. The IAB draws up agreements with, for example, RFC Editor and IANA about the information these are responsible for, and is also an 'appeals body' if somebody considers that there is something wrong with the IETF process. The IAB appoints representatives for IESG and IRTF is its direct subsidiary body.

[27] See 'Vem gör vad i Internetsverige? Nätet och aktörerna (Who does what on the Internet in Sweden? The network and stakeholders), ISOC-SE

The members of IAB are formally elected by ISOC, but in practice the same process is used as in the election of IESG members, NomCom.

IRTF

Where the IETF attends to application protocols and resolving specific problems, the task for 'The Internet Research Task' (IRTF) is repsonsibility for long-term basic research within the area of the Internet. The work is carried out by Research Groups (RG). The IRTF reports to the IAB.

IESG

The Internet Engineering Steering Group (IESG) can be said to be IETF's management team. Its main task is to examine how the working groups have reached their conclusions and other RFC proposals. Objections from two of the group members are enough to stop an RFC proposal. A very important task of the IESG is to ensure that the various standards do not conflict. The IESG comprises 'Area Directors' (AD). Each one is elected for a period of two years with responsibility for a particular subject field, for example security or routing. At present, there are eight fields. Area Directors are formally elected by the IAB, but in practice the IAB always approves the proposal of the special election committee, NomCom.

RFC Editor

The RFC Editor is one or more people who, in collaboration with the IESG, have the main function of determining which Internet Drafts should become RFCs. The RFC Editor should also ensure that all RFCs are set up in a uniform manner and that there is a reliable archive of all of the RFCs. The RFC Editor is commissioned by the IAB. At present, the IAB has a contract with the ISI Department of the University of Southern California (USC) for this assignment.

IANA

It is the task of the Internet Assigned Numbers Authority (IANA) to keep a check on all of the parameters and values that are needed for different Internet standards. The most important is the allocation of IP numbers and domain names. The IANA is a technical function within the organisation ICANN, which is now IANA's client. However, the technical management of the Internet Protocol is left to the IETF/IESG/IAB. A description of what IANA is working on can be found in RFCs and a MoU (Memorandum of Understanding) between ICANN and IETF.

Verisign

The private security company, Verisign, which among other things is a publisher of certificates for digital signatures, has an important role as regards DNS security. Through a contract with the US Department of Commerce, they are responsible for the operational management of the master name server for the most critical part of the DNS, namely the root zone file which includes all of the top-level domains, for example .se and .com. Updates for the root zone files are distributed from Verisign to the thirteen root server bodies for root.

In 1999, Verisign (previously NSI or Network Solutions) was divided into two different functions. One part is Network Solutions, a registrar where you can register domain names in many top-level domains, the other is Verisign Global Registry System (VGRS), which manages the DNS for '.com' and '.net'.

RIPE

Réseaux IP Européens (RIPE) is a collaborative organisation for Internet operators in Europe, other parts of the former Soviet Union, western parts of Asia up to and including Afghanistan, and Africa down to around the equator. RIPE aims to coordinate work so that the European part of the Internet functions effectively. Tbe bulk of the work is done in various working groups. An important part of RIPE's operation is to create instructions for the regional registry, RIPE NCC, which exists within RIPE's area. Other registries can be found in North America (ARIN), South America (LACNIC and Asia (APNIC). A fifth has recently been established in Africa (AFRINIC). They are given responsibility by IANA for allocating IP numbers in their areas. RIPE NCC allocates just over 1 000 local registries, which in their turn give IP numbers to end-users.

World Wide Web Consortium (W3C)

The W3C is an international body with the aim of developing the World Wide Web. One university in the USA, one in Europe and one in Japan act as joint hosts for the consortium. Timothy Berners-Lee, the creator of the web, is the Director of the W3C. The W3C was founded in 1994 and is thereby considerably younger than the IETF. The W3C is working on developing joint protocols for the web and has an important role as an archive of specifications of, for example, all of the different versions of the web's code language HTML and its various commands. The W3C manages, for example, XML, SOAP and thereby the foundation for many web services. The W3C also develops software to demonstrate the new opportunities that are available on the web. In addition to this, the consortium organises meetings and conferences. Only organisations and businesses can become members of the W3C. The consortium is careful to remain neutral between the various businesses and organisations.

International Telecommunication Union (ITU)

The ITU is an international organisation for the global coordination of telecommunication networks and services. The ITU was founded in 1865 and has been the UN's specialised agency within the field of telecommunications since 1947. The organisation is based in Geneva, Switzerland. One of the ITU's tasks, among others, is to maintain and extend international cooperation for the rational use of telecommunications of all kinds and to promote technical development within the field.

The main work of the ITU is divided into three different sectors:

The Radiocommunication Sector (ITU-R) mainly works to coordinate the radio spectrum and wireless services.

The Development Sector (ITU-D) is focussed on encouraging the use and dissemination of telecommunications networks and services in developing countries.

The Telecommunication Standardization Sector (ITU-T) is working to develop standards within the telecommunications field. There are currently approximately 2 800 Recommendations.

Furthermore, the ITU is responsible for the allocation of country codes (CC) for countries, geographical areas and for global telecommunications services. These allocations follow the principles referred to in Recommendation E.164, published by ITU-T. The organisation is governed by a constitution, a convention administrative council. The Plenipotentiary Conference (PP) is the supreme authority according to Article 7 of the Constitution. According to Article 3 of the Constitution, the Member States take on the duties of the Constitution and the Convention. In order to take part in the work of the ITU-T, it is necessary to be a member. There are three different categories of members:

- Member States – the same as the States that contribute work with the UN, currently amounting to 191.
- Sector Members – primarily made up of businesses from private industry, for example telecom operators and equipment manufacturers.
- Associates – Small companies that are only entitled to take part in the work of a selected single work group.

Over 450 private businesses are members of the ITU. Technical work within the ITU is carried out by thirteen study groups.

Swedish organisations

The Internet Infrastructure Foundation (II Foundation or IIS)

The II Foundation has two main functions: first, to manage and develop the Internet's Swedish top-level domain, .se; second, to promote the development of the Internet infrastructure in Sweden. The II Foundation was founded in 1997 on the initiative of ISOC-SE for this purpose, as the .se domain had started to grow more and more rapidly and needed a stable organisation that could take long-term responsibility. At the same time, the Foundation launched the wholly-owned operations company NIC-SE to look after the daily operational and administrative management of .se. There was a reorganisation in 2006 when NIC-SE was dissolved as a private company and in conjunction with this the II Foundation took over the operational management of the .se domain. Since 2004, the II Foundation has been annually giving out grants to selected natural or legal persons in order to promote initiatives within Internet security and development and support projects that do not normally receive money from research councils, research foundations and other research funding bodies.

ISOC-SE

The Swedish sub-branch of the Internet Society (ISOC-SE) is a not-for-profit association, whose aim is to develop the Internet. It is the Swedish branch of the Internet Society (ISOC), which is an international not-for-profit association working both with the network infrastructure and with issues about how the Internet influences working life, school and leisure time. Members of the ISOC-SE can be either individuals or organisations. The aim of the Society is to disseminate information about the Internet's function, technologies and regulations as well as acting as a forum where members can exchange experiences with each other and with non-members. Other main tasks are to act as a consultation body and to actively monitor important inquiries. A number of working groups look after certain specific subjects and the Society collaborates with other Internet-related organisations. The ISOC-SE has been actively engaged in the work to establish an organisation for domain name management in Sweden and appoints two board members to the II Foundation.

TU-stiftelsen

The sole purpose of the Stiftelsen for telematikens utveckling (The Foundation for Telematic Development – the TU Foundation) is to be owner of the Netnod Internet Exchange in Sweden AB. The structure of the foundation has been chosen to create stable and long-term ownership structure for Netnod AB. In this way, it is guaranteed that national Internet exchange points are operated and developed in a competition-neutral and independent way.

Netnod AB

Netnod Internet Exchange in Sweden AB (Netnod) establishes and operates exchange points for the exchange of traffic on the Internet between the various operators' parts of the network. Netnod was established as a competition-neutral and independent organisation for these exchange points. Netnod AB is owned by the TU Foundation. The purpose of the exchange points is to ensure high reliability in the central parts of the Internet in Sweden. For a long time, a large part of the Internet traffic in Sweden had travelled through the exchange point in Stockholm (previously called D-GIX). This was doubled in 1997 to reduce vulnerability and exchange points in Gothenburg, Malmö, Sundsvall and Luleå have now been established. Each operator pays a fixed annual charge for connection to an Internet exchange point. This charge is calculated to cover the operational costs of the exchange point as well as enabling the establishment of new exchange points. Netnod consults the Internet operators with national coverage in Sweden about all important issues. This occurs, among other ways, through participation in SOF (see below).

SOF

Svenska Operatörers Forum (The Swedish Operators Forum – SOF) is a collaborating body for the main operators on the Internet in Sweden. SOF mainly works with issues concerning national Internet exchange points, interconnection and other functions and operational issues that are necessary for the Internet to function well in Sweden. SOF worked informally for many years, but became a not-for-profit association in May 1999. SOF is represented in the II Foundation and has been a reference body for the Swedish Agency for Public Management's Internet inquiry. SOF can also be described as the counterpart to Netnod, the company that manages the national exchange points in Sweden. SOF is principally composed of operators with a direct connection to the national Internet exchange points on the network.

Autonomica

Autonomica is the company that, on the assignment of its owner Netnod, looks after the operation of the Internet exchange points in Sweden. Autonomica is also responsible for the operation of one of the DNS root servers located in Sweden, as well for as a series of joint competition-neutral services in the Swedish branch of the Internet. Among others, several experts on the DNS system and advanced routing work at the company.

SUNET

Before commercial suppliers had started to use Internet technology and had established themselves as suppliers of Internet services, the universities had shown the way by connecting their computer network to the Internet. The Swedish University Computer Network (SUNET) linked together the country's universities and colleges. Following a Government initiative, many of the country's museums and libraries also gained access to the Internet via SUNET. SUNET offers those organisations that are connected all of the normal Internet services, including Multicast and the transmission of e-mail as fax. Furthermore, the organisation has some popular content services, for example a large and popular FTP archive (ftp.sunet.se) where software and other files can be downloaded, an electronic catalogue of e-mail addresses and a web catalogue of web addresses that are grouped by subject. SUNET is managed by a board mainly made up of representatives from higher education. Administratively, SUNET answers to the Swedish Research Council. Umeå University has been assigned responsibility for the coordination and development of SUNET and the responsibility for SUNET's information services. KTH has been assigned responsibility for the operation along with Telia, who has been assigned to look after the basic supervision. SUNET is a part of the Nordic university computer network, NORDUnet, which links together the university computer networks of Nordic countries with high capacity connections. This is then connected to the rest of the Internet. In addition to basic Internet services, NORDUnet operates a DNS root name server with Netnod. The operation and supervision of NORDUnet is looked after by KTHNOC (see below).

KTHNOC

The KTH Network Operation Center (KTHNOC) is a competence centre at the Royal Institute of Technology in Stockholm. KTHNOC has operational and developmental responsibility on the assignment of customers and is responsible, among other things, for parts of the central operation of the Swedish University Computer Network, SUNET, and the Nordic equivalent, NORDUnet.

KTHNOC has played a significant role in the development of the Internet in Sweden, principally through having had operational responsibility for the first operator exchange point in the country for a number of years.

SNUS

The Swedish Network Users' Society (SNUS) is a not-for-profit association for Swedish network users aimed at increasing network knowledge in Sweden and thereby our national competiveness. SNUS is principally aimed at the technical aspects of network use. SNUS works to disseminate knowledge, mainly through working groups, seminars, test reports and a member magazine. Its aim is to increase the understanding of network technology, propel the development of interconnection and collaboration within the field and test which technical solutions function in reality. SNUS is based on individual membership. Businesses can also be members, but this is going to be phased out. SNUS is most well known for its interoperability tests. These are large tests where manufacturers, in the full glare of publicity, test whether their hardware and software products can interact as intended with other products.

SSNf

The Swedish Urban Network Association (SSNf) is an independent trade organisation for network owners who are actively engaged in the development of a broadband infrastructure. The association was founded in 1998 and the members are municipalities and companies that own or operate communications networks that are accessible by everyone. It also has members in the operator and supplier areas of the telecommunications and data communications sector. SSNf looks after the interests of network owners where there is a need to work towards an alternative, independent infrastructure for the telecommunications and data communications market that stimulates competition between service providers in all parts of the country. The Association also looks after the interests of network owners in its capacity as an advisory body on legislation and standardisation issues and follows developments within technology and the market. The Association also offers its members the opportunity to exchange experiences on matters such as operation and maintenance, operating reliability and documentation.

BitoS

Branschföreningen för innehålls- och tjänsteleverantörer på onlinemarknaden i Sverige (The Trade Association for Content and Service Suppliers on Online Markets in Sweden – BitoS) brings together businesses that develop and sell services via the Internet and in other electronic environments. The work of BitoS primarily takes place through various work groups that fund their operations themselves. The Association has the task of working for a clear, flexible and technology-independent set of rules and regulations facilitating the establishment of a market subject to free competition and based on open solutions. The Association is also working towards members following good business practices. BitoS represents and markets the trade relating to content services and also acts as an advisory body. The Association has (through petitions, among other things) run a campaign against the Personal Data Act and the threat to freedom of expression on the networks that this Act constitutes. Another important issue for BitoS is to create an instrument to measure visits on websites and other values that are important to develop the Internet as a medium for business.

IT-företagen

IT-Företagen is a trade organisation for companies that develop, manufacture and sell IT products and IT services. IT-Företagen has approximately 500 member companies. IT-Företagen promotes the increasing use of IT in Sweden and provides vital support to the development of individual member companies by promoting business opportunities and removng barriers. IT-Företagen is one of the member organisations of the Confederation of Swedish Enterprise. Any company that is a member of IT-Företagen is also a member of the Confederation of Swedish Enterprise.

The Industry Security Delegation of the Confederation of Swedish Enterprise

The Industry Security Delegation (NSD) is a forum for the exchange of ideas, experience and knowledge for issues relating to security. This is to promote better security and risk awareness in business and among the public. Work within the NSD aims to encourage risks being assumed on a well-informed basis through the exchange of experiences, increased knowledge, continuous awareness of reality and contacts with stakeholders within the field of security.

Confederation of Swedish Enterprise

The Confederation of Swedish Enterprise represents just over 55 000 small, medium-sized and large businesses. It is organised into 51 trade and employer associations. The Confederation is made up of members of the associations of the Confederation of Swedish Enterprises. The Security Issues Section of the Confederation of Swedish Enterprises arranges regular courses, some of which are organised in collaboration with the Confederation's Security Delegation.

SIG Security

SIG Security is a non-profit association and comprises 1800 members with a board that is elected at the annual general meeting of the association. SIG Security, which was founded in 1980, is an interest group for people active within the field of information security, and members are found in all sectors of society. The association's area of operation is to foster understanding about and provide inspiration for work concerning information security.

Appendix 3 – The operators' responsibility for security of their services

It is stated in Chapter 6, Section 3 of The Electronic Communications Act that a party that provides a public electronic communications service shall implement appropriate measures to ensure that the data processed is protected. Article 4 of the Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (referred to below as 'the Directive') deals with the obligation of service providers to implement appropriate technical and organisational measures measures to safeguard security of their services, which could possibly comprise measures to prevent the dissemination of virus and malicious codes.[28] Article 4 has been implemented in Sweden through Chapter 6, Section 3 of The Electronic Communications Act. This provision has been formulated so that it refers to security of 'data processed' and not as the provision is formulated in the Directive, 'security of its services'. It has thereby been given a significantly more limited scope of application than in the Directive.[29] As Chapter 6, Section 3 of the Act is worded, it is unclear whether the provision could possibly be used to filter virus traffic, for example, as it does not appear to be obvious that this contributes to enhancing the security of the 'data processed'.

The report PTS-ER 2005:7, 'Swedish strategy to secure the Internet infrastructure', concludes that there are currently few opportunities for operators to implement active measures, such as the filtering of communications, unless they have obtained the consent of all of the users affected. This report also proposes that operators should be given an opportunity to implement such measures.

In Sweden's standpoint for the forthcoming review of the EU's systems of rules and regulations for electronic communications, including the recommendations on relevant markets – response to the European Commission's 'Call for input' of 25 November 2005, of 8 February 2006, it has been pointed out that the opportunity of filtering should be investigated. Filtering in this context refers to the opportunity of all operators to implement necessary measures from a security perspective, such as, for example, the filtering of computer viruses, overload attacks, etc.

Whether this should really only be an opportunity or, in the event of a certain minimum level of security, should instead constitute an obligation, may be

[28] The possibility of filtering and impeding Spam under the Directive is dealt with, for example in ENISA's 'Survey on Industry Measures taken to comply with National Measures implementing Provisions of the Regulatory Framework for Electronic Communications relating to the Security of Services', Ref. number ENISA/TD/SP/06/0055, published in February 2006.

[29] It can be noted that Article 3 of the Directive should be applied to 'the processing of personal data' in connection with electronic communications services, even if it can be discerned, according to the preamble under item 20, that the aim of the legislator is to provide the service provider with some scope for action and a requirement to as such maintain the security of the service.

discussed. As regards the general measures required to ensure that the services and networks satisfy reasonable function and security requirements, such requirements may be regulated by general obligations. As pointed out above, Article 4 of the Directive includes an obligation for operators to implement appropriate technical and organisational measures to safeguard security of their services, which could possibly comprise measures to prevent the spreading of viruses and malicious codes. The aim of the Directive appears to be to impose upon operators the responsibility for impeding, discovering and responding to unacceptable behaviour, unintentional interruption and other disruptions in communications. Chapter 6, Section 3 of The Electronic Communications Act refers to the security of 'data processed', which means that it is unclear whether the provision could be possibly used to filter, for example, virus traffic, as it does not seem obvious that this contributes to enhancing security for the 'data processed'. It could possibly be argued that an operator should not only have an opportunity to implement measures, as in the current case, but should also have an obligation to implement, in any event, such measures as are necessary. Amending Chapter 6, Section 3 of the Act so that it corresponds more closely with the Directive could possibly provide the supervisory authorities with an opportunity to impose such requirements.

As regards more specific and active measures, such as the filtering of traffic, it may also be considered that operators should have an obligation to implement measures, as the efficient prevention of dissemination requires that several providers are implementing similar measures. A later review and analysis of both the action of the stakeholders and the general level of security may give PTS cause to revert to these adjustments.

Appendix 4 – CIIP Directory, national Swedish contact points

The purpose of the 'CIIP-directory' is to provide a reference document of national contacts in the field of Critical Information Infrastructure Protection (CIIP). The document was initiated by the G8 'CIIP Experts Conference' in March 2003 and is administered by the British infrastructure security authority, the National Infrastructure Security Co-ordination Centre, NISCC. The CIIP directory currently contains the government contact details for 18 countries.

No.	Area of expertise	Stakeholder responsible	Contact
1	Alert & Warning	PTS	Sitic
2	Threat	PTS	Sitic
		RPS	S-BIT
		KBM	KBM
3	Vulnerability	PTS	Sitic
		FRA	FRA
4	Industry	KBM	KBM
		PTS	PTS
5	Policy	Government Offices	Ministry of Industry, Employment and Communications
6	R & D	KBM	KBM
7	Sharing	PTS	PTS
		KBM	KBM
8	Crime	RPS	S-BIT
9	SCADA	KBM	KBM
		FRA	FRA

No.	Area of expertise	Responsible stakeholder	Contact
10	Assurance	FMV	FMV (CSEC)
		KBM	KBM
11	Standards	KBM	KBM
		FMV	FMV (CSEC)
		PTS	PTS
12	Resilience	KBM	SOTI
		PTS	PTS
13	Exercises	KBM	KBM
		PTS	PTS
14	Defence	Swedish Armed Forces	FM CERT